

**Implement for Today, Design for Tomorrow:  
How NERC CIP and Security Issues Impact  
Substation Design and Deployment**



GarrettCom, Inc  
47823 Westinghouse Drive  
Fremont, CA 94539  
Tel: (510) 438-9071  
Fax: (510) 438-9072  
[www.GarrettCom.com](http://www.GarrettCom.com)

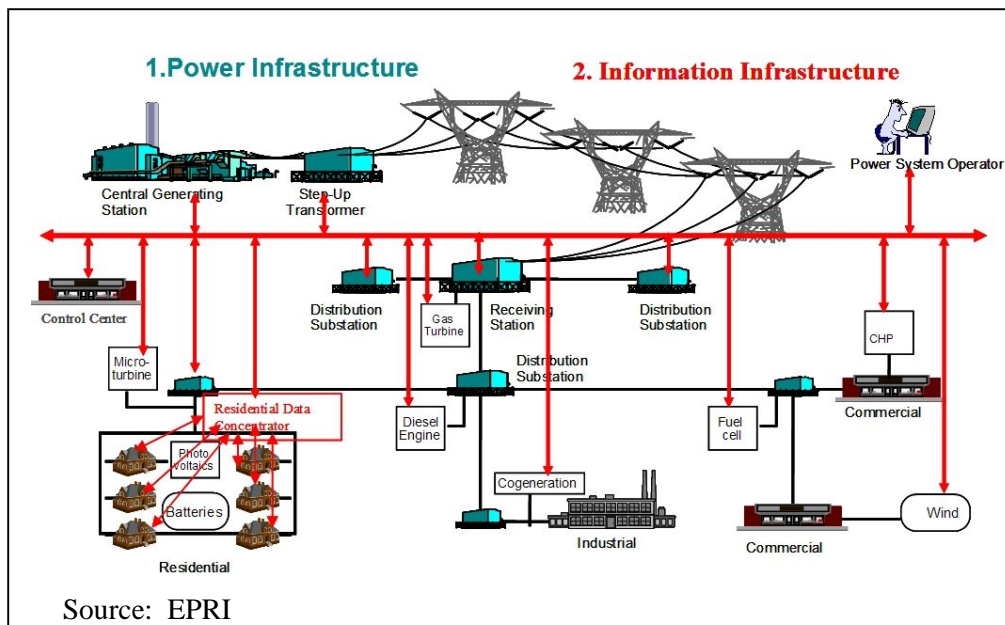
# Implement for Today, Design for Tomorrow: How NERC CIP and Security Issues Impact Substation Design and Deployment

## Overview

In the best of circumstances, each step taken in the design and deployment of a substation network infrastructure project can become a technological and economic enabler to projects that follow, while meeting current operations and regulatory objectives. One of the critical components for designing a future-proof network infrastructure is a solid integration strategy for network components that supports international security initiatives.

EPRI's IntelliGrid Project developed the IntelliGrid Architecture to model the power system of the future. It is instructive to view the tight meshing of both the power infrastructure (protection, SCADA, EMS, RTO, DER) and the information infrastructure (IP-based security, network and data management) in the architecture.

Standards are critical to effective and economical deployment of these tightly integrated infrastructures. It is fair to say that, without standards, such integration would not be possible. IEC 61850 is the international standard that provides the



overall development strategy for substation infrastructure, and Ethernet/IP is a critical component of IEC 61850 and other industry standards because of its beneficial effect in upgrade strategies, providing superior bandwidth and management features including security options. Equally important is avoiding premature obsolescence of existing serial IEDs -- and possibly new installations of

serial IEDs -- into the overall communications structure, and products are available today that provide the integration of serial and IP-based devices.

As the power industry migrates to a model that includes leaner staffing with changing skill requirements, fewer people will be working with more sophisticated data to make decisions that have larger scale impact. Field IEDs today provide more -- and more complex -- data such as waveforms, harmonic analysis, and video. The data is analyzed in sophisticated ways to support a variety of functions, and thus needs to be processed and shared with multiple groups within an

organization. IP provides for standards and interoperability and better management of the data and the network itself, and is at the core of security activities from IP video routing for perimeter security to cyber security support for access logs, and password and application management. See sidebar.

