GarrettCom®
A BELDEN BRAND

Nine Steps to Building a Smart Grid Ready Substation

By Jim Krachenfels, Marketing Programs Manager, Belden Inc.

Table of Conents

Introduction

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. The results are innovative ways to integrate the new and the old in order to position themselves for the future. The substation is at the heart of this change.

IP—the Game-changing Factor Enabling Smart Grid

IP has been the game-changing technology that is the basis for three compelling benefits for power utilities—particularly in the area of substation automation

- an overall reduction of operations expense due to an IP-based infrastructure that can integrate 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, the following nine steps allow substation engineers to develop a future-proof plan for substation communications.

1. Install cabling and systems capable of scaling bandwidth to handle the steadily increasing demand for data
2. Take advantage of heavy-duty substation-hardened switches and routers to support expanding demands for more Ethernet ports
3. Use wireless communications for simple, cost-effective data links to remote sites where wired solutions are impractical
4. Migrate to an Ethernet-based system at a pace that works for the utility by integrating existing serial equipment into the IP network – serial is not going away any time soon
5. Choose Ethernet products with flexible port configurations to easily integrate various types of new and existing equipment
6. Specify communications equipment with precision timing features to enable synchronized data management and control actions
7. Comply with NERC CIP regulations by integrating both cyber and physical security strategies 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

In the wake of 9/11 and the advent of malware attacks such as StuxNet and Flame and Advanced APTs (advanced persistent threats) such as Night Dragon, concerns about cyber security have increased. A combination of smart grid initiatives, which drive two-way communication all the way to the customer site to encourage the smart use of power, and concerns over cyber defense have unleashed 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, as well as out to the end user's meter and on to the central office, is high. 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 was the first international standard to outline 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.

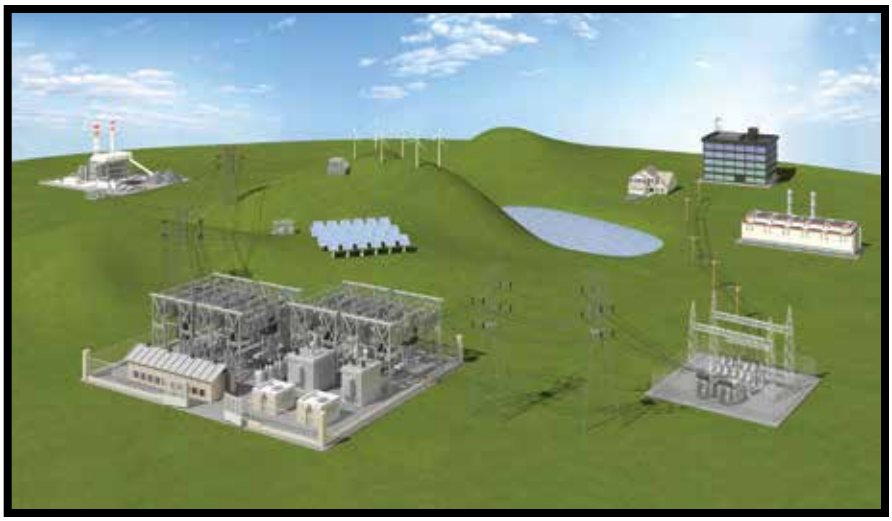

Figure1: Smart grid encourages distributed, two-way communication between the power sources and the users.

Smart Grid—Increased Complexity

With the advent of smart grid strategies, a relatively simple operation became more complex. Two-way communication and multiple stakeholders replaced the 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 grew dramatically. Because communications extended far beyond the boundaries of a single facility, issues including timing and security had to be addressed at a much more comprehensive level.

The Basics: Bandwidth, Capacity and Hardening

It should be clear from the description of the smart grid that additional bandwidth is necessary to successfully implement any 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 (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 steep 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. Today's substation network (Fig. 2) must accommodate the increasing number of intelligent IP-enabled devices available for connection, as well as support serial connectivity. Intelligent IP today ranges 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.

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 join multiple low-port-count switches together, wasting two ports per device for connectivity. This practice also results in additional and unnecessary points of failure, which is an unwelcome addition to substation infrastructure. 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 in place of fans to protect against dirt and dust as well as eliminate a potential point of failure
- 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

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.

