The SMP™ Gateway in an IP-based environment

With the increased use of TCP/IP-enabled devices, vendors of networking products have been promoting utility network architectures where field devices are directly connected to control centers through ruggedized routers and switches. However, this vision, which is part of the new “Internet of Things” trend, fails to take into consideration the benefits of a distributor layered architecture and the solutions that vendors of automation systems are proposing, such as data concentrators and security appliances.

This white paper presents the benefits of using Eaton’s Cooper Power Systems SMP™ Gateway data concentrators in an IP-based substation environment, and explains how it complements routers in such a context.

The router: securing access to the perimeter

Cyber security standards such as NERC CIP now require that Intelligent Electronic Devices (IEDs), Remote Terminal Units (RTUs) and other devices implementing critical electrical and protection functions, also known as “Critical Cyber Assets” (CCA), be deployed in a protected zone called an “Electronic Security Perimeter” (ESP). Access to the perimeter, to connect these devices to a SCADA master station, or any other control center station, shall be managed by an “Electronic Access Point” (EAP).

Increasingly, routers are being used as EAPs. A router is a network device used to create different network segments and to forward data packets between these subnets. Equipped with a firewall, it is a good choice for implementing an EAP. It is especially true from the NERC CIP perspective, as the EAP cannot be implemented by one of the critical cyber assets protected by the ESP itself.
Router limitations and integration issues

Building an ESP is one step of a distribution or substation automation integration project. However, there are some integration issues that cannot be solved by a router:

Substation data is simply... data

A router acts at the Transport layer of the network while most protocols used in a substation automation system are built on the Application layer. As a result, the router cannot process the data, and the benefits that result from the integration of the substation IEDs in the form of local automation, built-in logic, alarm management, and data visualization, cannot be implemented at the substation level.

Consequences of IED upgrades and replacements

All configuration changes at the IED level, including the replacement of legacy IEDs, will necessarily have an impact at the SCADA master station level with the resulting reconfiguration, commissioning and retesting costs in time and money; in those scenarios, the router does nothing to help.

Encryption and authentication

Routers can be used to create a secure VPN tunnel between the enterprise and the substation. Additionally, a protocol such as IPsec supports authentication of the endpoints. However, such an approach does not provide end-to-end security between SCADA and field devices as recommended by the IEC 62351 standard, or authentication and authorization of users to connect to IEDs.

Troubleshooting does not get easier

With such heavy traffic and the fact that the router has no knowledge of the application protocols that are used through it, troubleshooting communication issues can rapidly become complex and frustrating. Tools such as Wireshark are essentially designed to support networking protocols, not protocols used for SCADA.

Network bandwidth and traffic load

Depending on the number of integrated IEDs and their corresponding connections to the SCADA master station, the automation system can put a significant load on the router and the subnets it bridges. While the router can implement traffic management through QoS, it does not have enough “knowledge” of the application protocols and data types to perform any type of data reduction or filtering.

The good news is that all of these issues can be solved by pairing the router with a data concentrator such as the SMP SG-4250 or the SMP 4/DP, which are all part of Eaton’s Cooper Power Systems SMP Gateway product line.

The following diagram shows typical substation architecture based on IP communications:
The SMP Gateway: secure single point of access to substation data

The main function of a data concentrator is, of course, data concentration. Since its first inception, the SMP Gateway has always supported a vast array of standard and vendor-specific protocols, which allows it to interconnect with most IEDs, RTUs, Digital Fault Recorders (DFRs) and control centers on the market. By concentrating the data gathered from multiple IEDs before pushing it to the SCADA master and other master stations, the SMP Gateway acts as virtual RTU, greatly reducing the number of connections and the traffic that goes through the SCADA network. It also acts as a proxy that prevents direct access and attacks to IEDs as the data packets are never transmitted directly to the devices (even for direct access purposes).

Future-proofing substation architecture

The use of a data concentrator such as the SMP Gateway isolates IEDs from the SCADA master. If the data model implemented at the Gateway level is based on the actual electrical functions of the IEDs, any IED can be replaced with minimal configuration changes at the Gateway master communication level. The SCADA master configuration and the Gateway slave configuration will remain unchanged, which results in lower commissioning and testing costs. This is particularly true for legacy IEDs or low cost IEDs, which use non-standard and non-secure protocols and which will sooner or later be replaced by modern IEDs that support IEC 61850 or secure DNP3. By taking this into consideration while designing a substation data model, headaches and nightmares can be prevented when the time will come to replace legacy IEDs.

Securing substation data

The SMP Gateway supports secure authentication at the Application layer level (for application protocols such as DNP3, ICCP or IEC 61850), but also the Transport layer level (using X.509 certificates). It also supports Transport Layer Security (TLS) encryption for all of its TCP/IP communication links; from the master connections used to connect with IEDs to the slave connections used to connect with control centers, including those used for remote access and diagnostics.

The SMP Gateway also provides a local authentication mechanism based on security tickets that simplifies substation security architecture as compared with supporting Lightweight Directory Access Protocol (LDAP) or Remote Access Dial-In User Server (RADIUS) at the IED level.

Finally, the SMP Gateway provides additional security features that help implement a defense-in-depth approach:
- Redundancy is supported not only at the Gateway level, but also at the connection level.
- Only authorized and certified programs can run on the SMP Gateway; this whitelisting mechanism is used to protect the unit against malware, and is more adapted to the reality of a substation than antivirus programs that need frequent updates.
- An integrated firewall blocks all ports by default as required by security standards.

Local automation and HMI features: doing more with less

Integrated data can be leveraged at the substation level using the SMP Gateway local automation and HMI features.

The SMP Gateway provides basic automation functions that allow implementation of simple logic based on the data gathered from the IEDs. The resulting data can then be forwarded to the SCADA master and the other master stations. Moreover, the SMP Gateway supports a PLC engine based on IEC 61131-3. It is configurable using the CODESYS IDE and can be used to implement more sophisticated logic functions on the integrated data.

When connected to a touchscreen, an SMP Gateway equipped with the HMI module turns into a basic substation HMI providing the following display functions:
- A single-line diagram representation of the substation, based on the integrated data
- A communication dashboard that provides the communication status of all IEDs that are connected to the SMP Gateway
- Alarm annunciator capabilities

These features are not only available inside the substation, using a touch screen, but also remotely through a browser-based interface.

SMP Tools: superior tools for efficient commissioning and troubleshooting

The SMP Gateway comes with a suite of programs called the SMP Tools, which is available for configuration and diagnostics. One of these programs, called SMP Trace, is a packet analyzer that generates human-readable traces for all supported protocols. Such a tool is invaluable compared to standard packet analyzer programs.

Conclusions

Security is a fundamental requirement of distribution and substation automation integration projects. But the first and main requirement of such a project is the successful integration of all substation devices with the control center. Routers and security appliances will help build an electronic security perimeter around critical cyber assets.

However, it is the SMP Gateway that will help integrate all IEDs together to fully leverage substation data, and turn a substation integration project into a success story.
Biography
Mathieu Harvey is Senior Technical Writer in the Energy Automation Solutions group of Eaton’s Cooper Power Systems, where he is responsible of the technical documentation for the Substation Automation product line. He has a background of 13 years in technology and product development, and has worked in technical writing, quality management, and software development functions. Mathieu has a B. Sc. in Computer Engineering from Université de Sherbrooke and is a licensed Engineer in the province of Quebec, a certified ISO 9001:2008 lead auditor and a member of the Society for Technical Communication (STC).

References
“NERC Critical Infrastructure Protection Standards,” retrieved from: http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx