

## **Hardened Infrastructure for Distribution Automation**

**By Lee House, GarrettCom EVP and CTO**

The Smart Grid is designed to improve electricity efficiency and reliability by deploying equipment such as automated meters for home and corporate users, two-way communications, digital sensors and remote controls. In addition, power utilities have extensive capital equipment in the field that needs to be electrically monitored for fault isolation and for cost-avoidance maintenance activities. New synchrophasors, when installed in a Smart Grid, can sample voltage and current 30 times or more per second, more than an order of magnitude more often than older supervisory control equipment, providing utilities with a much more accurate view of how the grid is performing, and possibly offering an early warning system when power surges threaten the kinds of blackouts such as the one the East Coast suffered through in 2003.

When one considers that the Smart Grid as a means of efficiently managing capital equipment, power network load, distribution efficiency, and fault prevention and isolation, then it follows that the communication networks that support these goals must be designed for continuous up-time and long life. Also, because these networks connect to equipment considered as critical infrastructure (and in many cases mandated to be so by NERC CIP), the security of these networks is also critical.

While some of the back-end networking, computing and applications can use office-grade data processing equipment, much of the networking equipment needed to deploy a Smart Grid infrastructure is “field gear”, subject to the harsh environments and demands of the cold cruel world. Appropriately hardened products from the network edge, where IEDs are first connected to the network all the way through to the switches and routers that transmit data to the IT department provide the greatest level of reliability.

### **Reliability in temperature and environmental extremes**

Office-grade equipment is designed to operate in a controlled-temperature environment, typically 0° to 40°C. The communications equipment in a power distribution operation is likely to be installed in environments that run the gamut from well below freezing to 80+°C. In addition, environmental factors such as dust, insect penetration and moisture add to reliability challenges. Industrial-grade metal casings, designed with appropriate IP ratings, often supplemented with conformal coatings to seal out moisture on the components within, are a key component of hardened electrical systems.

## Redundancy

Designing redundant network paths to every critical device through a ring topology is a simple but effective method to increase uptime in power substations and distribution systems at the edge of the communications network.

Redundant ring solutions provide two points of connectivity in a ring with one forwarding or operating port, and one backup or standby port that becomes the forwarding port when the primary port becomes inoperative because of a broken link. (Figure 1 shows a configuration in which the original primary port has been blocked and the second port has taken over.) With the latest version of Rapid Spanning Tree Protocol (RSTP 802.1D-2004), low sub-second recovery times can meet the performance requirements of almost all mission critical applications.

