

# 9 Lessons Learned from Smart Grid Implementations

**How Smart Grid Technology Is Blazing the Trail  
for All Industrial Networks**

A White Paper from



**GarrettCom<sup>®</sup>**

*Industrial Networking at Its Best<sup>SM</sup>*

**May 2011**

[www.GarrettCom.com](http://www.GarrettCom.com)

## 9 LESSONS LEARNED FROM SMART GRID IMPLEMENTATIONS

By Jim Krachenfels, GarrettCom Marketing Manager

Planning for the Smart Grid has had a huge impact on the way power utilities manage their operating data and control networks. The convergence of IP technology, Smart Grid imperatives and the increased need for security as characterized in the NERC CIP regulations in North America has provided an opportunity for power utilities to rethink their operating strategies and come up with innovative ways to integrate the new and the old in order to position themselves for the future. This exercise has generated a body of knowledge that is instructive for all industrial networking applications.

### IP – the Game-changing Factor Enabling Smart Grid

IP is a game-changing technology that is the basis for three compelling benefits for power utilities—particularly in the areas of substation automation and power transmission and distribution processes

- the overall reduction of operations expense from creating an IP-based infrastructure that integrates operational and non-operational data
- viable distributed intelligence applications that allow decision making in remote locations as well as in the central operations or central offices
- comprehensive grid operations and grid management security

As the power utility community has grappled with these opportunities and issues, nine lessons have emerged that can be applied to any industrial networking system

1. Plan for scalable bandwidth to handle the steadily increasing demand for data
2. Explore heavier-duty switches and routers to support expanding demands for more equipment attachments
3. Expect to integrate wireless communications for simple, cost-effective data links to remote sites
4. Upgrade to equipment with precision timing features to enable synchronized data management and control actions
5. Know how to integrate serial equipment into your complex IP network – it's not going away any time soon
6. Choose switches with flexible port configurations to easily integrate various types of new and existing equipment

7. Integrate a strategy for cyber security as well as a physical security to keep control networks safe
8. Bring corporate IT into data management as a partner
9. Understand that developing an outstanding industrial network is a work in process, not a one-time event

The joint imperatives of 9/11 and the Smart Grid have created a massive amount of development and retrofit activity in power utilities. The need to protect the security of power installations and the data that is passing in increasing quantities within and among substations and central offices is high. While the utilities are struggling with this issue, Smart Grid requires two-way communications with users to encourage smart use of power. Opening communication while protecting the privacy of the users and the security of the transmissions adds another layer of complexity.

Government organizations such as NERC (North American Electric Reliability Corporation), standards groups such as IEC, and industry organizations such as The International Instrument Users Association (WIB), have all contributed to the development of protocols, standards and requirements for addressing these challenges. ([WIB](#) is the first international standard that outlines a set of specific requirements focusing on cyber security best practices for suppliers of industrial automation and control systems). Power utilities themselves, separately and through cooperative efforts, have also provided insights and ideas.

### **Smart Grid = Increased Complexity**

Daniel Wong, Principal Engineer, Protection & Control at AltaLink, summarized the opportunity—and the challenges—using Fig. 1 at the 2011 DistribuTECH Conference & Exposition. Suddenly, a relatively simple operation became more complex with two-way communication and multiple stakeholders replacing a simple one-way transaction from an omnipotent and (from the user’s standpoint) arbitrary source. Not only did control functions increase in complexity, but also non-operational data management increased dramatically, and because it was transported far beyond the boundaries of a single facility, issues including timing and security had to be addressed at a much more comprehensive level.

