



# Electric Energy T&D

## MAGAZINE

JANUARY-FEBRUARY 2007 Issue 1 • Volume 11



## Evolving to a Strategic Substation Network Architecture

By: John M. Shaw, EVP of GarrettCom, Inc.

Substation network planners are challenged to: integrate SCADA system connections, remote engineering access and other networking requirements for substations; do it now with minimal cost, and make sure the solution will evolve gracefully for many years across emerging requirements for scale, technology, security, performance, and manageability.

Planners must find the balance between near-term imperatives and longer-term vision. They may have a clear target architecture, but rarely do they get to put it into place all at once. In practice, the architecture unfolds one incremental project after another. To ensure an orderly network evolution, planners must shape each tactical deployment step to be consistent with a clearly defined set of strategic objectives.

### OVERARCHING SUBSTATION NETWORK DESIGN FACTORS

Among the many factors influencing network architecture, the four that are most prominent are:

- Network Integration

This involves consolidation of network connections onto a common infrastructure in order to reduce network costs, provide increased remote access to substation

devices, and facilitate implementation of additional substation automation applications.

- Cyber Security

Generically, this involves meeting best practices for managing the risk of cyber attacks on internal systems and grid operations. However, the current emphasis of cyber-security-related projects is on compliance with recent industry standards related to Critical Infrastructure Protection (CIP).

- Reliability

High network reliability is a growing concern as SCADA (Supervisory Control and Data Acquisition) and other operational systems play an increasingly critical role in grid operations. Also, as substations networks become more advanced and integrated, single network outages can affect a larger number of systems and control elements.

- Overall Cost Effectiveness

While the other strategic objectives all play a role in cost effectiveness, planners must manage not only initial costs, but also ongoing operations, telecommunications and maintenance expense, as well as longer-term life cycle costs such as premature network obsolescence due to feature or scalability limitations.

Effective planning requires both an integrated architectural vision that addresses these objectives, and a flexible set of tactical steps that allow projects to move incrementally forward on an opportunistic basis.

### NETWORK INTEGRATION

Ethernet and Internet Protocol (IP) have emerged as the unifying technologies for substation data networking. Both IEC 61850 and the related Utility Communications Architecture (UCA2) envision Ethernet as the universal connectivity medium for substation communications. The widespread adoption of Ethernet by vendors has driven down costs and provided a consistent technology across diverse systems. Ethernet provides the high-performance and prioritization features needed to combine multiple applications on a single network medium, as well as to support resilient topologies and software-controlled rerouting for network reliability. On a more end-to-end systems basis, Internet Protocol (IP) works over Ethernet to provide a flexible and widely accepted protocol framework for communications among intelligent devices and application servers.

As described below, Ethernet switches are available either in many stand-alone configurations or as components of hybrid, multi-function devices, giving planners

considerable flexibility to build out Ethernet-based infrastructure incrementally over time. The largest obstacle to Ethernet-based network integration is not Ethernet, per se, but rather the large number of existing non-Ethernet-based substation devices, including some newly deployed devices, since substation technology changes slowly. Also, planners must consider a still-evolving set of technology options for interconnecting substations and control centers

dedicated digital services. Many SCADA hosts that use Serial remote devices have short polling intervals; unless they receive a response from a remote IED in less than 100 milliseconds, they may assume a network problem. Some Serial-IP networks cannot consistently achieve this low latency. One element that affects network latency can be the protocol overhead of TCP/IP encapsulation. As shown in Figure 1, serial SCADA messages may be only a few bytes long,

and dedicated digital leased lines. IP/MPLS services should have greater bandwidth to help resolve most latency issues, but will still require traffic prioritization for critical applications. DiffServ, a specification for marking and treating IP packets such that all the routers in the network path can recognize and provide appropriate prioritization, must be used to prioritize critical data, such as SCADA, when utilizing MPLS services.

