Utilities

WHITE PAPER

May 2013

INTEGRATING SUBSTATION IT AND OT DEVICE ACCESS AND MANAGEMENT

Table of Contents

Introduction

Today's modern substation architecture requires information technology (IT) devices just as much as it requires operational technology (OT) devices. The design and operation of the substation networks play a part in the reliability and control of the power grid. IT and OT technology has traditionally been managed separately, meaning that utilities stand up separate solutions for the different types of devices. These solutions include securing remote access, adhering to NERC/CIP regulations, providing status reporting through SCADA, and providing local substation situational awareness through graphical visualizations. But implementing separate IT and OT solutions imposes higher costs in capital expense; training, operating, and maintaining separate networks; and guaranteeing security.

In this paper, Cisco and SUBNET Solutions Inc. (SUBNET) present several techniques that will help utilities solve the problem of requiring multiple device access and management solutions for their substation devices and specifically focuses on integrating the device access and management of substation IT and OT devices. The net results are an up-front savings in infrastructure costs, a continual savings in operations and maintenance costs, and easier access to information, with security and scalability to grow as needed.

Problem Statement

Traditional substation architectures demonstrate levels of discontinuity between device functions and business systems. This has mainly risen from vendor-specific device functions being aligned with the vendor-specific business systems as well as the use of serial-based point-to-point connectivity to integrate the devices within the substation. This is true for OT devices, and is more-so true when IT devices are part of the substation architecture. This leads to duplicate systems being installed, one for each vendor type. The resulting system is fragmented, complex, and requires significant up-front and operations and maintenance investment to maintain. Figure 1 illustrates the typical situation today.

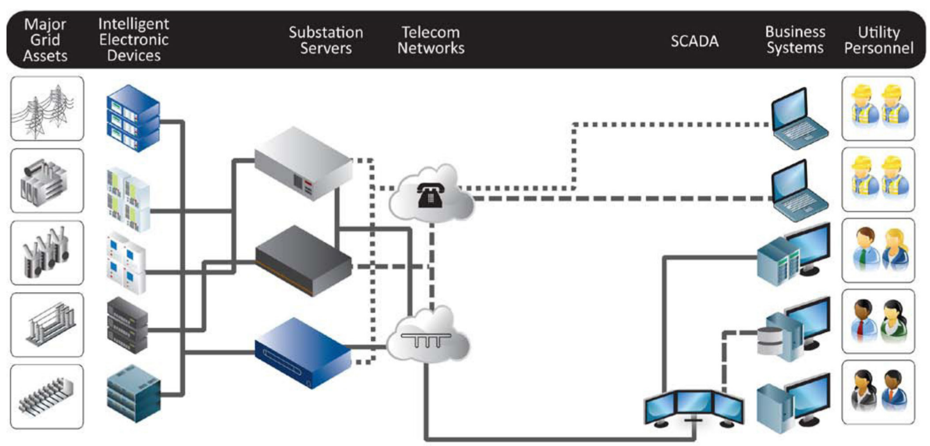

Figure 1. Traditional Substation and Business System Architectures

As shown in Figure 2, modern substation architectures using networking technology, physical and cyber-security infrastructure, and standards-based interoperability are able to normalize the environment and make sure the device and business system integration is consistent, does not require duplication, and is more cost-effective.