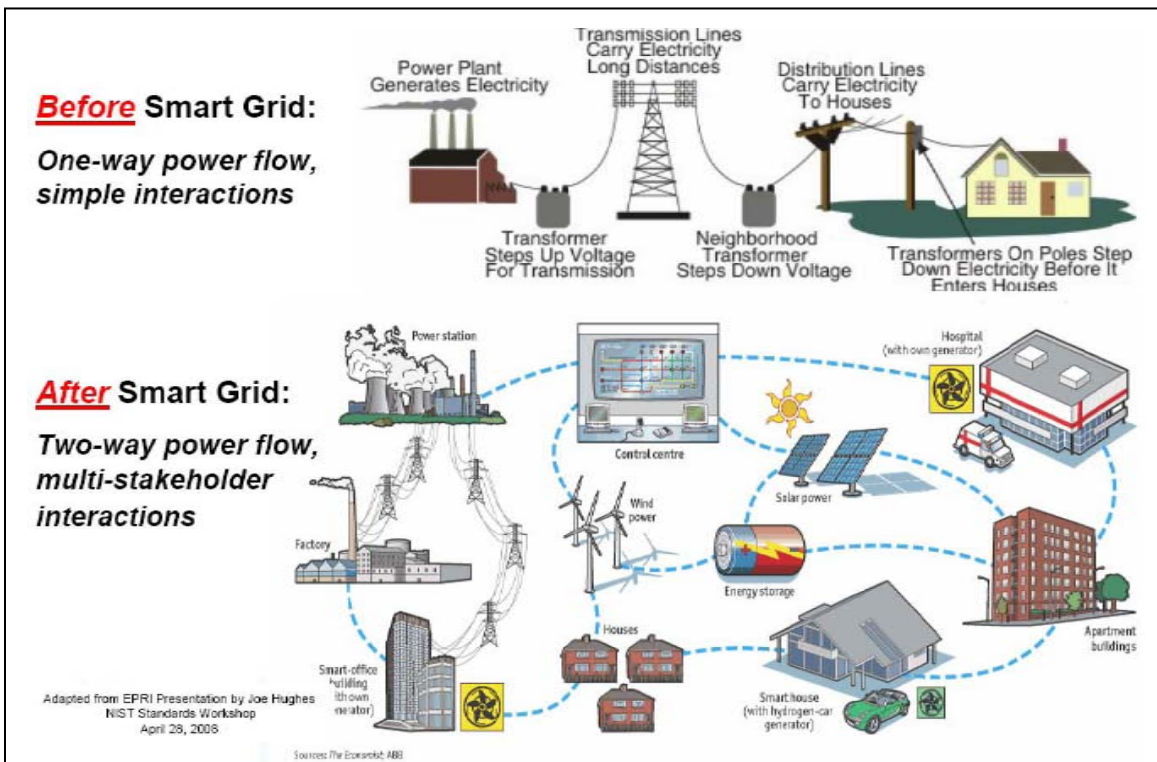


Figure 1

This is a starting point for understanding the nine lessons and their relationship to a broader range of industrial applications.

**The Basics: Bandwidth, Capacity and Hardening**

It should be clear from Fig.1 that additional bandwidth is necessary to successfully implement any Smart Grid strategy. Fiber backbones are a basis of most large-scale data management strategies because of fiber’s excellent properties for providing high bandwidth over long distances, noise immunity, and inherent security features (because it is not easy to tap). Fiber is also flexible enough to support the installation of new nodes as demand on the network increases. With increased acceptance, coupled with the step rise in the cost of copper, fiber is seen as a cost-effective alternative and a secure alternative to dedicated T1 or dial up lines, and it is well matched with IP infrastructure solutions.

Just as the numbers of entities on the overall Smart Grid infrastructure are increasing, so are the numbers of nodes required within each of those entities. Using a substation as an example (Fig. 2), it is possible to observe the increasing number of intelligent IP-enabled devices available for

connection—from sensors and monitors all the way to new security devices such as video cameras, card readers, and intelligent access control devices including fingerprint or iris scanners.