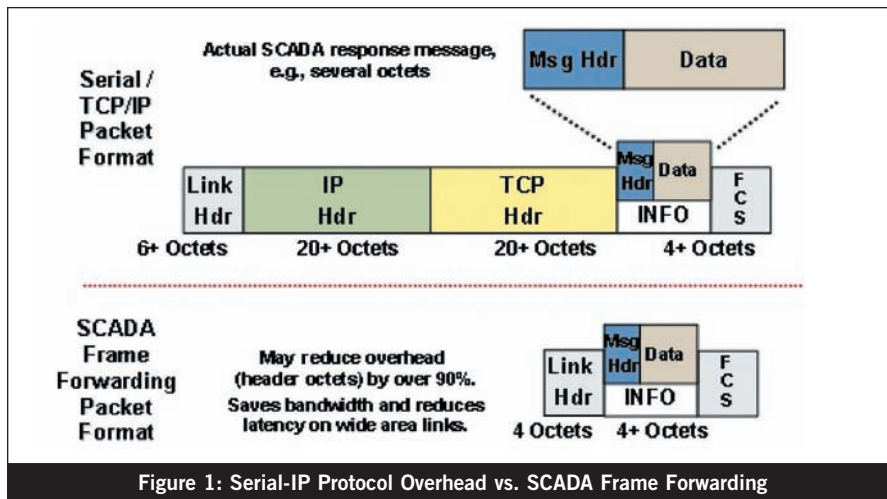


Figure 1: Serial-IP Protocol Overhead vs. SCADA Frame Forwarding

over Wide Area Networks (WANs).

Integration of serial protocol substation devices onto an Ethernet infrastructure is a major challenge. There are a number of devices called Terminal Servers, Serial Device Servers or Console Servers (all essentially the same thing). These devices encapsulate short serial data messages into TCP/IP packets (Transmission Control Protocol over IP) to send over Ethernet, and each serial stream is associated with a unique TCP/IP session. Terminal Servers may also be used at the host/master location to convert Serial-IP streams back to serial format. Alternatively, some master servers or remote PCs may interface directly to Serial-IP streams over IP/Ethernet connections. A newer generation of Serial-IP devices called Serial Device Routers may be deployed on a distributed basis in substations, creating a Dynamic Serial Edge for the substation network. This concept is described further in the context of security and reliability.

Performance over Wide Area Networks (WANs) can be an issue with Serial-IP network integration because of limited bandwidth, e.g., 56 kbps or fractional-T1 (less than 1.5 Mbps) frame relay or

but TCP/IP protocol headers increase the length of the Serial-IP packets by an order of magnitude. This can be remedied with a technique called SCADA Frame Forwarding that uses frame-relay-based encapsulation with only a few bytes of header to multiplex serial SCADA traffic on a WAN network. SCADA Frame Forwarding coexists on the WAN with IP-based traffic. SCADA Frame Forwarding includes fragmentation and prioritization features that, together with efficient traffic encapsulation, ensure that critical SCADA traffic has the high performance and preemptive prioritization needed to meet latency requirements.

It is important that WAN interface devices deployed in the near term, including those using SCADA Frame Forwarding, be compatible with longer-term WAN interface requirements for higher bandwidth and new protocols such as MPLS (Multi-Protocol Label Switching) and DiffServ. Over time, WANs will increasingly move to broadband speeds, whether using utilities' private fiber facilities or broadband services offered by carriers. Major carriers have introduced private IP services based on MPLS and have positioned these services to gradually displace other digital services such as frame relay

## CYBER SECURITY

The immediate drivers for implementation of cyber security measures in substations are the NERC Critical Infrastructure Protection standards, CIP-002 to CIP-009. These describe a number of new requirements for secure management of network devices that will now be factors in product selection. In terms of substation network architecture, the dominant concern, as defined in CIP-005, is creation of an Electronic Security Perimeter. In particular, this requires implementation of an IP-based firewall at the network boundary between the substation and the external WAN environment. The key roles of the firewall are filtering of IP addresses and TCP and UDP port numbers and forwarding traffic only for appropriate, authorized combinations of source and destination addresses/ports. The firewall function can be implemented as a stand-alone security appliance, but is usually integrated with an IP router at the boundary of a substation. For some utilities, CIP compliance will require deployment of a new network router/firewall device, but in other cases existing network routers will support an IP firewall as an incremental software feature.

