

INTEGRATED SUBSTATION NETWORK ARCHITECTURES

IEC 61850: THE KEY DRIVING FORCE FOR INTEGRATION

*(presented at the PowerGrid Europe Conference June 26, 2007 Track 2: 61850
<http://pgrid07.events.pennnet.com/fl/content.cfm?Navid=5902&Language=Engl>)*

From the first time a protection and control group needed to assign IP addresses to IEDs and discussed accessing devices through the substation's IP network, a fundamental change occurred, and Utility IT and Utility Operations discovered that there really couldn't be a wall between the two groups for much longer.

Substation automation has been evolving for decades. Ethernet at the network core is growing in acceptance, displacing older telecom technology for connecting to RTUs and IEDs. Shortly before the year 2000, companies such as ABB, GE, Siemens, AREVA and SEL had or were developing the capability to use fiber cables for proprietary protection functions. Ethernet-ready devices have come onto the market rapidly, often outpacing the ability of existing substation communications infrastructure, which is still evolving toward a high speed network paradigm.

Today's IED technology has changed expectations and requirements for data access and management within the substation. Driven in large measure by advancements in processor power, field IEDs now provide more -- and more complex -- data (waveforms, harmonic analysis, video). In turn, this data is used in more complex ways at the local and peer level in communication and logic such as current differential protection, remedial switching or throw-over schemes. Similarly, at the control and client end of the network, applications such as GIS, outage management, energy management systems or SCADA, and asset management and maintenance are more sophisticated. They require more real time operational and non-operational data presented in more sophisticated ways to more clients in real time. It is no wonder that IEC 61850 is needed to get the job done today! Greater dependence on more complex data requires better management of the data and the network itself -- from optimizing bandwidth demands, such as IP video routing, to supporting security requirements for access logs, password and application management.

Utility infrastructure in industrialized nations has long been designed under the assumption that trust and goodwill were appropriate armor. Global terrorist and security threats, coupled with vulnerability to theft of valued substation components made of steel or copper has changed how infrastructure assets are viewed, managed and protected. There is an urgent need to address a power infrastructure that appears frighteningly vulnerable. Project engineers attempting to deploy an ideal long term network infrastructure will be faced with a spectrum of challenges from projects that are part of well developed existing infrastructure expansion/retrofit, to large scale projects typical of developing nations. The pressure is on for engineers to meet current project requirements most expediently, yet keep an eye on future capabilities and needs. In the best of circumstances, each step taken in design and deployment of a substation network

infrastructure project can become a technological and economic enabler to projects that follow, while meeting company and regulatory objectives.

As utility engineers, managers and planners are well aware, there are many forces driving deployment of automation technologies at substations. Among these are: existing and emerging standards, regulations and threats; operational efficiency via improved asset management; system reliability; and overall capacity expansion. A well planned network strategy will take advantage of the superior bandwidth and management features of Ethernet as a core technology and, at the same time, seamlessly integrate serial IEDs and WAN protocols into the overall communications structure - minimizing stranded assets in the substation and providing a seamless migration path to an integrated substation.

For Greenfield projects, the optimal strategy is to incorporate best-in-class products that use standards-based technology to ensure interoperability and efficient management. With 61850-compliant Ethernet as a key architecture in current and future substation data networks, designers will be able to take advantage of newer highly integrated devices that extend network management capability and cyber security to both serial and Ethernet components in the substation network.

THE POWER OF STANDARDS

Power utility substations are a critical lynchpin for industrial societies. Communications components must be integrated into an overarching plan that addresses the entire range of substation automation systems – protection, operation, real world clocks, compliance and other systems. Standards for the utility industry evolve at local, regional, national and international levels. At the national level, in the US we see NERC/CIP regulations strongly influencing power utility planning, and IEC 61850 is recognized as the most widely accepted international standard for substation automation systems and networks.

IEC TC57, which encompasses IEC 61850 and other standards, addresses the need to manage both the power system infrastructure and the information management infrastructure. IEC 61850, among other things, defines the communication between devices in the substation and the related system requirements, and Ethernet is a key component in its design. It is designed to be flexible and future-proof.