### **NERC CIP Compliance – the First Level**

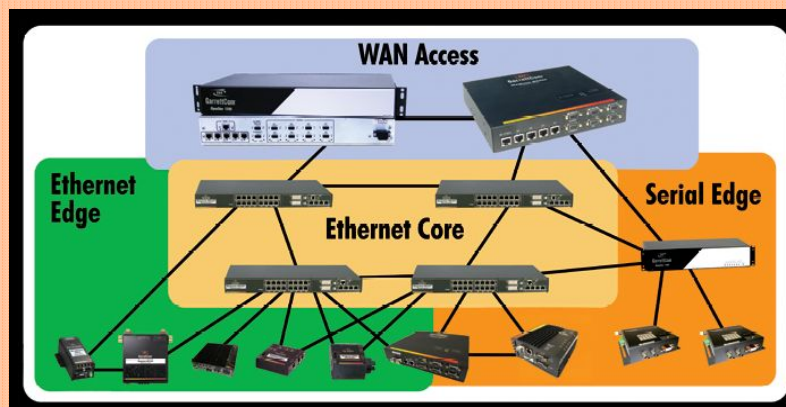
As the time draws near for completing work for the first level of NERC CIP compliance, choices regarding the integration of IP and cyber security into a substation design will have long-lasting impact. The drive towards standardization and integration through IP-based, IT-derived information collection and management, and with those technologies, remote access and web-based applications, is both the savior and the nemesis of modern substation design.

To a large degree, the automation of the substation, with its advanced IP-based technology is the driver for many of the NERC CIP Cyber Security standards. The need for Cyber Security is a function of the maturing of Ethernet communication technology, fiber communications media, wireless media, and the ability to apply that technology over large geographies. Today’s communications and control systems may extend automation and integration from the field device to the control room or regional operating center console. It is instructive that there is a “non-routable” network exemption in NERC CIP that grandfatheres serial-protocol SCADA systems using dedicated analog lines for communication.

It is likely no surprise that maintaining substation security is an ongoing task. FERC, in accepting the current standards, has a requirement that NERC continue to study and refine the standards, with ongoing assistance from cyber security experts. Not only will technology improve, but new forms of attack will emerge on a regular basis.

### **The Integrated IP Architecture for Substation Design**

Most “greenfield” substation designs, as well as substation upgrade designs look to Ethernet/IP technology as the core of any long-term architectural vision. This is consistent with dominant technology trends and is recognized by IEC 61850 architecture. 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 WAN infrastructure over a region. In general, fiber optic media is the first choice for noise immunity, bandwidth and speed, although there are certainly cases with retrofit or adds to existing work where a wireless or digital radio link can save extra costs in construction work.



An effective substation 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 connecting traditional serial devices, and WAN access – all of which are inter-related and need to be inter-operable and integrated with network-wide approaches to network resiliency and network security. GarrettCom offers one of the broadest lines of substation-hardened networking products, which can be viewed at: <http://garrettcom.com/substation.pdf>

As utilities struggle with the mandates, it is clear that there is a certain amount of latitude, and questions arise ; in the rush to comply with NERC CIP Cyber Security standards, how much cyber security is enough right now?

Utilities vary in their internal risk assessment and on the human and financial assets that the utilities are prepared to put forth during the initial compliance period.

The information below discusses the networking decisions that help define CIP -002's "Critical Cyber Assets" (CCAs), and a variety of considerations when determining a cyber security approach. A primary definition of a CCA is that it connects to a control center or other facility outside the substation perimeter using non-dedicated IP-based resources.

### **The Electronic Security Perimeter**

Substations with CCAs must establish both a physical security perimeter (CIP-006) and an Electronic Security Perimeter (ESP) (CIP-005). In most cases, an ESP will be implemented as a firewall. Since NERC CIP defines the firewall requirement loosely, utilities can choose the level of firewall sophistication that is most appropriate for their environment.