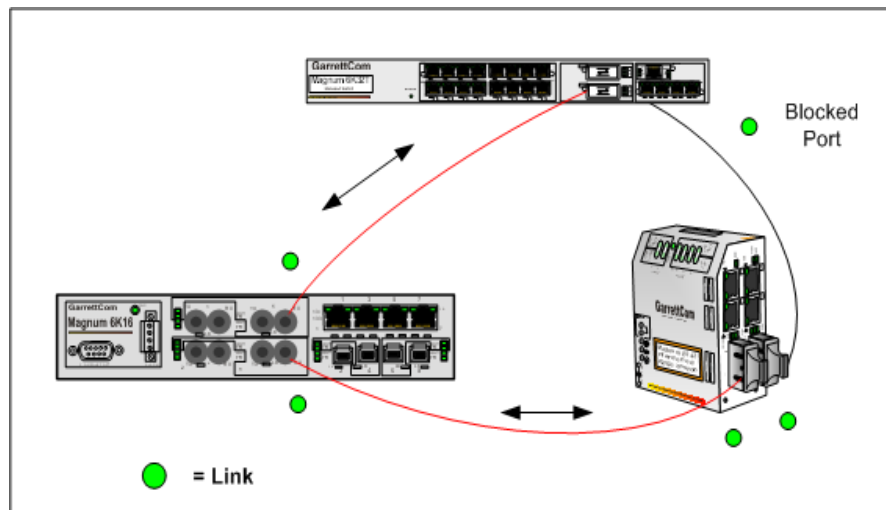


Figure 1

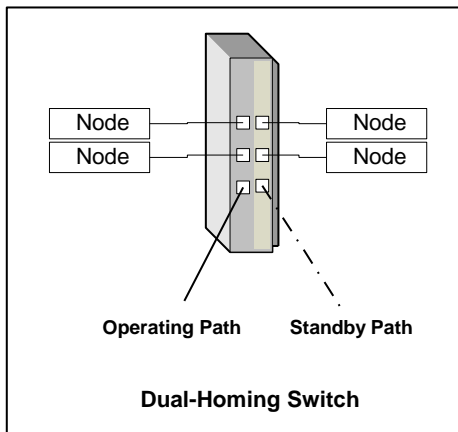


Figure 2

Dual homing adds reliability by allowing a device to be connected to the network by way of two independent connection points. One access point is the operating connection, and the other is a standby or back-up connection that is activated in the event of a failure of the operating connection.

Serial Device Routers (see Figure 3) integrate the functions of a Terminal Server, an Ethernet Switch and an IP Router with a firewall. New per-VLAN routing technology can allow a Serial Device Router to operate as multiple virtual Ethernet switches and/or multiple virtual terminal servers at the same time.

### Multi-function Integration in a Serial Device Router

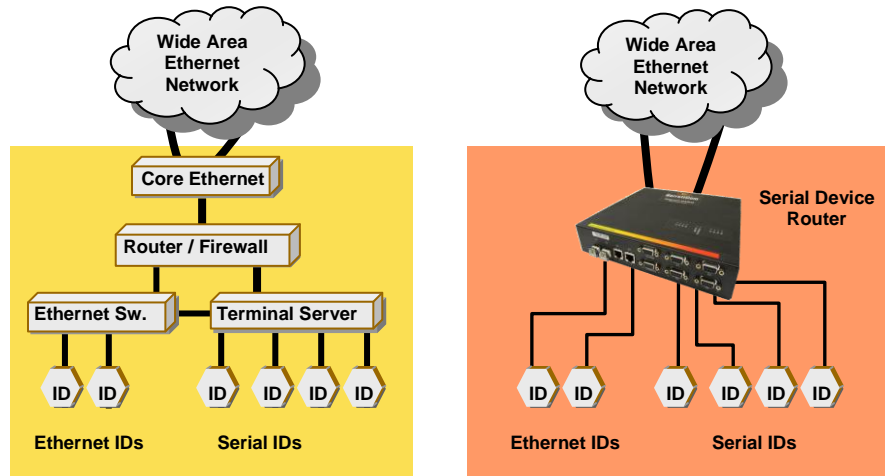


Figure 3

### Electrical Shielding

When deploying communications systems for the Smart Grid, it is important to protect electrical systems from EMI at two levels: fiber media for cabling and the metal cases typically used for industrially-hardened communications equipment, which also provide shielding.

Fiber has traditionally been employed as the backbone media and is the preferred medium for noise immunity and long-distance connectivity, but also has obvious benefits in high EMI environments. An added benefit to fiber is its extra security protection within a complex such as a substation. Security is a growing concern in these times, and, as opposed to copper, a typical media line tap will not work on fiber.

### Power Options

Power utilities typically require power options other than the standard AC used in commercial environments. The preferred voltage ranges in power utility substation automation are 88-150 VDC and

36-60 VDC, but >125 VDC, <48 VDC and 115 or 230 VAC can also be used. Modular systems that allow the customer the choice of power supply along with other configuration characteristics can provide the flexibility required for a variety of deployments.

### Cyber Security -- Defense in Depth

Defense in Depth is a layered security approach that uses several forms of network security to protect against intrusion from physical and cyber-borne attacks. The layers are setup to work in parallel, one technology overlapping, in many cases, with another; together they form a significant safeguard against attack.

### General Industrial Network Topology

Figure 4 shows a simplified look at a power utility network with multiple access points and multiple network hops (private and public) that is wide open to abuse from cyber or physical attacks.