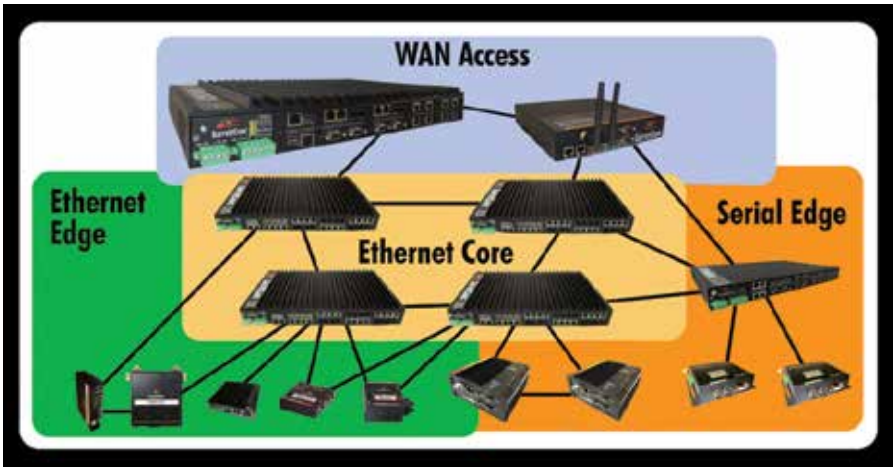

Figure 2: A network-centric view of a substation

At the other end of the spectrum, serial equipment is here for the long run. In power utilities, much of 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).

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.

Time after Time—The Precision Problem

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. Other solutions include GPS and 1PPS. The GPS (Global Positioning Satellite) can be used for direct time synchronization or as a time source for other time protocols, and requires either an antenna for each IED or a switch. The acronym 1PPS stands for "one pulse per second" and is a high-precision time pulse from precision clocks. Because 1PPS is sent to every user over a separate line, it poses a complex wiring challenge.

Another timing option is IEEE 1588 PTP (Precision Time Protocol). This is a standard Ethernet protocol that is a cost-efficient solution that can be applied to an existing Ethernet network in a substation.

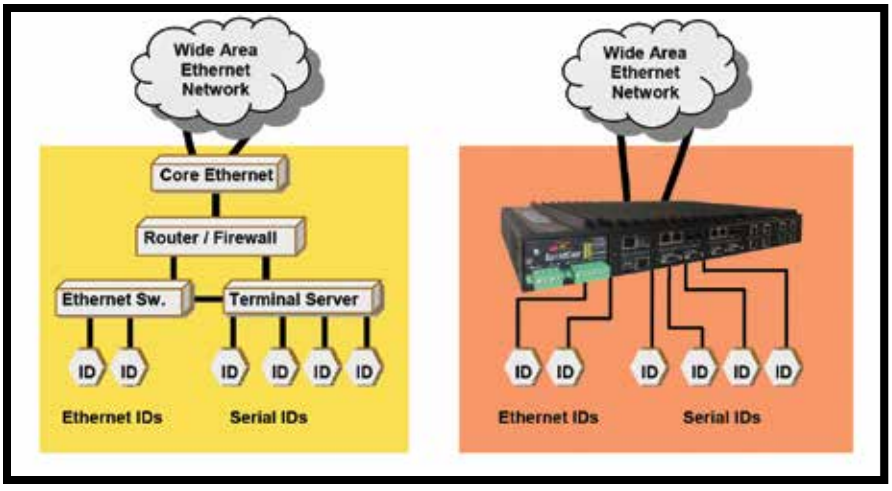

Figure 3: Integrated routers provide WAN access with firewall protection, as well as an integration point for both Ethernet and serial IDs.

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 (top right) shows a network that is wide open to attack.

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.