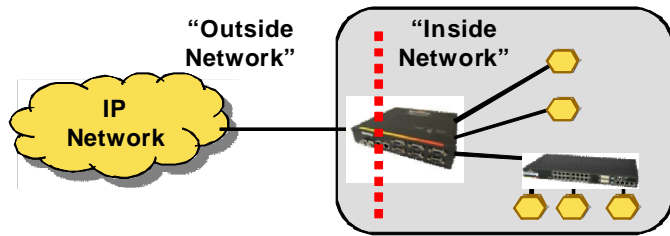
In the simplest case, a firewall can be implemented as a software function in a typical industrial or substation-hardened IP router that is used to manage Wide Area Network connections at the substation. A firewall-capable router such as in the following diagram filters out and rejects all data packets that do not conform to specified rules as to source and destination IP addresses and TCP port numbers. The router would log and report important information for use in auditing and network forensics.

The Ethernet edge network extends fiber media effectively throughout a substation and connects Ethernet-based IEDs back to the core network. While edge 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.

Although many serial edge connections still use static serial-over-fiber link/repeaters to extend IED connections from centralized data communications processors or terminal servers, Serial-to-TCP/IP protocol converters (often called device servers or terminal servers) can be 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. Increasingly, multi-purpose devices can provide both serial and Ethernet edge connectivity, and have the capability to incorporate routing and a WAN connection as well.

Finally, the substation may need to be connected to the outside world via WANs. As substations 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 changing. For example, WAN access must be able to effectively prioritize application traffic, giving Protection and SCADA preferred treatment over data. The WAN device is increasingly expected to fulfill the key role of Electronic Security Perimeter gateway for substation cyber security.

This illustration shows GarrettCom’s compact Magnum DX900 Industrial Router, which provides integrated WAN, serial and Ethernet connectivity in a single substation-hardened device. Designed to support increasing security requirements, the DX900 comes with a full complement of security protocols including, among others, firewall, SSL, SSH, and IPSec.



As utilities begin to take advantage of Internet-related services such as carrier-provided MPLS-based VPN services and wireless Ethernet networking, they are more at risk from attacks than they are with private facility networks, dedicated leased lines or frame relay services. Filter-based firewalls are an appropriate, sufficient ESP when the WAN is a private network dedicated to substation communications, and where other mechanisms are in place to log on-demand remote access such as engineering access to remote IEDs. However, when a utility is using a public IP service or sharing the substation WAN with Enterprise IT communications, then the substation connections should have Virtual Private Network protection in addition to basic firewall filters.

### **Physical Security**

Adding physical security is an easy extension to IP networks already in place in a CCA. Unlike traditional analog security devices, IP-based devices allow many more options for substations to route and manipulate data, greatly increasing the speed and accuracy when detecting security breaches.

By far the most popular IP-based security device is the video camera. Using IP-based video greatly reduces the cost of a video security system, while simplifying deployment and monitoring of video cameras. The average data rate for a video surveillance camera is between 2 and 4 Mb per second, so a 100 Mb network switch running over fiber can handle up to 25 cameras. The same fiber cabling can support 1 Gb switches, which makes it possible to support many more cameras on a single cable.

Substation security applications run the gamut from guarding outdoor parking lots and outlying facilities to physical access control and internal monitoring.

A typical network in a substation provides a system that manages physical access to the site with electronic keys, allowing a central control group to make basic security changes and garner real-time information such as access logs, intrusion detection and security and safety alarms, from the sensors without having to send personnel to remote sites. Secure VLANs are recommended to keep physical security network traffic separate from data, voice and operations traffic.

## Remote Access vs. Remote Servers

Access control is a major challenge in NERC CIP, and is the subject of several of the standards, especially CIP-007. Access control is concerned with systems in the control center as well as with CCAs at the substation including RTUs, IEDs, servers, routers and other network devices.