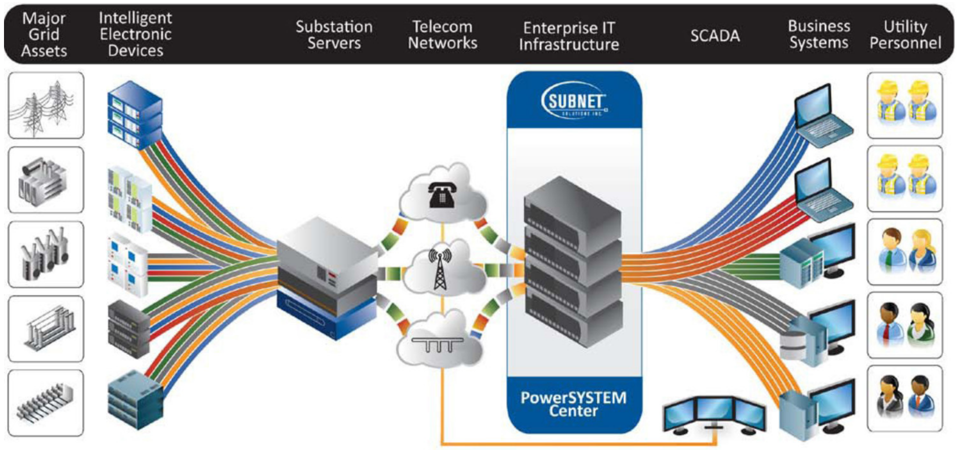

Figure 2. Modern Substation and Business System Architectures

Solution Requirements

Any solution to this problem must include the following elements:

- Centralized and in-the-field visualization of the system as a whole and all of its components. Multiple, disparate visualization systems can be confusing, require more training, and might lead to operator errors.
- Remote engineering access to the substation devices. Once the problem is consistently visualized, implementing a solution in a timely and cost-effective manner is the next challenge. Remote access from the operations center reduces truck rolls and cuts to the time to rectify a problem.
- Strong security. Remote access and visibility without adequate cyber security can be disastrous if the communications network does not effectively mitigate the ever-present threat from hackers and coordinated attackers.

Components of an Integrated Solution

Integrated Remote Access Management

SUBNET's PowerSYSTEM Center manages access to IEDs, allowing utilities to securely perform a broad range of operational, maintenance, and asset management tasks remotely. Through its single-sign-on capability, role-based access control is based on the user's IT username and password. Instead of having to know specific connection and password information for every different IED in the system, users need only know their existing IT username and password; the IED management system manages user access rights based on these credentials. (See Figure 3.)

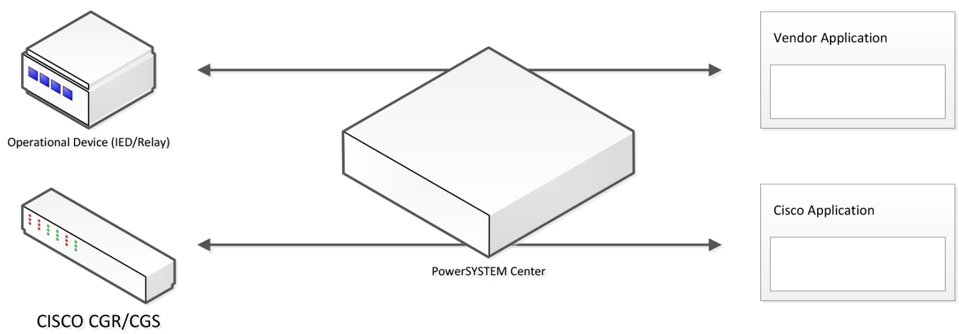

Figure 3. Integrated Remote Access Management

This capability is also used to provide access to Cisco® 2500 Series Connected Grid Switches and the Cisco 2010 Connected Grid Router (CGR 2010). When integrated with PowerSYSTEM Center, utility personnel manage access to the IT devices in the substation in the same manner as they manage the access to their OT devices. Role-based access control can make sure that only qualified personnel are allowed access to the Cisco equipment.

Among the many benefits of remote access:

- Remote access avoids truck rolls, saving on the utility's operating costs
- Remote access leads to faster response times. Faster completion of work orders means:
  - o Better operational efficiency
  - o Improved CAIDI/SAIDI
- Remote access means less on-site human presence in the substation, enhancing worker safety
- Remote access usually leads to centralized, unified access with a common set of tools, reducing training costs
- PowerSystem Center provides interleaved SCADA control with remote access on a serial link, using existing substation cabling to provide remote access

Integrated Password Management

SUBNET's PowerSYSTEM Center automates the password management process for all IEDs, including the communications network, all of which are needed for compliance with NERC CIP. It becomes the secure password vault and repository for all IED passwords. More than that, however, administrators can make password changes at prescheduled times, while preserving the ability to make password changes on demand or manually, as required. They can grant and control local IED access without additional hardware at the substation.

