Substation Networking with Non-Routable Protocols: A Practical Alternative for NERC CIP Compliance

GarrettCom, Inc.
Technical Brief – Overview Version

GarrettCom's network products provide important options for utilities that are addressing NERC Critical Infrastructure Protection standards. Magnum DX and DynaStar substation hardened routers provide Wide Area Network (WAN) connectivity between power substations and operations control centers for numerous electric utilities. These WANs commonly use a combination of routable and/or non-routable protocols. When only non-routable protocols are used, substations with critical assets are networked without requiring the use of Critical Cyber Assets (CCAs) at remote substations, as defined in CIP-standard CIP-002. Avoidance of "CCAs" means that the other CIP-002 to CIP-009 requirements do not apply at these substations, which will likely defer significant implementation costs and ongoing administrative overhead associated with CIP compliance.

Background and Motivation

The North American Electric Reliability Corporation (NERC) has adopted Cyber Security Standards as part of a larger power grid reliability and Critical Infrastructure Protection (CIP) program. The set of eight NERC CIP cyber security standards (CIP-002 to CIP-009) are expected to be endorsed by the Federal Electric Regulatory Commission (FERC), with enforcement including possible fines as empowered by the Energy Policy Act of 2005. Utilities must be in compliance with the standards in August 2009 with full compliance audits beginning a year later.

A first step in compliance is to identify "Critical Assets" (CAs). These are defined by NERC as, "Facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the Bulk Electric System." In effect these are major transmission facilities and the equipment and systems that can directly affect the operation of these transmission assets. If communication with a Critical Asset involves "routable protocols" or dial-up facilities, then the Critical Assets and all other devices involved with the same routable/dial-up network are considered "Critical Cyber Assets" (CCAs) and their management is closely governed by CIP standards. If routable protocols or dial-up facilities are not involved, then these assets are not CCAs and thus are not subject to CIP standards.

Clearly much is at stake in determining whether routable protocols are involved with a critical substation. If CCAs exist at the substation then all CIP-002 through CIP-009 requirements apply. CIP-002—009 standards include physical perimeter and access controls (CIP-003), Electronic Security Perimeter (CIP-005), and many other administration and auditing requirements. These will likely necessitate additional investment at each affected substation as well as ongoing administrative expense.

A practical interpretation of the standard is that a routable protocol is one that includes Internet Protocol (IP) as part of the protocol "stack." (In theory, there are other, but now rare, Layer 3-4 "routable"

protocols with similar function to IP.) In general, any devices using Ethernet interfaces will involve IP-based protocols. Many carrier or Internet Service Provider (ISP) services, including IP Virtual Private Networks (IP VPNs), as well as many Enterprise "Intranets" are based on IP protocols. When there is any involvement of Ethernet-based LANs at the substation (that are connected back to central systems) or use of public or private IP-WAN services, the network is using "routable" protocols.

Many substation RTUs and other Intelligent Electrical Devices (IEDs) have serial protocol interfaces, rather than Ethernet. Most serial interfaces (commonly with RS232 or RS485 physical/electrical device interfaces) with protocols such as DNP3-serial or vendor-specific legacy serial protocols, do not inherently involve IP.
The non-routable protocol exception in CIP-002 was created primarily for those cases where the only communication to a substation is serial-based protocols from a SCADA master to remote devices such as RTUs over dedicated facilities such as analog leased lines. Unlike most modern, integrated networks, transmitting serial protocols over analog leased lines does not add "routing."

The analog leased line alternative exempted by CIP standards has many unattractive limitations, however. Analog leased lines are already expensive services from telecom carriers, and carriers are making analog lines more expensive and difficult to obtain over time. Compared to newer digital network alternatives, analog lines have limited bandwidth and high error rates. Dedicated circuits are inflexible. Each new substation automation project may require yet another physical circuit to be installed. For all of these reasons, many utilities look to shared, digital network architectures. Private fiber networks, Frame Relay Services and new carrier-provided IP services are among the alternative WAN network technologies that offer greater economy and flexibility than analog lines.