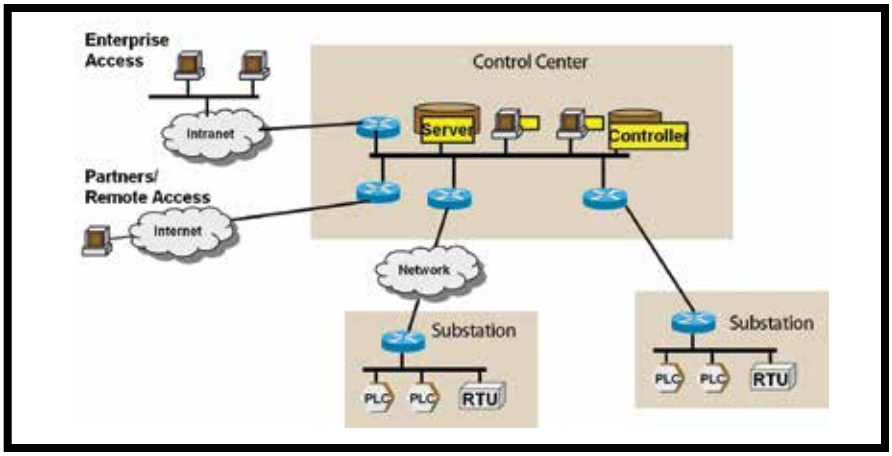

Figure 4: A wide open network—open to attack

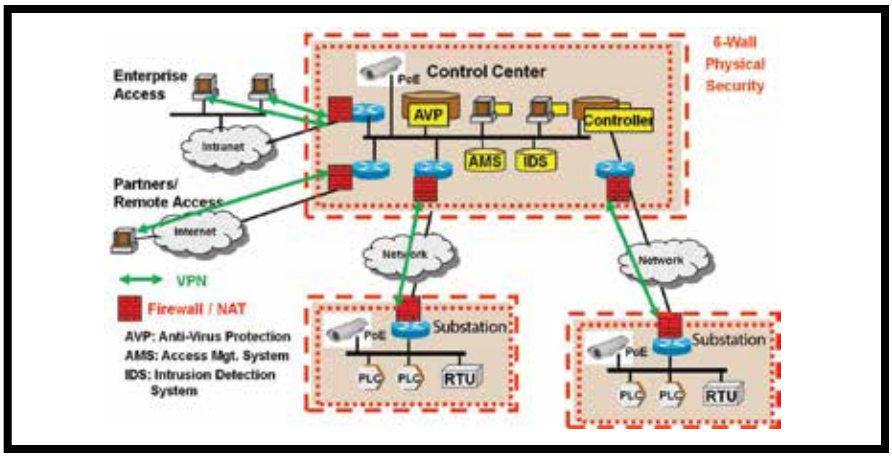

Figure 5: shows the same type system with a stringent physical and cyber security layer inserted.

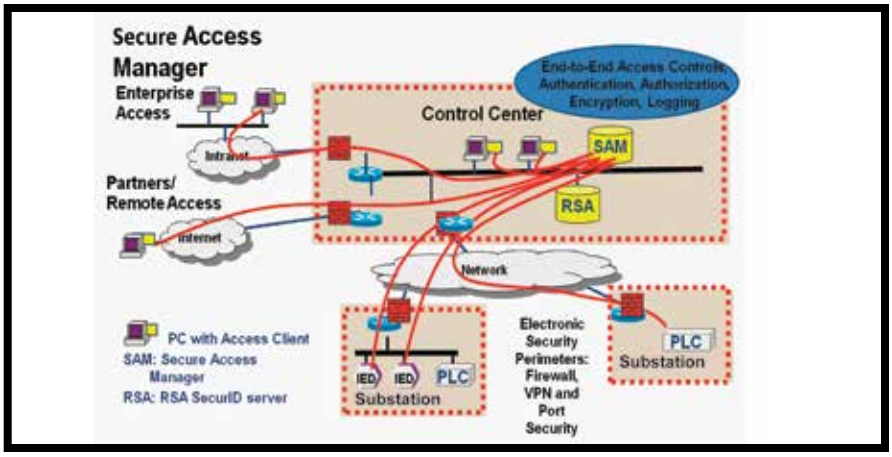

Figure 6: goes one step further, implementing CIP 007 requirements for access control.

- 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 (that 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 the Belden white paper titled "7 Steps to ICS Security."

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

Working Well Together

As is made clear by the discussion on security, operational facilities, such as substations, 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 for a substation can conflict with corporate information flows. Substation functions cannot wait if the IT department arbitrarily shuts down the network for maintenance. 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.

Be Certain with Belden

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 steps 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 when wired solutions are impractical
4. Use an architecture that integrates serial equipment into the IP network and allows migration at the pace the utility can handle
5. Choose equipment with flexible port configurations for easy integration of any IEDs
6. Synchronize distributed
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

Belden is dedicated to power utility networking solutions that combine high availability networking technologies, substation-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 21st century. The challenges utilities 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, Belden 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.

References:

1. "Environmental Standards for Network Devices Installed in Electric Power Stations," GarrettCom, March 2013, http://www/garrettcom.com/iec61850_ieee1613.htm
2. "7 Steps to ICS Security." Eric Byres, Tofino Security, 2012, https://www.tofinosecurity.com/professional/7-steps-wp
3. "Grid operators, planners face challenges," Intelligent Utility Magazine, November/December issue 2012 http://www.intelligentutility.com/magazine/article/292881/grid-operators-planners-face-challenges
4. "IRIG Time Code Formats," Meinberg Global, http://www.meinbergglobal.com/english/info/irig.htm
5. "Guidelines for Smart Grid Cyber Security: Vol. 1, Smart Grid Cyber Security Strategy, Architecture, and High-Level Requirements," The Smart Grid Interoperability Panel – Cyber Security Working Group , National Institute of Standards and Technology Interagency Report. December 2010 http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol1.pdf

GarrettCom®

A **BELDEN** BRAND