NERC/CIP requires devices to have their passwords rolled every so often. And "critical infrastructure" includes the communications network equipment in the substation. PowerSYSTEM Center provides this functionality. It can be a password vault solution for Cisco Connected Grid routers and switches.

By providing role-based access control and comprehensive password management functionality, the SUBNET IED and substation device Management Solution – PowerSYSTEM Center facilitates NERC CIP compliance and is a key part of a comprehensive solution needed for full compliance. It simplifies and facilitates NERC CIP audits by delivering easily maintained and accessible audit records. And, of course, it lowers security risk.

The solution allows employees to better focus on their job function. It minimizes labor required to perform password changes by simplifying the password maintenance process. As a result, it lowers risk and increases reliability for both IEDs and networking equipment in the substation.

Integrated Configuration Management

The Configuration Management aspects of PowerSYSTEM Center are provided with the My Settings module. This module integrates PowerSYSTEM Center's native Data Model with SharePoint's Document Library infrastructure. This allows for the full search capabilities as defined by the Data Model metadata along with the full archiving and version control management capabilities of SharePoint's Document Libraries.

Integrated Visualization and SCADA Control

Most utilities today manage substation devices (IEDs and RTUs) using SCADA systems at the headend. Toolsets have been created using SCADA protocols. To enable use of this investment in management systems and personnel training and expertise, Cisco's substation switches report status via SCADA. This means that a management system such as PowerSystem Center can give unified access to both operational as well as IT equipment deployed in the substation.

Modbus allows for the substation switches also be integrated into the SubSTATION Explorer HMI for local situational awareness and control. This aids in on-site diagnostics and troubleshooting and reduces the time it takes to determine errors and validate function. Visualization of Cisco substation switches is quickly realized in SubSTATION Explorer through the use of pre-built templates. Figure 4 illustrates how this looks to an operator.