GarrettCom's SCADA Frame Forwarding Non-Routable Networking Solution

GarrettCom's substation routers have two principal modes of transporting serial communications over a WAN, one routed and one non-routed. In many implementations these two modes will co-exist on a common WAN. The non-routable transport mode is referred to as "SCADA Frame Forwarding" and sometimes as "Serial-over-Frame Relay" (or "Serial-FR"). In the context of NERC CIP, this may best be thought of as a "Frame Relay Multiplexing" technology. As a "multiplexing" technology, Serial-FR encapsulates each RS-232 or RS-485-based serial data connection at a substation into a unique Serial-FR logical connection (a Permanent Virtual Connection or PVC); then multiple FR PVCs are multiplexed over a single digital connection using Frame Relay protocol (layer 2 only). Typically at the control center, each Serial-FR connection is then converted back to a native RS-232/RS-485-based serial interface, then connected to a Serial-based SCADA master. Figure 1 depicts GarrettCom routers used with multiple substation connections in Serial-FR mode. (Note that GarrettCom has two families of substation routers, DynaStar and Magnum DX. These are referred to collectively in this paper as DynaStar/DX.)

DynaStar/DX SCADA Frame Forwarding will work similarly whether implemented using point-to-point digital circuits from substations to control centers or using a frame relay network ("cloud") – either a private frame relay network or a carrier-provided Frame Relay Service. There is no IP routing provided over frame relay. The protocol 'stack' remains Serial-over-FR without IP. When using a frame relay network, the frame relay PVCs are merged onto common trunks via intermediary frame relay switching nodes. Serial-FR using a frame relay network, rather than frame relay over dedicated digital circuits, is also depicted in Figure 1. Note that some GarrettCom DynaStar models can also provide frame relay switching as well as frame relay access functionality. Utilities can implement private frame relay networks using only DynaStar equipment.