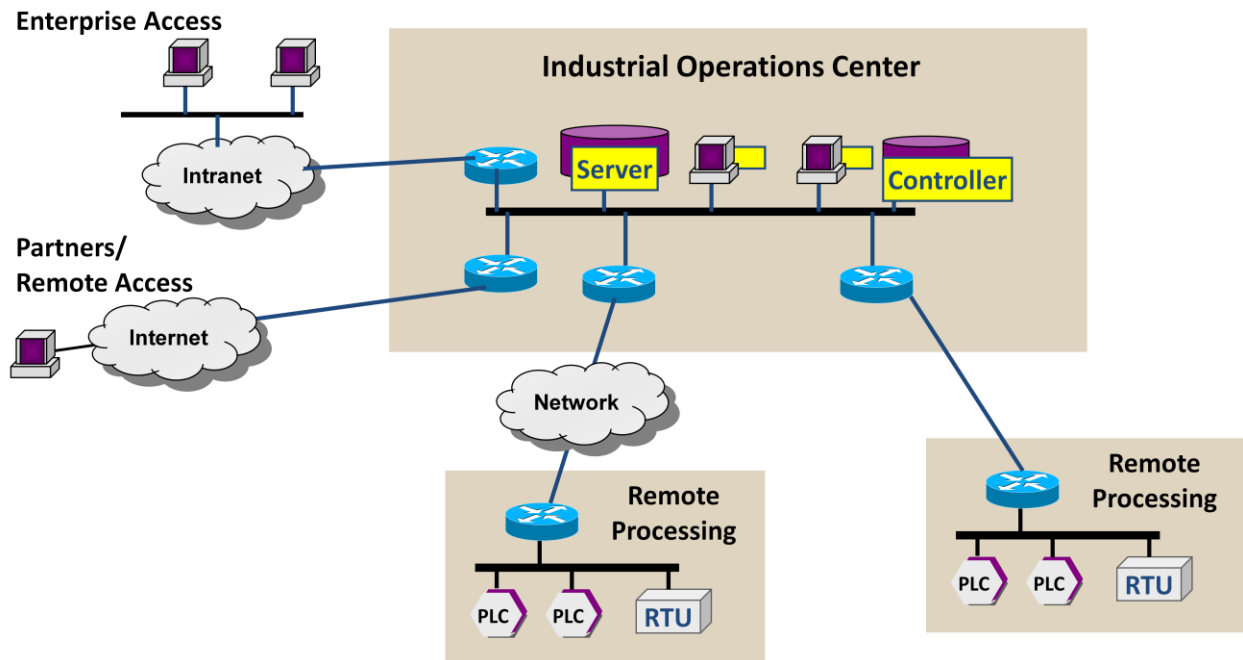


Figure 4

Defense in Depth uses a variety of techniques to protect critical assets.

**Firewalls:** Use of firewalls at the entry points to the core network and to all remote facilities provides a “gate” to protect and ensure that nothing private goes out and nothing malicious comes in. A firewall regulates the flow of traffic between computer networks of different trust levels, denying or permitting passage based on a set of rules. Network address translation (NAT) functionality provides hosts protected behind a firewall commonly with addresses in the "private address range".

**VPNs:** VPNs (Virtual Private Networks) are networks that are layered onto a more general network using specific protocols or methods to ensure “private” transmission of data. VPN sessions tunnel across the transport network in an encapsulated, typically encrypted and secure, format, making them “invisible” for all practical purposes. They can be implemented using different technologies including L2TP, IPsec, SSL/TLS VPN (with SSL/TLS) or PPTP (with MPPE).

**VLANS:** VLANS make it possible to segregate the different traffic flows (such as VoIP, video, management, and control applications) into separate broadcast/multicast domains – keeping applications more secure by limiting where the applications are visible and also providing damage control: if one of the applications is compromised, the other applications remain isolated and safe.

**SAM:** Secure Access Management systems enforce security policies using “Triple A” security (authentication, authorization and accounting), ensuring that only specifically authorized people are able to electronically access the control system components or other devices that are part of the network. SAMs also log all actions or changes that are made, making them available for later analysis.

**AMS:** Access Management System (AMS) servers obtain credentials from the end user and authenticate both the user and the target devices he is authorized to use after interrogating security systems such as Microsoft’s Active Directory or two-factor authentication systems, such as RSA SecurID servers, as well as their own profile data bases.