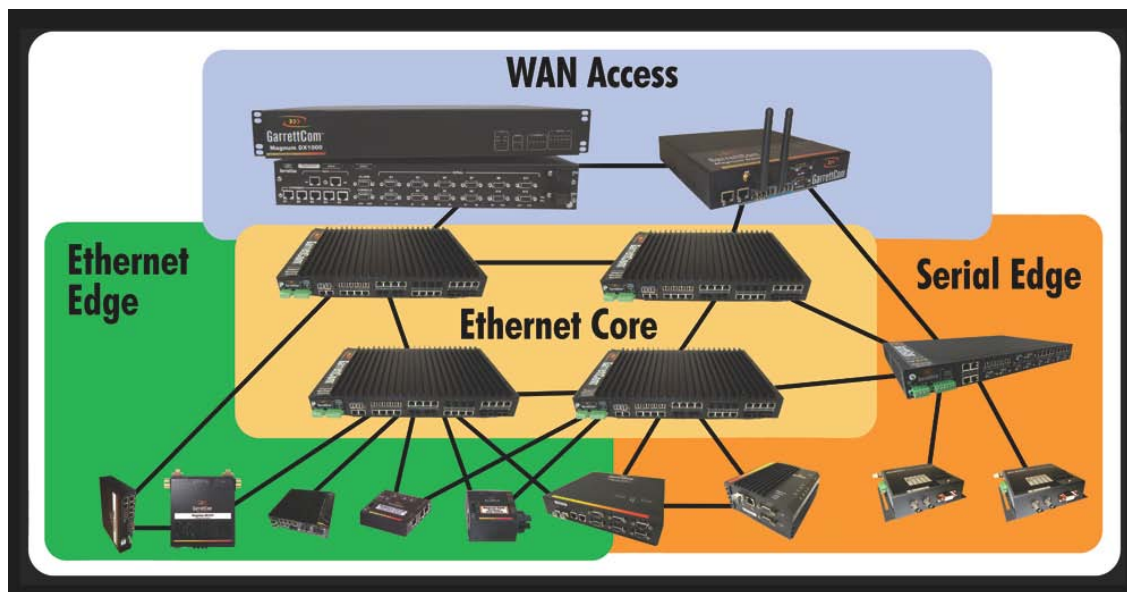


Figure 2

To cleanly support data and control systems demand generated from increased substation complexity, designers need to be able to choose Ethernet switches and routers equipped with varying numbers of ports. Particularly at the core of the network, it is inefficient and expensive to pile multiple low-port-count switches together, wasting two ports per device for connectivity, and this practice results in additional and unnecessary points of failure. Where larger port-count devices were once deployed only in climate-controlled central offices, today one sees installations of 24-port and 36-port switches at the nerve center of the substation, where the environmental conditions demand substantial hardening—in fact, [substation-level hardening](#). These larger substation switches connect with smaller-port-count switches installed as the deployment approaches the network edge.

There are a number of components needed to create a hardened, robust switch, but the most significant are

- Extended temperature range for extreme environments (-40°C to +85°C)

- Strong EMC design to protect against electrical magnetic interference (EMI), which is often prevalent in substation environments
- Convection-cooling, eliminating the need for fans as a potential point of failure in hot, high-particulate environments, and protecting against the intrusion of dust and dirt
- Shock and vibration resistance
- Fiber configurability to support security and high-bandwidth demands
- DC power as well as AC to support installation in areas requiring specialized power sources
- Redundancy options to ensure high availability

### **WHAT IS INDUSTRIAL ETHERNET?**

It is important to note that “Industrial Ethernet” is more than just a marketing phrase; it describes the environment in which an Ethernet device must operate. Hardened Ethernet switches are a complete rethinking and redesign of office-based Ethernet components. Electronics in extreme industrial environments can be subjected to high levels of EMI, heat and moisture, as well as dust, dirt, and corrosive chemicals. In addition, required levels of availability may exceed those for a commercial environment. It’s never good when the network goes down in an office, but it’s likely to have a more serious impact if an electrical blackout causes hundreds of thousands of subscribers to lose power.

The ability to support increased bandwidth and an increasing number of IEDs, combined with the ability to survive in extreme environments are all critical to substation success.

### **Transport Flexibility – Wireless, Ethernet, Serial**

Another aspect of Smart Grid networks is the increasing demand for wireless connectivity both for the larger grid and within specific facilities. Distributed alternative power generation resources, as well as the need for two-way communications at users’ meters, often require wireless connectivity support. Wireless provides an alternative to support the needs of the growing infrastructure, and, in fact, the use of wireless connectivity in developing countries has allowed some of them to accelerate their infrastructure development. Within a facility, wireless is increasingly being used, along with Power over Ethernet (PoE), for security applications and other specific functions where wiring is difficult or uneconomical.

“Wireless” is not a monolithic concept, and the broad variety of wireless connectivity options are beyond the scope of this paper. Nonetheless, it is important in planning a network to ensure that wireless connectivity is an option, at least at the router level, to support growing demand for this type of connectivity.