IEC 61850 allows the “clients” of substations to have access to relevant operational and non-operational data, through sophisticated data management and use of secure network practices. The benefits to utilities include better efficiencies and a roadmap to guide a rapidly automating industry.

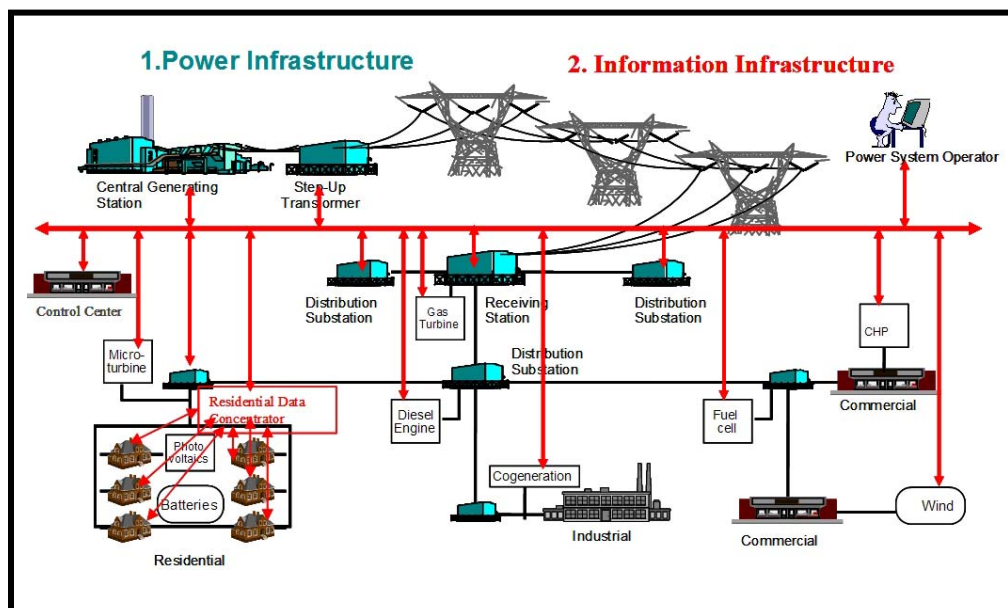
Over the last 10 years, the industry has seen engineers and technicians emerge that have “grown up” in the information age. Workforce acceptance of computer-based tools is growing. As industry privatization and consolidation occurs, older regulated business models give way to more automation and leaner staffing with changing skill requirements – fewer people working with more sophisticated data to make decisions that have larger scale impact. Automation is changing the structure and core functions of whole organizations as business leaders embrace

and leverage technology in new ways. Developing nations are demonstrating this dramatic change as they leap ahead of more traditional industrialization paths with state-of-the-art, best-in-class technologies and new infrastructure, unburdened by previous generations of technology.

A GLOSSARY OF STANDARDS

In many ways, IEC 61850 is becoming the glue for other substation communication and data security standards. Associations and partners such as IEC, IEEE, KEMA, CIGRE and EPRI play a key role in defining and managing standards. The universal goal is to have a standardized set of policies, procedures, interfaces, and other components of automation to allow for highest efficiencies, safety, and interoperability. For example, the Utility Communications Architecture (UCA), which was developed under the sponsorship of the Electric Power Research Institute (EPRI) through a process of broad industry involvement, was designed to allow for seamless integration across the utility enterprise using off-the-shelf international standards to reduce costs. Later, EPRI initiated a project to develop a database of enumerated UCA™ data objects (called GOMSFE - Generic Object Model for Substation and Feeder Equipment) for the Utility Initiative, which is actively developing and refining the data object specifications. GOMSFE was then integrated into IEC 61850. It is heartening that the working groups of various standards organizations often consist of a number of overlapping members that can ensure that there is consistency and coherency among the different components.