CIP standards require both individual user profiles and access controls that ensure that only authorized personnel can access systems and devices – and only to perform the specific operational functions for which they are authorized. Strong access controls include two-factor authentication (such as both a password and an RSA SecurID token), strong form passwords, and archived logging of all sessions. Ideally, logs will include actual session activity -- even the archival of all key strokes used during the session -- to enable forensic analysis of user activities.

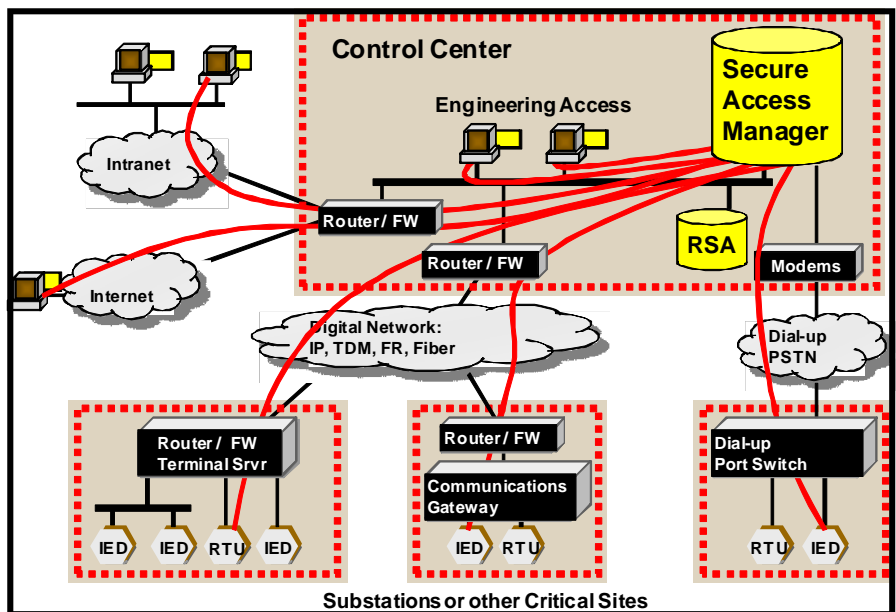
Approaches to access control vary, but an effective way to put an access control system in place quickly is to use an architecture that can work with many existing network arrangements rather than require new technology at every substation.

A centralized architecture provides authentication of users, maintains individual profiles and logs all communications from a central location. One or more centralized Secure Access Manager servers provide for all on-demand communications to substation devices. Thus WAN technologies such as IP, frame relay, dial-up, fiber Ethernet, and remote substation communications technologies such as dial-up port switches, Ethernet LAN, communications gateways, and terminal servers can all be supported transparently to the end users.

In the simplified diagram at the right it is possible to see a variety of connectivity solutions including direct lines (which might be private leased lines or direct Ethernet connection) as well as connectivity through an IP-based Internet cloud which requires a router on either end.

GarrettCom's hardened DX Industrial Routers provide integrated connectivity support. For more detail regarding network architecture at the substation level, (See Sidebar., page 3)

An alternative approach is a less centralized architecture that places secure gateways at each substation and requires that the local devices at the substation are all locally connected to the secure gateway device. This device is typically a server, and thus requires its own "patch management" and ongoing



system administration as a complex CCA. In the long run, such distributed gateway/servers may provide greater overall flexibility, but planners can consider the more centralized architecture to enable a quick start, followed by selective, gradual deployment of remote servers.

### **Security and Productivity**

The impact on end user productivity is an important consideration when implementing NERC CIP access controls. When access controls are implemented with generic IT-oriented technologies, they can add overhead to the process of end users connecting and getting their jobs done. Solutions that are specifically designed for use in a substation environment such as GarrettCom's CrossBow Secure Access Manager are available. CrossBow has pre-configured drivers for all substation IED types, eliminating the need to develop customer drivers. Based on proven remote access software solutions and using the security and management features of GarrettCom's hardened remote networking and security devices, CrossBow provides an Electronic Security Perimeter and auditable secure remote access to intelligent electric devices (IEDs) and other industrial devices.

