21, rue d'Artois, F-75008 PARIS
http://www.cigre.org

CIGRE US National Committee
2019 Grid of the Future Symposium

Cybersecurity Considerations for Power Substation SCADA Systems Using IEC-61850 Communications

Matt Cole, PE and Jeff Pack, CISSP
3 Phase Associates, LLC and POWER Engineers, Inc.
USA

SUMMARY

Because of recent cyber-attacks and threats against power utilities, cybersecurity continues to increase in importance and be on the minds of substation design engineers.
One major concern for power distribution utilities is "ensuring that all communication protocols performing control functions and data acquisition for substations are properly secured. With IEC-61850 being one of the most widely used communications protocols by utilities today, particularly in distribution automation (DA)," increases the need for greater security in communication protocols. [1]

IEC-61850 is also becoming the preferred standard for substation design and operations due to the common framework and object-oriented design for point names as well as the increased performance and lower lifecycle cost of SCADA systems utilizing the methodology and protocols. This paper will discuss major vulnerabilities and cybersecurity considerations that require proper analysis when designing and implementing a secure IEC-61850 standard-based SCADA system within a power substation.

When including security controls into a SCADA system design, it is sometimes difficult to separate design goals from security requirements. The foremost goal for a SCADA system is to provide protection, automation, and data acquisition. The security controls must support the SCADA system design goals and not become the entire focus of the design.

Major areas of interest include the security of the Ethernet cable plant and switching equipment, the access controls at layer 2 of the OSI network stack, network latency for protective relay messaging, and network intrusion detection and prevention. Adding additional network resiliency by implementing redundancy protocols, such as, parallel redundancy protocol, and high availability seamless redundancy protocols will also be discussed.

KEYWORDS

SCADA, IEC-61850, cybersecurity, Ethernet, cyber resilience.

INTRODUCTION

With the prediction of many more digital devices being connected to the Internet over the next few years, cyberattacks and the focus on cybersecurity protection will forever increase.

Despite recent increases in cybersecurity spending across many businesses and industries, cyberattacks and security breaches still occur at a higher rate. Adversaries continue to use more sophisticated and clever techniques in penetrating an entities secure network.

Critical infrastructures are the key systems and necessary facilities required to serve public, private and government sectors in order to keep a society and its economy moving forward. Critical infrastructures are the primary essential functions required for nations and cities to maintain health, safety, order, freedoms, business, and government. Major disruptions to any nation's critical infrastructure, like the electric power grid, can create havoc, chaos, and death. Cities can be debilitated if key important elements in an infrastructure become inoperable through acts of sabotage, terrorism, or natural disasters.

Venezuela experienced a nationwide power outage earlier this year that nearly affected the nation's entire grid. This caused complete blackouts in almost 18 of Venezuela's 23 states. It left some states without power for weeks, causing loitering, chaos, and even death; mostly due to many failed black start attempts to restore power. A humanitarian crisis and state of emergency was declared due to an inadequate supply of life's necessities – food, water, transportation, electricity, lights, etc. Although the root cause of this extreme power outage is still under investigation, it is suspected that a well-planned sabotaged, cyberattack infiltrated their Internet, telecommunications, and electrical grid infrastructures. Investigators believe that Venezuela's power grid lacked maintenance upgrades of legacy and failing equipment, which added to the failed restoration efforts. [2]

Critical infrastructure protection (CIP) is planning ahead by preparation and being ready to respond to any major incident or catastrophe that may disrupt or affect a critical infrastructure of a nation, city, town, or region. [3]

"Today, any cyber incident has the potential to disrupt energy services, damage highly specialized equipment, and threaten human health and safety." As enemy states and cyber criminals continue targeting energy systems, the federal government must aid in lowering security risks in hopes of preventing a largescale or lengthy energy interruption. This primary goal is the uppermost national priority in defending America's energy grid against all cyber incidents. [4]

One of the most important and critical components of a utilities' power system is its substation.

Power substations play a vital role in controlling, transferring, and delivering electric power to end users and are equipped with several smart devices, such as intelligent electronic devices (IEDs) and supervisory control & data acquisition (SCADA) systems, that monitor and control the power flow.