It is useful to review EPRI's IntelliGrid Project (previously known as the IECSA Project). The project's objectives were to identify current and future power system functions to determine the business direction for the industry, including self-healing grid concepts, and to develop an IntelliGrid Architecture to support the needs of envisioned power system of the future. The diagram below shows the tight meshing of both the power infrastructure (protection, SCADA, EMS, RTO, DER) and the information infrastructure (security, network and data management) that resulted.



Source: EPRI

North America has recently seen national legislation in the form of NERC/CIP rules. In the EU the drivers appear to be mainly through utility and manufacturer participation with IEC TC57 and related workgroups 3, 7, 9, 10 and 13-19; CIGRE Study Committee B3 for Substations, in particular working groups 1 and 6; and additional related organizations such as the IEC 61850 Users Group, UCA International Users Group, CIM Users Group, and others. We can expect these standards will continue to evolve to meet current and future challenges and opportunities, and will tend towards open, globally-accepted criteria for design and implementation. With this in mind, how does one plan for the future given the dynamic nature of the industry. How does one implement with confidence today?

UPGRADE PLANNING – OPPORTUNITIES AND RISKS

Common mistakes in network planning include missing still-emergent product and standards requirements, having too narrow a technology focus, introducing too many vendors with no clear strategy for management and interoperability, and making short-sighted tactical compromises on requirements.

Missing future features: Keeping up with the various standards, set forth by individual utilities, IEC, IEEE, as well as surveying all the relevant groups and agencies, could indeed be a full time job. Planners need to scan technology developments with the help of trusted peers and suppliers and project likely future requirements onto current product decisions.

For example, with cyber security, there is a danger of paralysis. The emphasis on planning and “compliance” with industry standards is strong right now – but complete clarity on requirements is still missing. In the US, the recent NERC Critical Infrastructure Protection cyber security standards for substations (CIP-002 to CIP-009) present a foundation, but these requirements will surely evolve over time and become increasingly sophisticated. Similarly, TC57 workgroups are publishing and revising 61850, 62351-1 through -7, defining Data and Communication Security for TCP-IP, MMS, DNP 3.0 and peer to peer profiles (GOOSE, GSSE, and SMV).

Narrow focus: Within the framework of standards, technology domains need to be viewed in the context of a single holistic architecture, or problems will arise. For example, some plans correctly identify Ethernet switching as the clear winner for long term core substation infrastructure from both a technology and standards base, but if those plans do not integrate the world of non-Ethernet protocols and technologies (e.g., serial-based IED interfaces, cyber security and carrier-based Wide Area Network or WAN services) in planning decisions, walls can arise between these worlds and reduce system flexibility and create duplicate costs.

Too many vendors: Different project champions often find point solutions that appear to be the most expedient solution to their particular short-term needs. But the overall plan must include some guidelines; introducing too many vendors into a network environment creates issues, even with open standards, and interoperability, can result in indirect costs, such as higher training and administration costs. In addition, there is more potential for interoperability problems as advanced protocols are introduced, and approaches to critical issues such as network resiliency can become less consistent. .