At the other end of the spectrum, serial equipment is here for the long run. In power utilities, much of the networking equipment installed to date has used serial connectivity—and it has been there for decades. Serial is still popular in new equipment installations today. While some utilities may have some Greenfield projects where they are deploying fully IP-based networks, most will be using serial components for years to come.

IP technology advances are making it possible to more fully utilize and integrate serial data, and, in fact, include it in IP security protocols. For this reason, ease in connecting serial devices into the IP architecture is a high priority. Terminal servers and routers that support both Ethernet and serial devices reduce complexity and also provide greater security options (see Fig. 3).

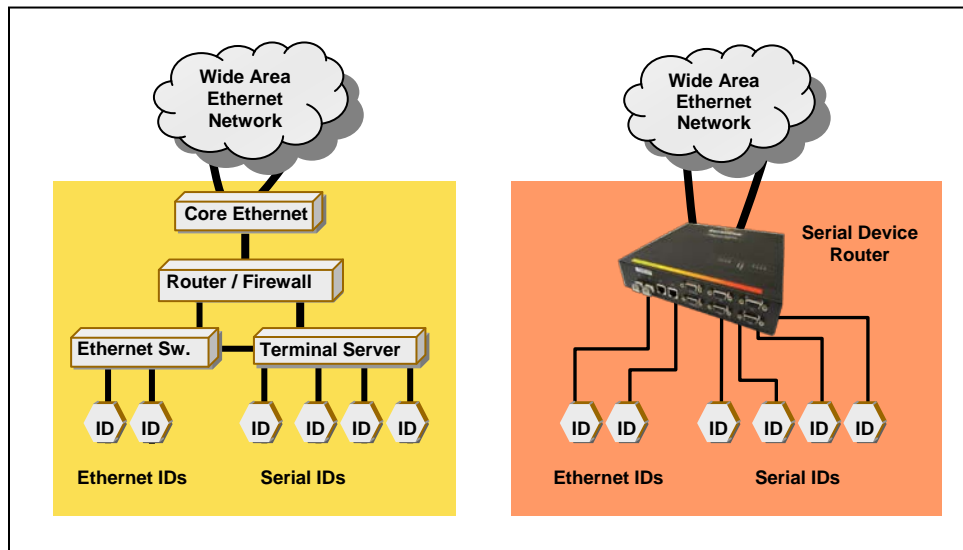


Figure 3

A typical substation will have IEDs and other equipment outfitted with a wide range of standard Ethernet and serial connectors. Modular technologies that support the mixing and matching of blocks of ports on individual switches and routers provide cost-effective and easy-to-deploy alternatives to fixed-port boxes.

## **“But I thought Arizona was on Mountain Time . . .”**

Continued integration has made precision timing much more important as well. Most of us are well aware of the challenges in communication that result from coordinating different time zones, especially since some states don't follow daylight savings practices. Within a Smart Grid infrastructure, the challenge is even more complex.

In the case of a security incident, it is necessary to ensure that the time stamps on data from various cameras and intrusion detection devices are synchronized to a universal clock to ensure that accurate sequencing of events can be tracked. Internally, when there are operational events, it is equally necessary to make sure that comparisons of data—even from serial devices in the network—are based upon a single time standard. An example of a time code standard is IRIG-B, developed by Inter-Range Instrumentation Group, the standards body of the Range Commanders Council; it offers a standard by which it is possible to synchronize geographically separated instruments throughout a power delivery system.

## **Decision Making at the Source and the Expanded Role of Security**

The good and the bad news about IP is that it makes it possible to transfer and manage large amounts of data over geographically separated areas. This enables informed decision-making at remote locations—from determining whether a user should be provided access to certain operational or non-operational data to helping a commercial power user to decide when to schedule power-hungry but discretionary activities. In addition to the challenges of ensuring consistent system-wide timing synchronization, flexible access to information in a distributed environment creates security issues that need to be addressed to ensure the integrity of the operation.