As more smart devices continue to be added in substations with connections to SCADA, "cyber resiliency continues to become a greater challenge due to the ever-increasing cyberattack surface." [1]

"Today, with the demand of Smart Grid (SG) and Distributed Generation (DG) becoming more popular by adding more 3rd party connections and vendor renewable resources to power utilities' electric grid, this adds more stakeholders, users and interfaces to existing legacy SCADA systems. These existing or legacy SCADA systems were not manufactured to handle these new business decisions within the power sector compared to today's newer SCADA technologies.

Additionally, these older and legacy SCADA systems were not built with robust security controls in mind, since in the past, the design philosophy centered more around reliability and operations rather than security. In light of the increased cyber threats facing electric utilities today, SCADA systems are one of the greatest threats. The first cyber-attack on Ukraine's power grid in December 2015, for the most part, infiltrated a legacy SCADA system (via spear phishing emails and data loggers) that allowed full access to the operation of 30 substations via remote terminal units (RTUs), ultimately de-energizing power circuit breakers that interrupted the power to over 250,000 users for up to six hours. The second cyber-attack against Ukraine, which happened approximately one year later," was a different and more severe incident, affecting their transmission network by the attacker using a CRASH Override framework, which surprisingly caused less outages to customers. [5]

IEDs in substations have helped power operators and technicians utilize more real-time data in order to better operate, control, manage, monitor and test their power grid. "Advances in high-speed communication technologies have made it possible for utilities to operate their system by using automation, allowing for faster and more consistent decision making. With all the various devices interconnected together and serving the common goal of providing robust and more reliable power, it's important to have a common high-speed communications language protocol that is secure and that all devices understand." [1]

Main Benefits of a Substation SCADA System

Power substations are continuously being designed and upgraded with newer IED microprocessor devices that provide more real-time controls and monitoring. The substation local area network (LAN) allows local communications between all IEDs and smart devices, including SCADA systems, with the use of ethernet switches. The station LAN also connects to the main router for allowing two-way communications outside the substation onto a wide area network (WAN).

Power operators continue to depend on SCADA as the backbone for the smarter grid, both for substation automation (SA) and distribution automation (DA) functions. Newer SCADA systems provide more robust, more real-time, and better remote-control functionality with the use of advanced communication protocols. A SCADA system "is a thriving technology that has helped various industries, such as: electric utilities, telecommunications utilities, oil & gas suppliers, water/waste utilities, transportation, manufacturing, and others improve their overall control of intelligent systems. SCADA has helped them better supervise, manage, monitor, and control their critical infrastructure." [5]

There are many reasons that provide several benefits for implementing SCADA systems, such as:

1. Allows remote control functionality
2. Provides alarming of system abnormalities
3. Provides real-time operations
4. Produces real-time metering data
5. Capable of performing automation functions
6. Performs data collection and calculations
7. Allows several reporting options for event history and trending
8. Increases system reliability along with improved customer satisfaction
9. Allows for reductions in equipment and labor maintenance costs
10. Streamlines processes for improving efficiencies

For power utilities, SCADA systems "have played a crucial role in helping deliver reliable and safe power to its customers. Over the last few decades, implementing SCADA systems has been a forefront in the requirements for many electric utilities in allowing their power operators, engineers, management, and users' enhanced visibility with more data sets to allow for better decision making." [5]

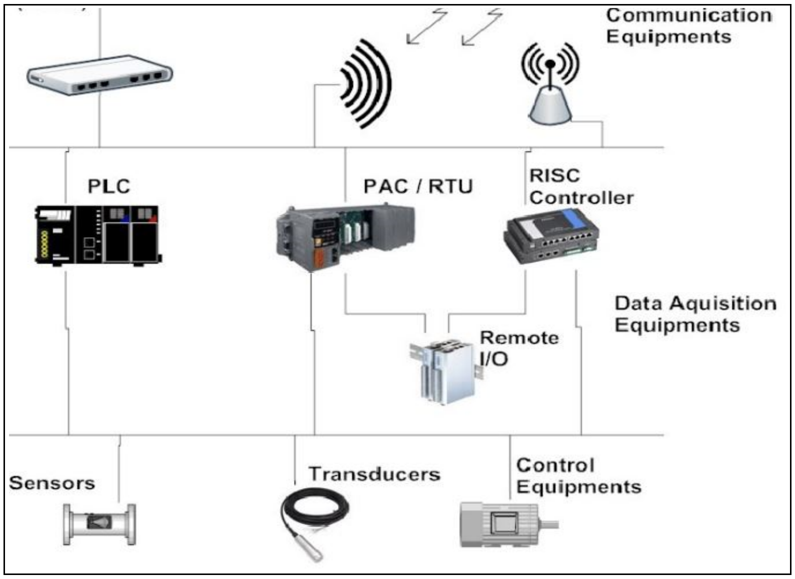

Figure 1: Typical SCADA System Network Diagram [6]