Another key CIP requirement is port access security. This includes assuring that ports "nailed up" to IEDs are in fact associated only with those IEDs, and that inactive ports remain inactive. Port access security also requires rigorous access authentication and authorization schemes for ports associated with intermittent, on-demand applications (e.g., console ports shared by various remote engineers and administrators). While initially only a few ports on a few devices may be involved, over time reliability, efficiency and scalability strategies will require more ports, more devices and wider distribution of the devices within the substation. These requirements call for a consistent, structured approach to port security.

Ethernet port security should involve three main technologies. VLANs (802.1Q Virtual LANs) provide closed communities of interest among Ethernet ports, even distributed over several switches. MAC-level port security enables Ethernet switches to learn a unique MAC address for a specific IED that is nailed up to an Ethernet port; other devices that might be attached to the port are blocked. The 802.11x Ethernet port security is best for more intermittent access; it intercepts new connections to Ethernet ports and works with central authentication servers such as RADIUS or TACACS+ to authorize newly attached users or devices. An important planning consideration is that advanced port security requires managed Ethernet switches. Historically, Ethernet architectures have often used managed switches for core switching, with simpler unmanaged devices for media extension and access aggregation around the edge of the network. Advanced port security features will push managed switch technologies further out toward the edge of the substation.

For Serial-IP-based port security, as with nailed up Ethernet ports, static IED connections can have static Serial-IP network definitions; however, remote console access is intermittent and on demand and it requires greater access control. The perimeter firewall and centralized access management systems will generally provide port access security for initial CIP compliance; however, planners should look for incremental opportunities to deploy Serial-IP technology close to – and eventually adjacent to – serial IEDs and then provide port- and user-specific authentication via security protocols optimized for serial-console applications, such as Secure Socket Layer (SSL). Serial Device Routers incorporate SSL technology and can be used to extend dynamic Serial port security across a harsh substation environment.

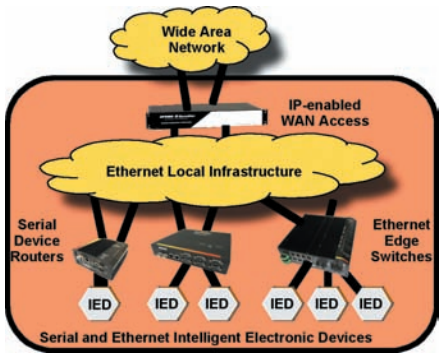
**RELIABILITY**

Network reliability has three major factors: device reliability, media protection and resilient networking.

Device reliability can be addressed as part of every product selection. Within the substation environment, conformance to substation equipment standards IEEE 1613 and IEC 61850-3 is an important indicator that the equipment is built for survivability and extended

Mean Time Between Failure (MTBF) in utility applications. These specifications address surge withstand, immunity and operating temperature range, among other factors.

Media protection means that all cabling connections other than very short runs within control house environments should use fiber optics rather than metallic media. Fiber optics provide both signal immunity and surge protection for attached devices. Most substation networks already use serial-over-fiber-optic Links/repeaters and optical stars for serial connectivity, and media converters when required for Ethernet connections, usually on point-to-point bases from the control house to distributed substation devices.



**Figure 2: Resilient Connectivity of Distributed Devices to Ethernet Core Infrastructure**

As substations evolve to an Ethernet core infrastructure, there is more opportunity to increase the resiliency of fiber network connectivity by adding dual-homing or ring topologies when linking to distributed devices. For Ethernet IEDs, there are a range of compact Ethernet switches, both managed and unmanaged, that can be distributed close to remote devices. These can support two connections back to the core network and can control network traffic rerouting with resilient software such as Rapid Spanning Tree Protocol (RSTP).