**Secure Network Management:** Secure Network Management requires each network element to implement secure management interfaces requiring rigorous authentication/authorization, as well as both local logging and remote event notification regarding status, configuration changes and network security events. Secure access include SSH/SSL(HTTPS) for console access, SNMPv3, secure FTP, and Syslog remote logging.

**Video Surveillance Technologies and Physical Access:** Ideally, a building would have “six wall” physical barriers, but practically utilities need to use access control devices such as electronic card readers and video cameras and pixel-based systems, which focus on certain parts of the video frame and send an alert if movement is detected. PoE (Power over Ethernet), which can provide power to both access control devices and remote monitoring devices, makes digital video security and access control easier and less expensive to deploy than older analog-based systems. Other physical security measures include prohibiting unauthorized devices from being plugged into an Ethernet switch or router, or into a terminal server using technologies such as VLAN, static MAC security, and 802.1x (Ethernet port security), and static Serial-IP and filters, serial-port SSL and serial-port VLANs (serial-port security).

Introducing a number of simple security elements into a power utility substation and distribution network will significantly reduce the risk of physical or cyber attacks. The resulting network topology should look very much like this:

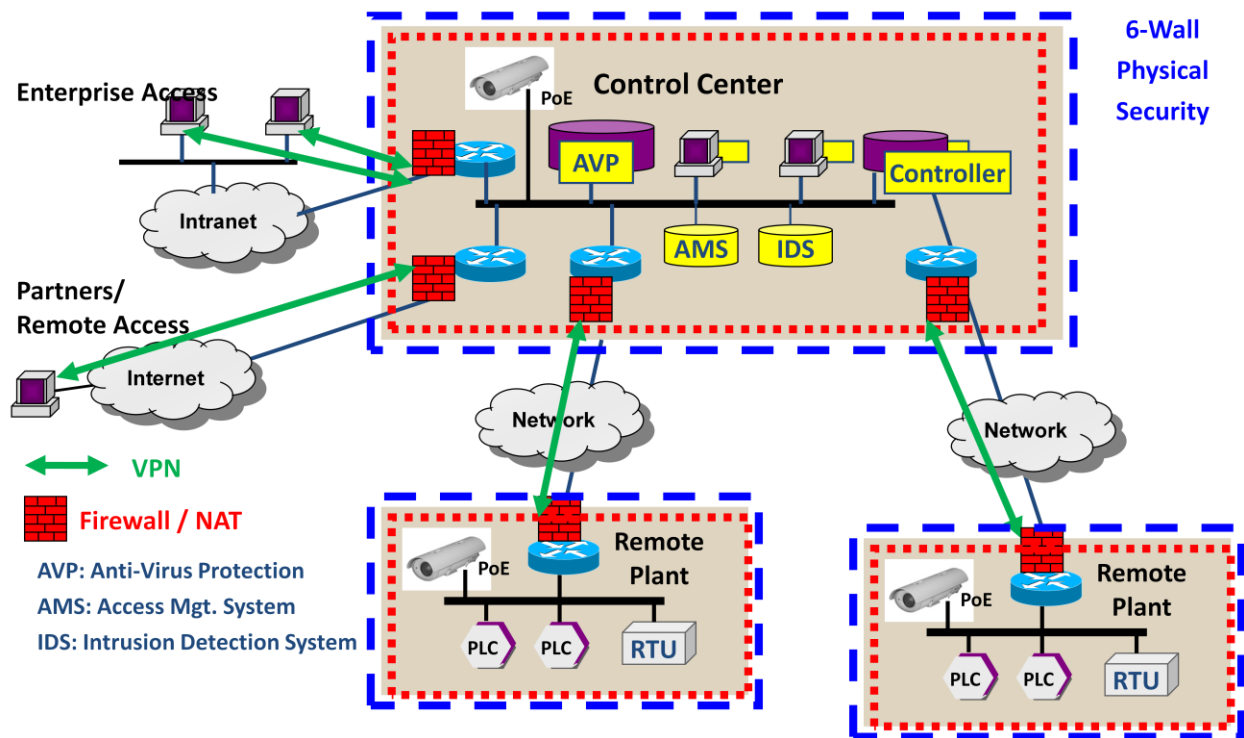


Figure 5

## **Application Example**

When Blue Ridge EMC wanted 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 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. Figure 4 shows the new substation and distribution layout that is a combination of Ethernet-connected IEDs and serial links.