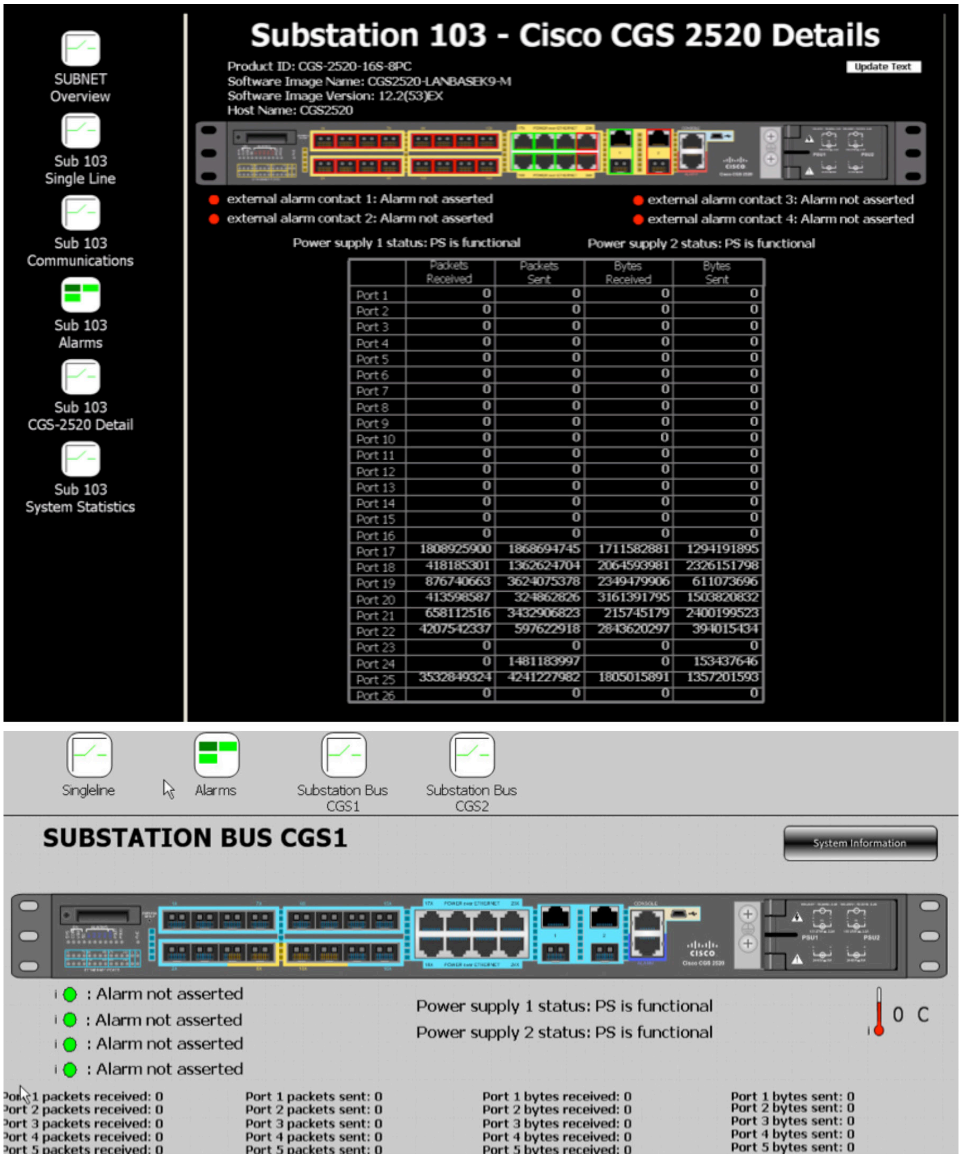

Figure 4. Examples of centralized management of substation devices

While command line interfaces and SCADA protocols are the norm for utility operations and control, many utilities are investing in the tools and protocols used in traditional IT network management – such as SNMP and CiscoWorks NMS. Together, these tools smooth the path to integration of IT and OT by extending the view of the substation devices into the traditional IT network view, while extending the view of the substation LAN devices into the traditional SCADA-based HMI and visualization.

Complete Substation Security Designs

Moving beyond password security and into the realm of network security, the CGR 2010 helps to maintain a secure perimeter and access around the substation network. In conjunction with SUBNET's SubSTATION Server, the electronic security perimeter can be preserved through the security posturing within the router while working in combination with SUBNET's secure IED access features. Specific routing policies and firewall capabilities can be employed on the router and network to create and restrict all logical paths to IEDs to transit through the SubSTATION Server.

Other functionality can also be deployed on the CGR 2010 to provide additional security aspects for the Substation Data Gateway.

- Data Confidentiality for all SCADA traffic can use the on board hardware acceleration within the CGR 2010 for increased encryption performance. Advanced VPN functionality within the router will also help integrate further with the network to provide greater end-to-end flexibility for the Substation Data Gateway.
- As mentioned previously, the Cisco IOS® Firewall is a zone-based stateful firewall built into Cisco IOS Software that makes the CGR 2010 an ideal security and routing solution in one device for protecting the WAN entry point to the substation data gateway and associated IEDs. The Zone-based firewall capability provides segmentation while providing traffic inspection.

Cisco can provide additional functionality for SCADA protocols like Firewall, Intrusion prevention, Data classification for Quality of Service (QoS) and Segmentation to bind the substation gateway and the network gateway more closely together.