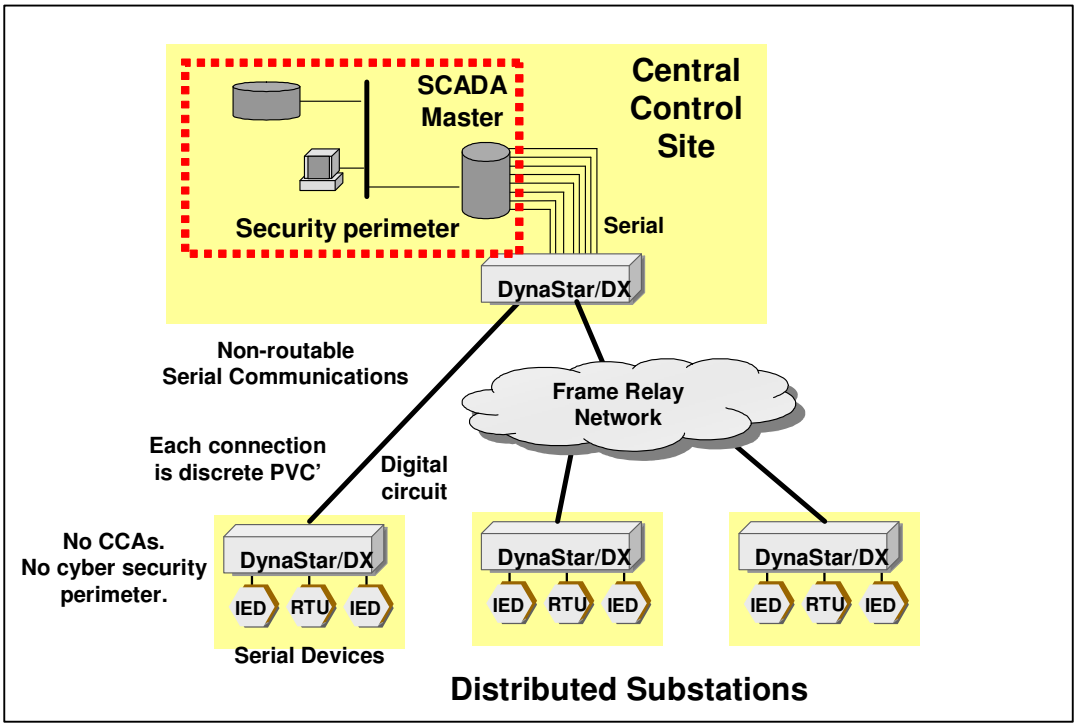

Figure 1: DynaStar/DX non-routable networking with SCADA Frame Forwarding

DynaStar/DX Migration to Secure IP Routed Networking

Utilities will eventually migrate from serial-based substation automation systems to IP and Ethernet – based systems. The non-routable networking 'solution' is at best an interim measure to defer full CIP compliance at critical substations that will someday require full CIP-002—009 compliance.

The transition to IP can occur in two separate phases, creating different issues. As a likely first phase, central servers will move from serial interfaces to Ethernet interfaces within the control center before remote devices using Ethernet are deployed at substations. These Ethernet-based Master systems will assume that the WAN network is based on IP and that remote devices are accessed by remote Serial-IP terminal servers. A non-routable WAN does not support serial-IP.

DynaStar products can resolve this issue. DynaStar can enable the migration of central servers to Ethernet without disrupting the Serial-FR non-routable approach to remote substations. A DynaStar network node can act as a gateway between TCP/IP traffic originating from Master systems and Serial-FR SCADA Frame Forwarding traffic to the remote substation.

The likely later, second phase of IP migration occurs at the substation where eventually Ethernet devices will be deployed requiring IP-based connectivity to central systems. Also, there will be increasing

pressure over time to provide engineering and administrative access to substation RTUs and other IEDs via an IP network, both to substation Ethernet devices and to serial devices (using Serial-IP).

DynaStar and Magnum DX products integrate serial, Ethernet, and WAN interfaces with frame relay and IP routing in a single compact device. Ethernet-based IEDs, serial devices via Serial-IP, and serial devices via SCADA Frame Forwarding can all be attached to the same DynaStar/DX within a substation. The frame relay WAN connection can migrate from Serial-FR-only to a hybrid of IP-FR and Serial-FR, and then eventually to IP-FR only. If appropriate, the WAN connection can move from frame relay to IP-over-Ethernet-fiber or new MPLS-based IP services provided by telecom carriers.

This migration to IP routing requires compliance to the full set of CIP-002—009 standards. These include establishment of a substation Electronic Security Perimeter and other measures. The same DynaStar/DX routers used to provide a non-routable solution can also become part of a comprehensive cyber security compliance plan, providing an Electronic Security perimeter and other capabilities needed for full compliance. More specifically, DynaStar/DX products support a combination of Perimeter security, LAN Security, and Management Security.

Summary

NERC CIP standards are a catalyst for disruptive changes at power utilities. Many of the IP networking and cyber security technologies implied by full CIP compliance are forward looking and will help accelerate effective deployment and utilization of advanced substation automation. However, for many utilities, the CIP deadlines are pressing quickly upon them. The amount of available IT and cyber security expertise, the scope of existing IP-based technology deployments, and the resources available to address CIP compliance are all limited. GarrettCom's DynaStar and Magnum DX products offer an attractive alternative for these utilities to meet networking needs while deferring full implementation of CIP standards at selected critical substations, and then to implement fully compliant IP and Ethernet-based integrated substation networks as substation needs evolve.

GarrettCom™
Industrial Networking at Its Best™

GarrettCom, Inc.
47823 Westinghouse Drive • Fremont, CA 94539 • PH: (510) 438-9071
Email: mktg@garrettcom.com • Web: www.GarrettCom.com