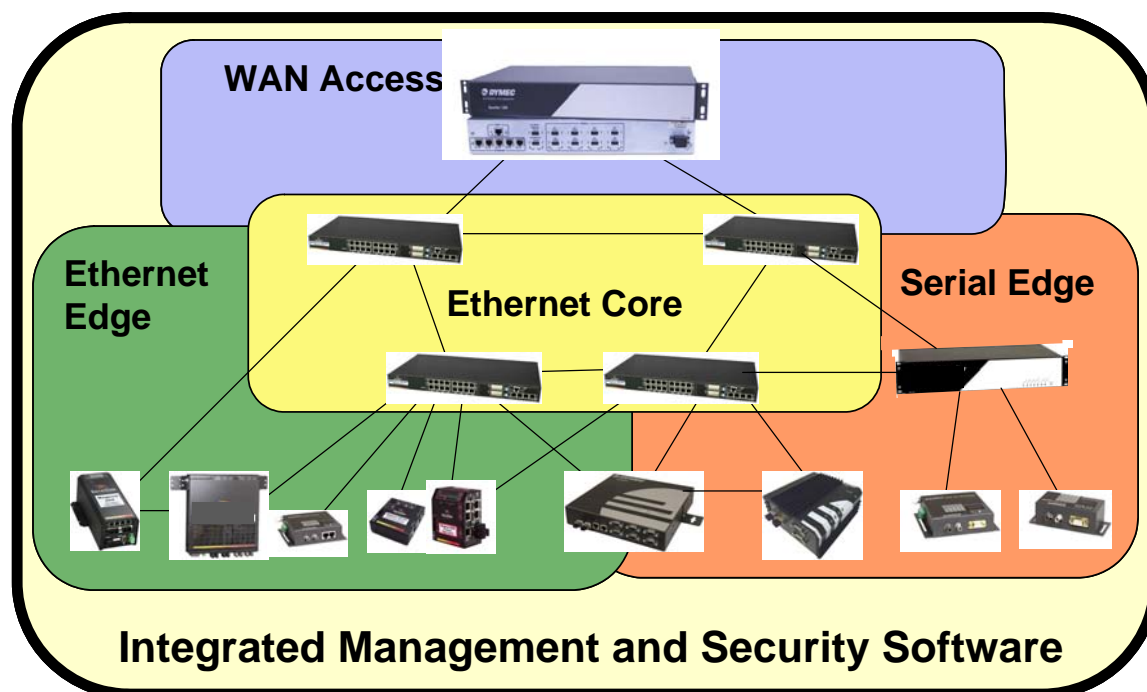
Lowered standards: Narrow, project-specific product decisions may also lead to dropping standards for product performance. A particular issue is ignoring environmental hardening requirements specific to substations. Attempting to adapt office-grade products to hostile environments may lead to quicker, lower cost implementations, but equally, the practice may lead to shorter-lived, less reliable investments that future planners will need to replace.

KEY PRINCIPLES FOR FUTURE SUCCESS

There are a few key techniques can help substation networks evolve effectively. First is a comprehensive architectural vision that builds upon standards such as IEC 61850. Second is a strategic requirements forecast that looks into the future to anticipate feature requirements. Third, an analysis of Total Cost of Ownership can help drive decisions towards long asset life and low operational cost. For example, network topology choices within a large substation, and from substation to substation, can impact redundancy, speed of recovery, number of switches required and the level of complexity required in the software configuration and management of those data networks.

Strategic Architecture

The most fundamental requirement is to define a clear and comprehensive long term architectural vision for the substation network. Ethernet technology belongs at the core of this architecture. This is consistent with dominant technology trends and is recognized by IEC 61850, 62351 and UCA architectures. Most utilities have already begun the deployment of Ethernet switching as the basis for new systems in larger substations, in turn leveraging high speed gigabit backbone or SONET ring type infrastructure over a region. With extremely wide adoption, Ethernet has become a low-cost physical media, universally accepted across IT systems suppliers. In substation environments, it provides enormous data network capacity, plus advantages in flexibility with fiber and copper connectivity. In larger substations, the Ethernet core requires multi-Gigabit capacity switches with growth capacity for video, high-volume file transfers and high-priority process control traffic.



An effective industrial network architecture will include several elements surrounding an Ethernet Core, including the Ethernet Edge (the fringes of the network where Ethernet connectivity may be required), the Serial Edge (“legacy” devices), and WAN access – all of which are inter-related, inter-operable and integrated with network-wide approaches to network resiliency and network security.

A Strategic Substation Network Architecture

The Ethernet edge network extends fiber media effectively throughout a substation and connects Ethernet-based IEDs back to the core network. The most basic edge network is point-to-point links with fiber-copper media conversion units. Many substations now have hierarchical edge networks using multi-port Ethernet collector switches. These come in a variety of compact form factors and can be effectively panel-mounted throughout a substation. Ideally these distribution points have dual-homed fiber connectivity to the core network, now selectively available in both managed and unmanaged switches. While collector switches may be unmanaged devices today, increasingly the Ethernet edge will use compact managed switches that provide additional resiliency, access security and network event monitoring capabilities throughout a distributed substation network.