For serial-protocol IEDs, there are also recently available devices, sometimes called Serial Device Routers, that are hardened for distributed placement next to serial-based substation devices, with Serial-IP services and dual fiber-optic Ethernet connections to the core infrastructure. These devices have intelligent

software to provide protection switching on both a local Ethernet basis (RSTP) and also for end-to-end network connectivity to remote master systems using dynamic IP routing and multi-master network features of advanced Serial-IP networking.

**OVERALL COST EFFECTIVENESS.**

Substation network planners are expected to keep project-specific costs down, but this does not always translate to purchasing the least expensive device(s) for the task at hand. Total costs are also a function of ongoing maintenance, operational and telecommunications carrier expenses, as well as life cycle costs that are dramatically affected by early product obsolescence due to missing features or an inability to scale. For cost management it is important to minimize the number of discrete devices and suppliers required, and to have flexible growth options, both in terms of the number of ports and the physical distribution of connection points throughout a substation. Ultimately, the substation network should evolve with logical phases of incremental deployment.

In the largest substations, a near term design may utilize discrete networking products for WAN access, cyber security firewall functions, local Ethernet switching and Serial-IP services; in fact multiple distributed Ethernet switches and Serial-IP servers may be used. However, for initial integration projects at most small, medium and even moderately large substations, it may be more economical to utilize integrated multi-function network products. There are substation-hardened “routers” that combine all or many of the functions needed for substation network integration in a single unit, effectively providing a “one box solution” for network deployment. These may be deployed with only a few total ports or a few dozen, with a mix of Ethernet, serial and WAN connectivity.

Use of an integrated networking product should be viewed as only the first step in the evolution of the substation network. In the longer term, this key element can play a primary role as router/firewall at the WAN boundary, establishing the cyber security electronic perimeter. A likely second phase of deployment would be to add local Ethernet switches connected to this router to support growth of Ethernet-based IEDs and other Ethernet-based applications such as

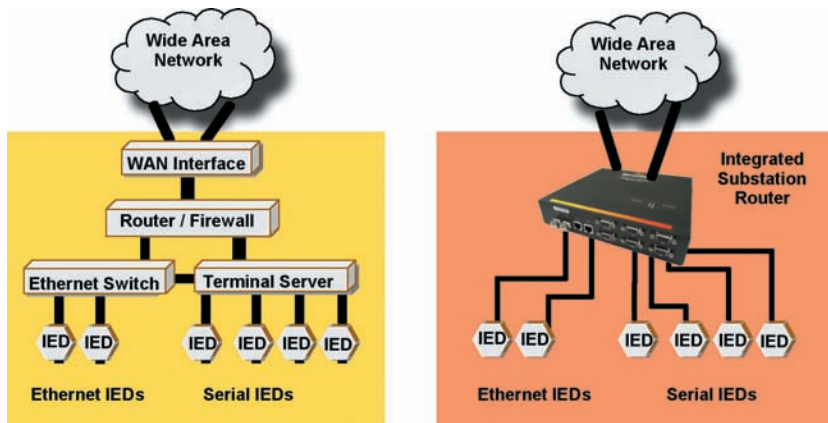


Figure 3: Functions of Substation Network Devices Available as Hybrid, Integrated Products

surveillance cameras. These Ethernet switches would also create a core infrastructure for supporting deployment of a more dynamic edge network. A third phase of network evolution would be the establishment of a dynamic edge network for connectivity to both Ethernet and serial devices. Managed Ethernet switches and Serial Device Routers can be gradually deployed further out into the substation network using dual or ring connections to the core Ethernet network. This architecture, employing both Dynamic Ethernet Edge and Dynamic Serial Edge technology, moves port security functions out adjacent to critical devices and extends network resiliency features locally throughout the substation. With compact devices, distributed device placement and a shared core infrastructure, the dynamic edge approach enables integrated substation networks to expand on a flexible, incremental and cost effective basis.