Many industrial facilities are watching what is happening in the power utility industry because of stringent NERC mandates. NERC created a series of security requirements for the power utility industry that were meant to protect critical assets. These requirements have impacted how power utilities manage their business. A set of requirements that is expected to evolve over time CIP requirements today address the following network components of a substation security

- CIP-002: Critical Cyber Asset (CCA) Identification—which require identification of switches, routers, and data concentrators with access to the outside world
- CIP-005: Electronic Security Perimeter(s)— which requires switches and routers with access to the outside world to be protected by access control applications such as firewalls
- CIP-006: Physical Security of CCAs—which typically requires an integrated cyber and physical security strategy to protect the communication cabinet and the SCADA cabinet—and, in fact, the entire plant
- CIP-007: System Security Management—which includes test procedures, ports and services, patch management, prevention of intrusion by malicious software account management, and security status monitoring via syslogs
- CIP-009: Recovery Plans for CCAs—which include change control and basic recovery kits or protocols

While some utilities have adopted an attitude of removing as many critical assets from the inter-facility communications network as possible, the momentum toward shared data networks is huge because of the possibilities offered in terms of operational efficiency and distributed decision-making. In addition, as StuxNet proved in 2010, even unconnected systems can fall victim to the good old “Adidas network” as employees intentionally or unintentionally expose systems to malicious attacks.

Developing a strong cyber (and physical) security strategy is critical in today's world. Fig. 4 shows a network that is wide open to attack.

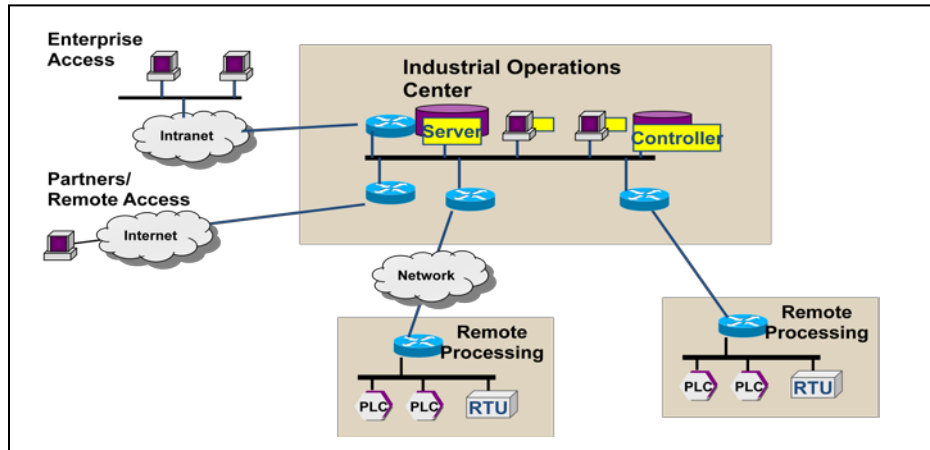


Figure 4

Fig. 5 shows the same type system with a stringent physical and cyber security layer inserted.