An appropriate access control system can be a major productivity boost for engineers and operators requiring remote substation access. Authorized IEDs and RTUs can be easily organized in graphical directories. Access across complex networks can be simplified to a basic click-through operation, and vendor or device-specific client applications can be preset and automatically launched to facilitate IED interaction.

Considering the potential productivity boost, it makes sense to implement access control systems as a more universal remote access tool, not just for CIP-designated critical substations. In particular, the centralized approach of CrossBow-type systems enables use of a common user environment across all substations without having to put sophisticated Electronic Security Perimeters or other CIP processes at substations that are not CIP-critical. This also positions the utility to more readily expand full CIP controls to more substations in the future.

### **Defense in Depth**

There are many measures that NERC CIP requires in the relatively IT-oriented world of control rooms. "Defense in Depth" is a concept of providing layer upon layer of threat remediation technology. Thus, Control Centers will typically have a "DMZ" (a so-called demilitarized zone) with sophisticated Enterprise firewalls and Intrusion Detection Systems (IDS) to provide greater separation between the control center and the substation WAN on one side and the utilities enterprise "Intranet" or any Internet connections or other connections to outside partners on the other. "Malware" (e.g., anti-virus protection) and careful "patch management" (control over software and configuration file changes) are critical, especially when control center servers have general purpose operating systems such as Windows and Linux that are more vulnerable to various sophisticated attacks than individual legacy devices.

As utilities move general server technologies out to substations, these additional defensive measures, including ‘malware’ and patch management processes, will have to move out to substations as well. Over time, some utilities will likely pursue IDS and other technologies at substations, although these are not required in the current CIP standards.

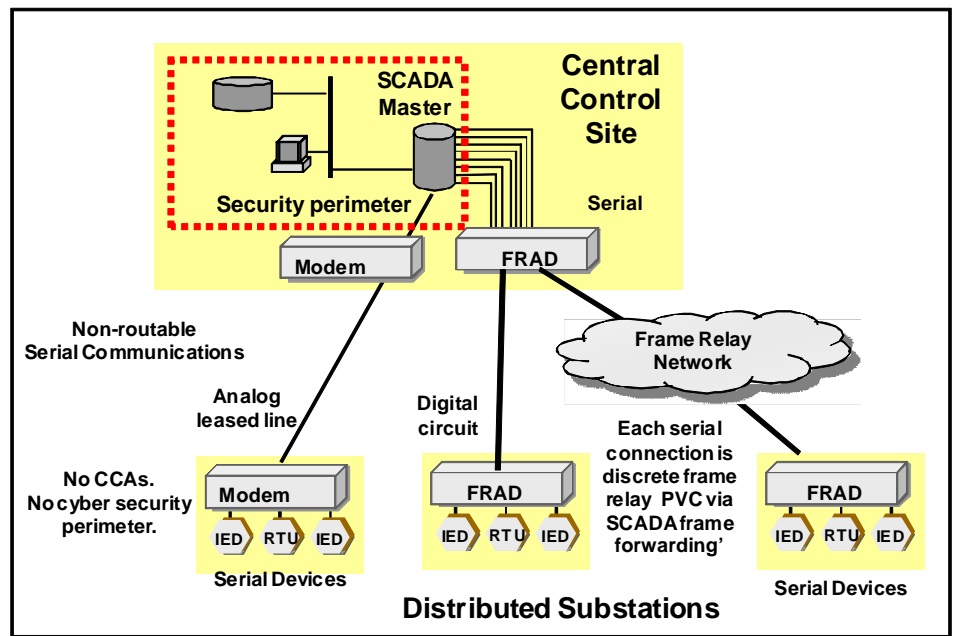
Physical security also plays a role in Defense in Depth since physical monitoring and control within the substation is equally as important as perimeter security.

**The “Non-routable” Exemption: Limiting Critical Cyber Assets**

NERC CIP provides for a “non-routable” network exemption. It was put in place to grandfather existing serial-protocol SCADA systems that use dedicated analog leased lines that cannot be hacked to communicate from control centers (SCADA masters) to remote RTUs. Because all bulk transmission assets are deemed critical under NERC CIP -002, the initial compliance project scope can be minimized by designating as few critical substations as possible.