A similar transition is underway at substations for connecting serial IEDs. At present, many serial edge connections use static serial-over-fiber link/repeaters to extend IED connections from centralized data communications processors or terminal servers. In the case of some widely deployed SCADA protocols, the associated systems are not readily integrated with an Ethernet-based core architecture and require special handling on wide area network connections back to SCADA masters. But for full-time or occasional-use access to serial-based IED administrative ports and for many serial SCADA protocols (e.g., 62351-5, 60870-5 serial DNP3), Serial-to-TCP/IP protocol converters (often called device servers or terminal servers) are often placed at centralized substation hubs to provide integration with the IP/Ethernet core infrastructure. As with the Ethernet edge, this device/terminal server function will increasingly be distributed using compact devices deployed throughout a large substation. This more dynamic serial edge network will provide dual fiber connectivity and resilient networking features and extend security (e.g., SSH/SSL) to the connection point of remote serial IEDs. In some cases, multi-purpose devices will provide both serial and Ethernet edge connectivity.

Finally, the substation must be connected to the outside world, often to redundant remote control centers via WANs. Many substations are still making the transition from per-application dedicated leased lines or dial up connections to integrated WANs across all substation systems. The demands placed on WAN access are rapidly changing. For example, to integrate SCADA with other applications, WAN access must be able to effectively prioritize application traffic, giving SCADA preferred treatment. As discussed below, WAN service options from carriers are continually evolving and access devices should be flexible enough to support multiple options. Also, the WAN Access layer increasingly must play the role of Electronic Security Perimeter for

substation cyber security. WAN access solutions must meet these varied external requirements while effectively integrating with Ethernet core and serial edge architectures.

While not every substation automation project will impact all elements of the substation architecture, it is important to fit any incremental element into the larger picture. There should be no architectural barriers created that will inhibit utilizing a more comprehensive network design in the future.

Strategic Features Forecasting

In setting requirements for near-term projects, planners need to also look towards a longer planning horizon for new requirements that will likely emerge for this project or for future projects in the same substation environment.

The physical layer considerations include higher level topology: the linear nature of high voltage transmission systems with data rich “clumps” such as generation tie ins, switchyards and major substations, versus the meshed or ring topology for distribution networks, above or below ground. Each topology has different inherent strengths and weaknesses from a data network perspective. The physical architecture and the logical (data flow) architecture, must be designed so that the system retains N+1 robustness, at the asset level (switchyards, throwover schemes); the device level (IEC 61850 uses the term “graceful degradation”); and the network level (network, device and port level redundancy options).

Increasingly intelligent devices are enabling increased performance and reliability, while physical characteristics such as lead-free circuit boards, packaging and component hardening to withstand extreme temperature, and conformal coatings for dirty, damp or corrosive environments are being specified to ensure long-lived device performance.

One clear area of concern globally is cyber security. In North America for example, most of the cyber security attention is focused on the recently approved NERC CIP (Critical Infrastructure Protection) standards, and for the purposes of substation data network infrastructure, most particularly on CIP-005 Electronic Perimeter Security and CIP-007, Systems Security, but, these standards are only a baseline. Most strategic planners can already project additional requirements that will emerge. For the European Union, IEC TC57 will likely continue as a central focus for many countries, but what potential individual country or EU-wide mandates may become a factor? In the case of the North America, NERC may act on its own, or be influenced by initiatives sponsored by DOE (Department of Energy), DHS (Department of Homeland Security) or other Federal mandates. Even industry best practices will continue to evolve. For the planner, this means a high likelihood of additional requirements or more stringent definitions of requirements already proposed.

Additional security features that are not yet specific requirements, but are recognized as best practices include SSH for serial (e.g., CLI) console access, SSL/HTTPS for access to web-based management interfaces and SNMPv3 security for system-level management applications. Other

“futures” that should be taken into account include Virtual Private Networks with IPsec, strong data encryption such as AES, and Intrusion Detection Systems (IDS) in substations, which are now mostly limited to control centers.