#### CONCLUSION

Many planners view an all Ethernet and IP network as the strategic target architecture, but few have an opportunity to implement and take full advantage of its strengths in a single-phased network deployment. It is important to under-

stand the primary design objectives driving this universal architecture and then look for opportunities to move forward in each area progressively. Network consolidation, security, increased reliability and managed life-cycle costs can all be achieved with an evolutionary deployment approach. A responsible plan starts with a central integrating router/firewall network element, adds core Ethernet switches for scaling and provide a core infrastructure. The plan gradually pushes resilient and secure Ethernet-based Serial-IP and managed Ethernet switching elements throughout the substation as a reliable and secure distributed infrastructure. ■

#### About the Author

John M. Shaw is EVP of GarrettCom, Inc., a leading supplier of substation-hardened networking products. He has more than 25 years experience in telecommunications including executive roles at network technology start-ups and large carrier-equipment suppliers. As Director of data services at NYNEX (Verizon) he pioneered frame relay and fiber-based data services. He has extensive early career experience with design and implementation of large-scale utility-grade data networks. Contact him at [jshaw@garrettcom.com](mailto:jshaw@garrettcom.com)



#### Corporate Headquarters-USA

GarrettCom, Inc  
47823 Westinghouse Drive  
Fremont, CA 94539  
USA  
Tel: (510) 438-9071  
Fax: (510) 438-9072  
Email: [mktg@garrettcom.com](mailto:mktg@garrettcom.com)  
Web Site: [www.GarrettCom.com](http://www.GarrettCom.com)

#### GarrettCom Utility Networks

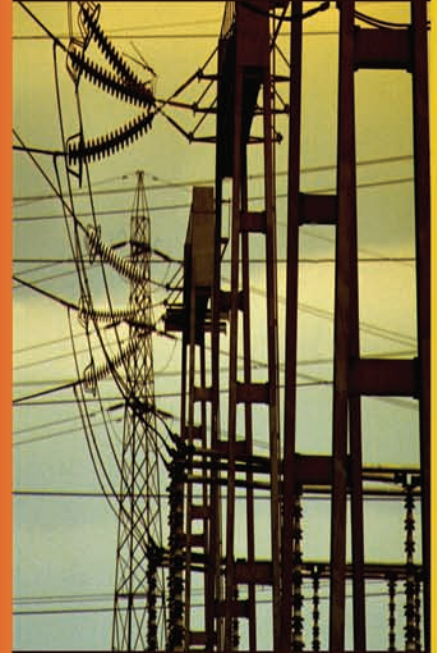
25 Commerce Way  
North Andover, MA 01845  
Tel: (978) 688-8807  
Fax: (978) 688-8771  
Web Site: [www.garrettcomutilitynetworks.com](http://www.garrettcomutilitynetworks.com)

#### Europe

GarrettCom Europe  
Haslar Marine Technology Park  
Haslar Rd, Gosport, Hants PO12 2AU  
United Kingdom  
Tel: +44 (0) 870 3825 777  
Fax: +44 (0) 870 3825 098  
Email: [mktg@garrettcom.co.uk](mailto:mktg@garrettcom.co.uk)  
Web Site: [www.GarrettCom.co.uk](http://www.GarrettCom.co.uk)

# Substation Networking Your Way

- »»» Hardened
- »»» Secure
- »»» Reliable



- »»» 61850 Compliant
- »»» Integrated LAN, Serial and WAN
- »»» Configurable Fiber
- »»» Advanced Security

Ask the experts!



## GarrettCom™

Industrial Networking at Its Best™

For more information contact  
510.438.9071  
[www.GarrettCom.com](http://www.GarrettCom.com)



DYMEC DynaStar Magnum