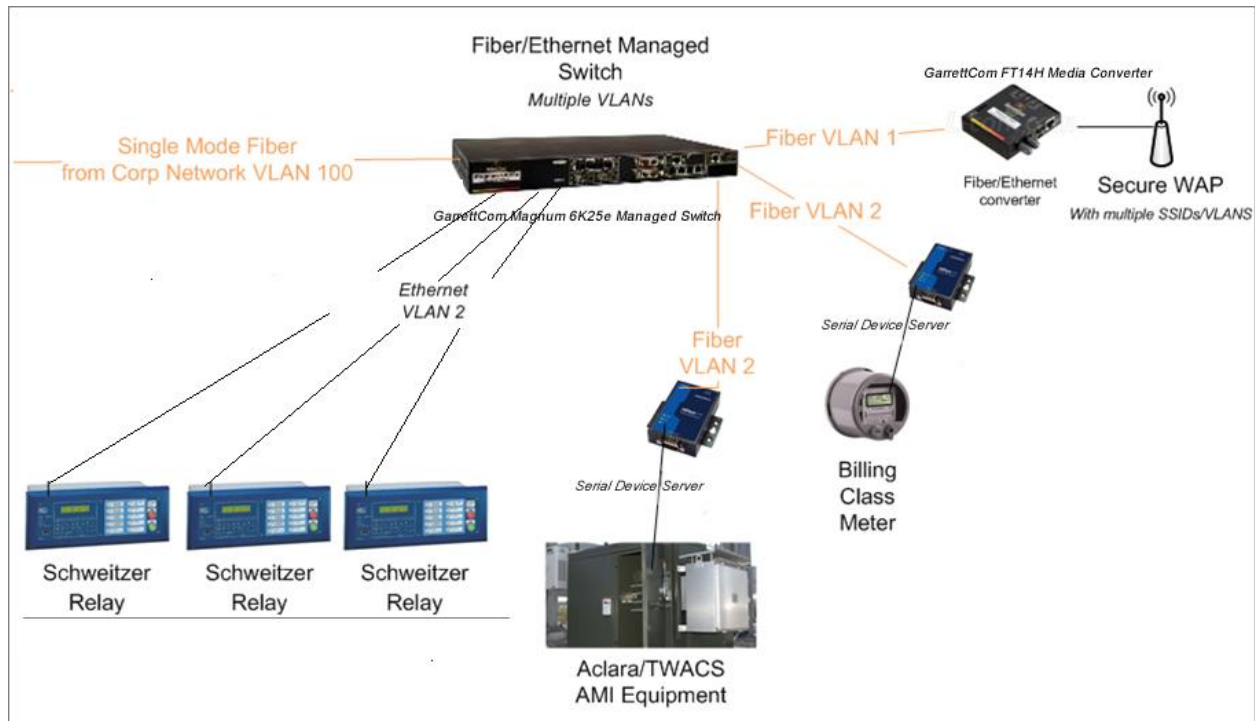


Figure 6

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

Smart Grid strategies require reliability, flexibility and security (both physical and cyber). In a time of evolving standards and government regulations, identifying equipment, software and protocols that can be adapted over time is important for providing cost-effective, long-lived, secure solutions. The Smart Grid uses technology that will continue to develop over time, providing cost savings for utilities and their customers alike. The best hardened solutions today are those that take advantage of the best network solutions available today and are designed to be flexible enough to evolve over time.

####

### About the Author

*Lee House is Executive Vice President and CTO at GarrettCom. Lee has more than 20 years experience in R&D and product development, with a focus on LANs, WANs, and IP at companies including 3Com, IBM, and Jetstream Communications. Recently, Lee spent five years as Vice President of Engineering at DiTech Networks where he led an engineering team to develop a new VoIP switch, Session Border Controller, and TDM voice processing platforms. Lee received both his Masters in Business Administration and his Masters in Electrical Engineering from Duke University. He also holds a BA from Rhodes College and a BSEE from Christian Brothers University. Contact him at lhouse@garrettcom.com*