Changes in carrier WAN service offerings are another area where technology trends need to be taken into account. As an example, Frame Relay remains a popular and extremely effective service technology for connecting distributed substations to control centers, supporting resilient connectivity and providing rigorous traffic prioritization. However, virtual private IP network services based on Multi-Protocol Label Switching (MPLS) are being positioned by major carriers as strategic replacements for Frame Relay, as well as for dedicated leased analog or digital circuits.

From the European Union perspective, TC57, WG 15 is looking specifically at security relative to 61850, 60870, and 62351. With WG 15 and others, 61850 encompasses the spectrum of requirements including perimeter security, device security, application security and management security. Details on security issues are referenced in several more detailed published papers referenced by this paper. One example of a more critical security requirement for substation networking is denial of service, whether that is link layer denial or association denial (locking up resources). In both of these cases, network monitoring looks for application associations with the capability to reclaim the connection or resource upon expiration of the timeout. These functions and others must be inherent in both the network management equipment and software.

Planners can never see all possibilities nor can they afford to cover all contingencies, but it is important to probe suppliers about their own awareness of industry trends and their current and planned accommodation of foreseeable future requirements.

Total Cost of Ownership

The keys to optimizing Total Cost of Ownership (TCO) are to build for a long-lived installation and to factor in both immediate equipment costs and longer-term costs of maintenance, replacement and ongoing systems integration.

A basic consideration for substation project longevity is network product hardening. IEC 61850-3 and IEEE 1613 standards define equipment requirements that increase product reliability in harsh substation environments. This requires high levels of protection for both power input and I/O interfaces against surges, fast transients and other electromagnetic events common in substations, as well as component and system hardening against extended high and low temperature ranges (-40 to +85° C). Many “industrial-hardened” products claim some heightened electrical immunity relative to basic commercial grade products, but “substation” standards are considerably more stringent. Also, while some products can tolerate short term exposure to harsh environmental factors such as high temperatures, sustained high temperatures above product ratings significantly diminish long-term product failure rates (MTBF). Planners should look at both third party “type test” results and more extensive product MTBF analysis before depending upon products in substation settings.

The number of different vendors introduced into a substation network environment significantly impacts TCO through increased maintenance costs, training costs, and vendor administration costs. Having too many vendors sacrifices “economies of scale” in all aspects of vendor interaction. Perhaps most importantly, with multiple vendors, there is no focused responsibility for interoperability and systems level integration. A role of a network architecture is to identify key standards for interoperability among network elements and make this set of technology standards (e.g. RSTP, VLAN, SNMP, SSH) part of the baseline that all products must meet. In the end, nothing helps to prevent or resolve interoperability questions better than the handy “one neck to grab.” Suppliers who can provide all or most of the design elements needed both now and to complete the long term network vision add value far above the sum of their product parts.

LOOKING AHEAD

There is a responsibility for IT divisions and operation divisions to work more closely together than ever before. Manufacturers and suppliers of products and solutions must also take the initiative to participate in the standards process, inform and be informed of technologies, requirements, and mandates or legislation intended for the public good. As technology and complexity grow, security and reliability must be actively managed to ensure they will remain complementary. There is reason to be optimistic, even with significant challenges in the industry - from security concerns to workforce dynamics and technology change. Technology and capabilities exist today to solve these problems, and will continue to improve and enable engineers and managers to adapt and take advantage of new opportunities – whether that is demand management and real time pricing at the consumer level, requiring new “last mile” connectivity, additional distributed generation requiring tie ins to regional control centers, or mandates for higher levels of security including Video and Voice over IP.

Charles E. (Ted) Witham, PE, MBA, director of International Business Development at GarrettCom, Inc., has 20 years experience in industrial measurement and control, with 15 years of specialization in power industry generation, transmission and distribution. In addition to GarrettCom, Witham has held technical and sales positions with companies including General Electric Company, Honeywell Industrial Automation and Control. He was licensed as a Professional Engineer in Control Systems in 1995 and is a member of BICSI, the National Society of Professional Engineers, Instrumentation Society of America and IEEE.