If a utility chooses avoid the use of dial-up or routable protocols to communicate with Critical Assets (CAs) at the substation, then the substation does not contain CCAs and the other aspects of CIP standards do not apply.

Since NERC CIP includes a requirement to establish relatively extensive physical security measures at remote substations, such as enhanced fencing, gate access systems and video monitoring—as well as advanced network and system security measures – eliminating CCAs to limit project scope can significantly reduce the initial cost and work load of the first phase of compliance.



**Non- routable Networking to Substations**

Routable protocols as identified with IP protocol, generally used with Ethernet-based substation devices (RTUS and IEDs) and sometimes with serial devices such as Serial-IP terminal servers. However, some fiber multiplexer systems and some frame relay-based networking systems can be configured to connect control centers and substations without use of routable protocols. For example, GarrettCom’s DynaStar Industrial Frame Routers with frame relay support can encapsulate serial SCADA messages directly into frame relay protocol (considered a non-routable protocol) using a technique called SCADA Frame Forwarding. Since it does not use the TCP/IP headers that are common with Serial-IP terminal servers and routers, SCADA Frame Forwarding can combine several serial data streams over a single digital

circuit or across a frame relay network without creating CCAs at the substation.

While some utilities are finding it necessary to disconnect some Ethernet devices and revert to completely serial communications in order to defer the upgrading of some substations and focus initial activities more narrowly, this is only a short-term solution to gain breathing room.

### **Life Cycle Costs**

A part of any NERC CIP compliance strategy must be a consideration for Total Cost of Ownership (TCO). When practicalities dictate less-than-ideal solutions to meet urgent needs, it still pays to take the time to look to the future. For any plan, it pays to factor in both immediate equipment costs and longer-term costs of maintenance, replacement and ongoing systems integration, as well as the extensibility of new products and technologies over time. It is critical that anticipated future directions of technology and standards be incorporated into life cycle costing so that systems and components do not have to be prematurely retired.

Looking for products that are both IP-ready and hardened for substation use is a wise step in any substation automation project.

GarrettCom's Magnum product line offers a broad line of substation-hardened, flexible products that can help a substation migrate from serial or mixed serial/Ethernet to a fully IP-based facility as time goes on. Some of them have been mentioned in this paper.

IEC 61850-3 and IEEE 1613 standards define equipment requirements that increase product reliability in harsh substation environments. Many "industrial-hardened" products claim some heightened electrical immunity relative to basic commercial grade products, but "substation" standards are considerably more stringent.

### **The Future Looks Better with a Plan**

As noted above, the NERC CIP standards are not fixed in stone, and are likely to evolve, perhaps at a fairly rapid clip. Technology is also moving inexorably forward. No utilities will consider avoidance of routable or dial-up communications to be a viable long-term approach to cyber security, since IP networking is becoming the mainstay of automation systems.

Network planners deploying new devices for either non-routable networks or more basic filters-based private-network firewalls should consider implementing devices today that can also meet future requirements. There is some speculation that future versions of NERC CIP standards may both eliminate the "non-routable exception"

described above and also mandate the use of VPN technology for critical substations.

In reality, full cyber security implementation will likely never be completed. New threats will emerge. New regulations will emerge. Perhaps most importantly, as utilities proceed with cyber security implementation, they will become more comfortable with the technologies and related processes and begin to view heightened security measures as the normal way of doing business and protecting business assets, not only at CIP-mandated facilities, but throughout the utility network.

NERC CIP provides a good opportunity to review substation architecture and plan for the future. Rather than simply patching together something to meet imminent requirements, taking the time to plan can set a substation up on a strategy that will serve it well into the future. Secure, flexible, reliable and extensible data management and communications technologies today will form the basis for future upgrades and new systems. With standards such as IEC 61850 providing a strong base upon which to build Ethernet/IP-enabled deployments, power utility designers are able to design and implement upgrades – and “greenfield” projects that will serve their companies and their customers well into the future.