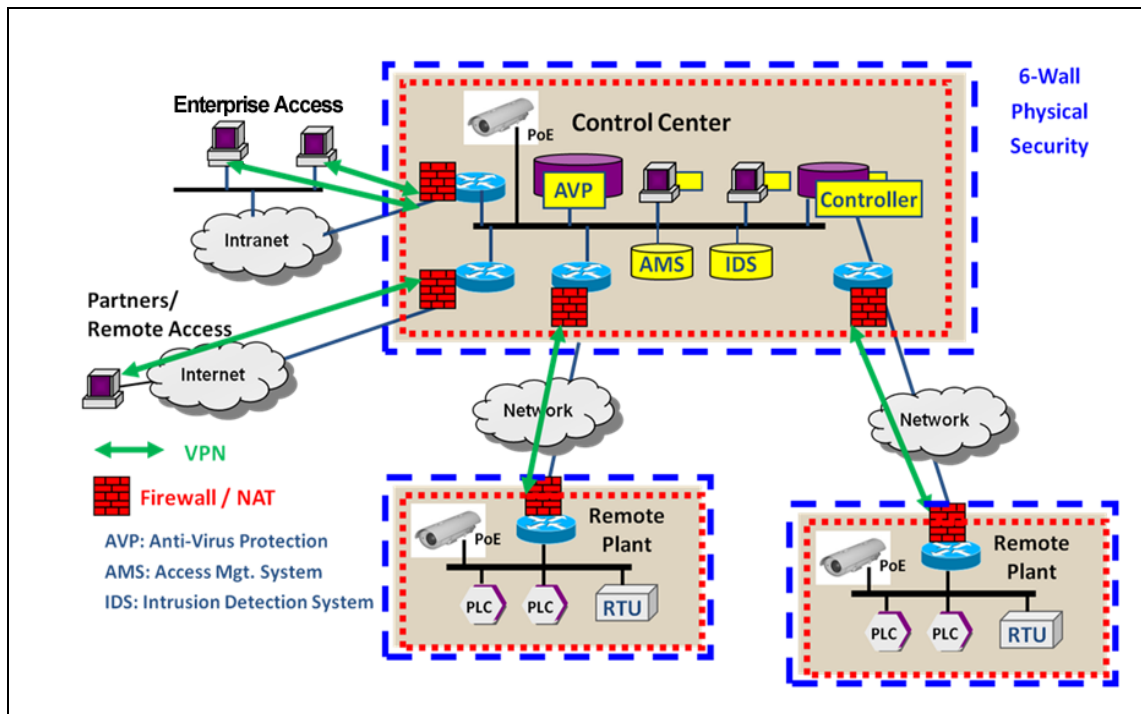


Figure 5

Fig. 6 goes one step further, implementing CIP 007 requirements for access control.

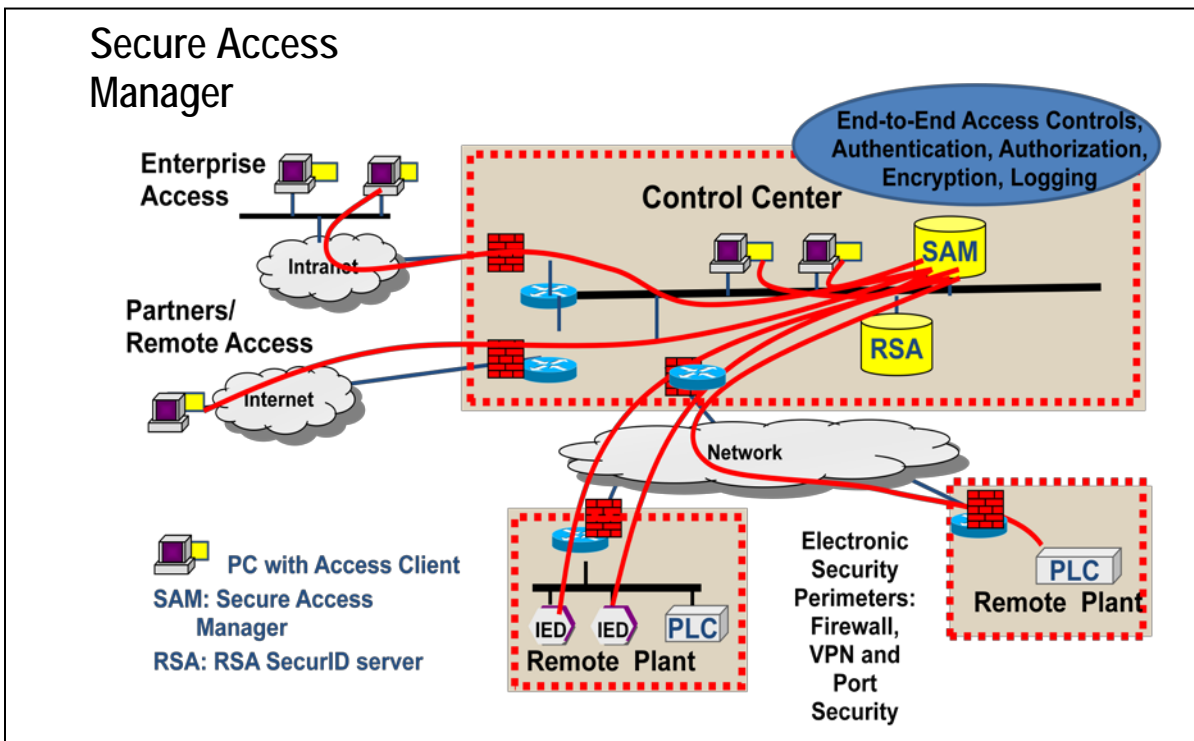


Figure 6

Some of the components involved in implementing a power utility security strategy are

- *Physical security:* Cyber security starts with physical security. If outsiders cannot gain access to the premises, it is harder for them to access sensitive data.
- *Firewalls:* It is necessary to protect cyber assets with firewalls at the cyber perimeters of critical cyber assets just as the physical perimeter is protected.
- *Port access control:* In addition to denying access to the building, disallowing unauthorized devices to be plugged into ports on switches and routers makes for a more secure environment.
- *Password health and authentication:* Prudent practices should include changing passwords regularly—and making sure that they are long enough and complex enough that they are difficult to crack. Authentication is more secure than simple authorization (which only ensures the person accessing the system is using the right code); it goes one

step further by ensuring that the person or device requesting access is who he says he is.