Other Benefits of the Joint Solution

Operations Center Integration and Applications Deployment

Cisco's powerful and cost effective Cisco Unified Computing System™ (Cisco UCS®) servers can host PowerSYSTEM Center and other SUBNET applications in a native or virtualized environment. Integrating and consolidating multiple management applications systems as VMs on a single Cisco UCS rack mount server can reduce the capital cost of operations center server infrastructure, and save on maintenance and enhancement costs, while providing scalability and future growth.

Certified Interoperability

SUBNET Solutions Inc. is a member of the Cisco Developer Network (CDN) for Connected Grid. Solutions described above have been jointly designed by Cisco and SUBNET, verified to be interoperable, and certified as "Cisco Compatible." The certification helps ensure the customer that the joint solutions can be easily and cost-effectively deployed, avoiding time-consuming integration and testing at each site.

Conclusion

Cisco and SUBNET are partnering to enable an easier transition from traditional substation architectures to an integrated and secure substation architecture. Multiple devices, access technologies and vendors need to be accommodated during this evolution. As shown in this paper, SUBNET and Cisco provide real solutions for this integration by using networking technology, physical and cyber-security, and standards-based interoperability. The net result to the utility company is operational cost savings, improved reliability and safety, and improved security of the substation and power system infrastructure.

About Cisco Products

The Cisco Connected Grid portfolio of solutions is designed specifically for the harsh, rugged environments often found in the energy and utility industries. These solutions include the CGR 2010 and the Cisco 2520 Connected Grid Switch (CGS 2520), which have been designed to support the communications infrastructure needs of the energy delivery infrastructure across the generation, transmission, and distribution sectors. Designed for highly secure, reliable, and scalable infrastructure, the CGR 2010 and CGS 2520 are an ideal platform to support the Smart Grid and other energy delivery infrastructure needs of customers. These ruggedized products have been extensively tested and are KEMA certified to meet challenging substation compliance standards, including IEEE 1613 and IEC 61850-3.

In addition, Cisco's Physical Security and Mobility products help monitor the substations while allowing secure and auditable access to maintenance personnel. Cisco's best-in-class WAN infrastructure products help to connect the substation and the operations center together seamlessly and securely. Finally, Cisco brings the highly scalable and cost-effective Cisco UCS platforms and associated data center products for hosting applications to the table.

The SUBNET portfolio of solutions is designed specifically to provide utilities with multi-vendor compatibility for substation operational and non-operational data access, local substation data visualization, secure remote device access, automated password management, and configuration management. These solutions include SubSTATION Server, SubSTATION Explorer, and PowerSYSTEM Center.

About SUBNET Solutions Inc. Products

SubSTATION Server is a multi-function software application that performs data concentration, protocol translation, automation logic, event file collection and enterprise connectivity. It replaces outdated RTU data concentrators, relay communication processors and other legacy integration devices and enables utilities to get more out of existing IED investments by helping them avoid unnecessary IED upgrades and replacements just to add new IED communication or security functionality.

SubSTATION Explorer is an HMI that revolutionizes the way electrical utility substations are maintained and operated today while transforming these traditional substations into tomorrow's smart substations. For personnel who manage electrical utility substations, SubSTATION Explorer is a software application that enables you safely, securely and reliably view and control all of your critical substation data.

PowerSYSTEM Center is a powerful multi-vendor, multi-function IED management solution. With PowerSYSTEM Center utilities are able to securely and centrally manage their large install base of many different intelligent electronic devices (meters, relays, RTUs, etc) deployed throughout their entire transmission and distribution system. Used by dozens of the largest T&D companies in North America for NERC CIP IED access control, PowerSYSTEM Center is a multi-function IED management solution that supports several additional functions including: unified relay event file collection and archiving, unified password management, unified asset monitoring and unified data historian interfaces.

SUBNET™
SOLUTIONS INC.

For More Information

For more information on the Cisco Connected Grid portfolio of products, visit *www.cisco.com/web/strategy/energy/external_utilities.html*.

For more information on SUBNET's portfolio of products, visit *www.SUBNET.com*.