- *Encryption*: Fiber cabling is much more secure than copper when used to relay data between secure locations. Sending encrypted data adds an extra level of protection outside secure facilities.
- *VPNs and VLANs*: Virtual Private Networks and Virtual LANS both provide extra layers of security for transmissions over multi-purpose transport networks.
- *Employee training*: Security is only as good as the practices that are in place. Employees, without meaning to create a security breach, can be lax with passwords, security codes and other primary measures unless they are educated – and reminded – about the importance of security.

For more information on cyber security, see GarrettCom’s white paper titled “[Cyber Security for Industrial Applications](#)”.

### **Working Well Together**

As is made clear by the discussion on security, operational facilities are more hard-pressed than ever to seamlessly integrate data flow with corporate IT. While conflicting priorities and needs have traditionally made the two groups “friendly adversaries” at best and outright enemies at worst, there is a growing body of stories on how the two groups have collaborated to bring about the best results. Simply put, the two groups have very different goals and objectives in many cases – the precision timing issues and maintenance schedules on the plant floor can conflict with corporate information flows. In one memorable situation, a customer recounted the story where plant work was disrupted when a single IP network was installed and a corporate data run consumed all available bandwidth for plant operations and shut down the factory’s night shift production line. However, multi-discipline workgroups are identifying and solving these types of problems – and providing more information and greater efficiencies across entire organizations.

### **An Ongoing Project**

In power utilities, as well as other industrial facilities, there is a growing understanding that creating an efficient network is a work in progress. Progress is measured in increments and phrases: from quality circles and CPI (Continuous Process Improvement) to the planned phasing

in of NERC-CIP requirements to the practical demands of resource planning. In the latter case, it is rarely feasible to implement the wholesale overhaul of physical plants that have hundreds of thousands—or millions of dollars invested in equipment that has not reached the end of its life cycle.

### **The Blue Ridge EMC Story**

Blue Ridge EMC recently executed an upgrade as a result of both NERC and Smart Grid. In order to plug into the Smart Grid, the first order of business was being able to provide reliable, IP-based communications services in its demanding service area in northwestern North Carolina. Much of the territory it serves is located in the Appalachian Mountain range.

Blue Ridge had to provide communications to remote locations at a reasonable cost to enable its TWACS AMR System to remotely read electric power meters with a granularity of up to an hour. AMR would save costs and reduce vehicle rolls (often difficult or impossible during severe winter weather). In designing the network for the substations, Blue Ridge followed NERC CIP standards, which helped to insure network security and reliability.

Fiber connectivity at substations is the logical choice for backhauling meter reading and load analysis data to the corporate office. Where IEDs have been installed, engineers can analyze fault data and the dispatchers in the operations center can ping individual meters to determine exactly where an outage has occurred.

#### ***Network Equipment Requirements***

To build out this project, Blue Ridge Telecom/IT team needed switching equipment that was hardened to withstand the electrical and environmental extremes found in substations and beyond in the distribution system. In addition, new equipment had to be compatible with the existing network equipment; had to meet today's NERC CIP requirements (as well as be flexible enough to support anticipated future directions); and had to be easily monitored and managed remotely.

Security gateways made by Astaro Corp. and Magnum 6K Ethernet Managed Switches from GarrettCom, Inc., formed the basis of the communications network. Where fiber has been deployed, it is connected directly to the Magnum switch at the substation. To securely transmit information over the DSL lines, the security gateways act as a firewall between the substation

network and the internet. The network switching equipment protects the substation network and transmits data over a separate DSL line to corporate. All unused ports on the Magnum switches are disabled to further enhance security. Fiber was used to deploy multiple VLANs to segregate engineering applications and corporate Ethernet traffic; DSL does not support VLANs, and therefore works best in distribution stations that have minimal transmission equipment.

Fig. 7 shows the new substation and distribution layout that is a combination of Ethernet-connected IEDs and serial links.

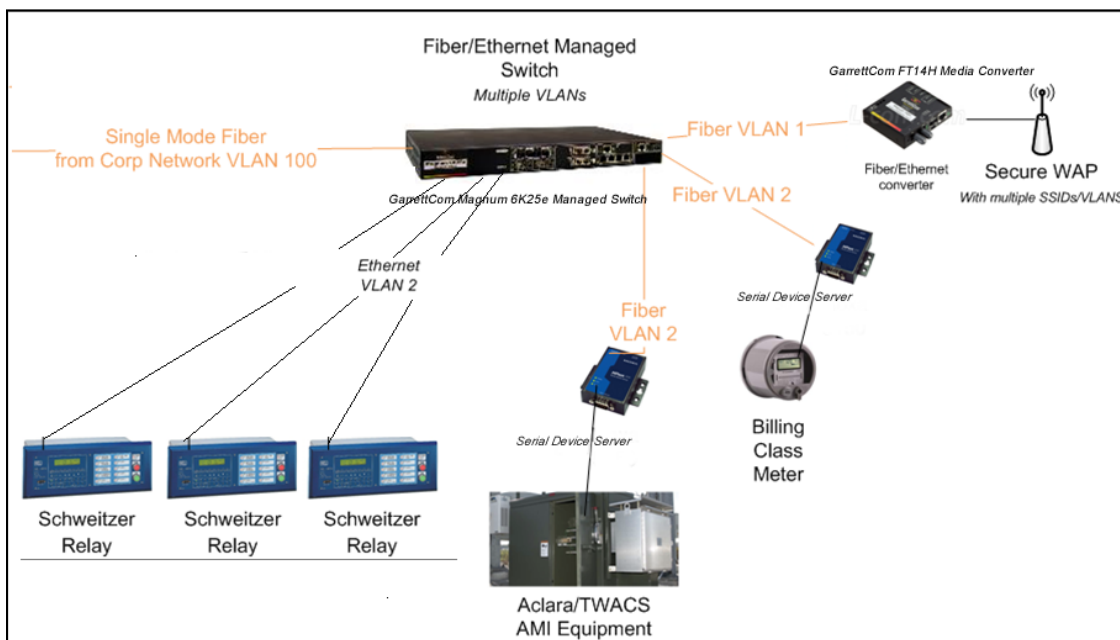


Figure 7

With its new system in place, Blue Ridge enjoys both the additional flexibility of the Smart Grid and the security afforded by its expanded, secure IP network.

## Summary

The combination of NERC and Smart Grid initiatives requires a major review of power utilities assumptions and objectives in collecting, managing and analyzing data. Consequently, the nine lessons discussed become increasingly critical to success

- 1) Plan to scale bandwidth to accommodate increasing demand for data
- 2) Look for a family of industrial-strength switches and routers to support expanding demands for equipment attachment—ranging from 24- and 36-port boxes for centralized data management to small four-port units to support the edge
- 3) Expect wireless requirements and have a plan for integrating them
- 4) Ensure that distributed data is synchronized
- 5) Create an architecture that can easily integrate serial equipment into the IP network
- 6) Choose equipment with flexible port configurations for easy integration of any IEDs
- 7) Build in cyber and physical security—it is no longer an option
- 8) Bring corporate IT into the loop as a partner
- 9) Prepare for phased continuous evolution of your network

GarrettCom is dedicated to stepping up to the plate with solutions that combine high availability networking technologies, industrial-strength design, flexibility, and innovative cyber-security solutions. These solutions are engineered to support industrial networking customers that devise, maintain, and improve the systems that support the expanding needs for operational and non-operational data in the 21<sup>st</sup> century. The challenges industries face today can become a springboard to more efficient, more effective operational practices. Through the use of standards-compliant hardware and software, an innovative approach to new data and data management requirements, and a broad portfolio of IP technologies and products, GarrettCom is working with customers to deliver the bandwidth, redundancy, reliability, and security to provide an extensible infrastructure that will serve them for years to come.

#####