Main Benefits and Uses of Using IEC-61850 for SCADA Systems and/or Substation Control

To meet the growing demand of the data driven burden on SGs and automation, standard protocols such as IEC-61850 and others are being improved for the future. As the hardware innovations are sprinting to keep pace with advances in software communications, more and more Internet protocol (IP) based equipment are being installed. Below is a list of some IP based equipment commonly installed in substations that use digital communications:

- SCADA Remote Terminal Units (RTUs)
- SCADA I/O Controllers
- Human Machine Interfaces (HMIs)
- IEDs and Programmable Logic Controllers (PLCs)
- Phasor Measurement Units (PMUs) and Synchrophasors
- Digital Fault Recorders (DFRs)
- Communication Processors and Smart Meters

These devices are each contributing data and functions that are integrated to help produce the SG. Looking closely at the list of devices above will reveal that it is very common for a vendor to produce most, if not all of this equipment, and in any given substation it is very uncommon to find all of the equipment produced by the same vendor.   Having multi-vendor equipment at a substation, as an A (primary) and B (backup), improves reliability by reducing the probability of a vendor specific error being present on both sets, but creates a more complex environment for overall communications and life cycle maintenance. IEC-61850 "supports interoperability between vendor systems and IEDs" attempting to make this environment less complex. [7, 8]
IEC-61850 protocol has become widely used in the US and Europe for SCADA Systems, SA, DA, SG, and Protection & Controls (PRC). IEC-61850 provides ease in communicating and issuing commands with many other systems, like: SCADA systems, protective relays, IEDs, HMIs, PMUs, PLCs, etc. IEC-61850 is considered as an easier protocol to implement with SCADA in comparison with other protocols. IEC-61850 also eliminates the need for proprietary vendor protocol converters. Because IEC-61850 uses an object oriented data hierarchy, it allows for reliable, high priority network messaging and smooth data exchanges with SCADA systems and others. This provides the perfect combination in substations for both SCADA control and PRC. Using IEC-61850 as the main communications protocol for SCADA presents cost savings for the substation design, installation, commissioning, and operations compared with other, less popular protocols. IEC-61850 is also the preferred protocol for communicating outside the substation when compared with other proprietary vendor protocols.

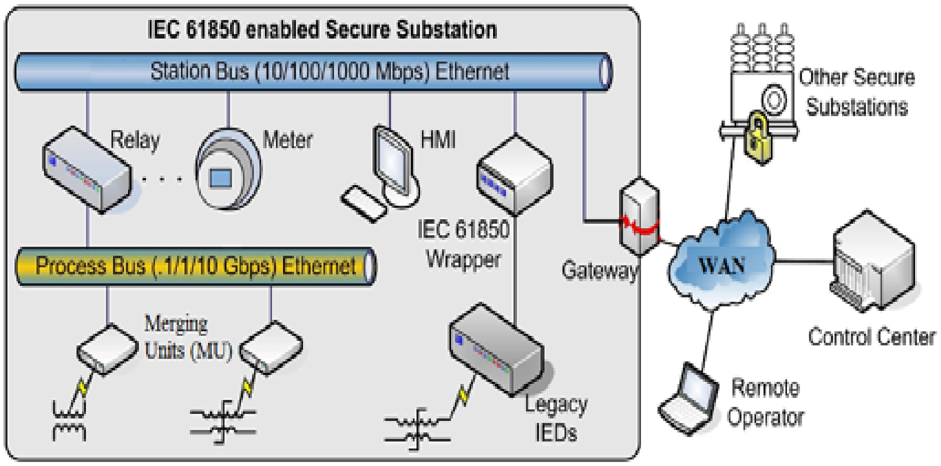

Figure 2: IEC-61850 Substation Architecture [7, 8]

Although, using IEC-61850 with SCADA systems in a substation as the main protocol presents many benefits, there also remains several cyber vulnerabilities if not designed and configured properly. For example, in substations, “a maliciously or erroneously misconfigured CT or PT ratio can cause trips in the presence of normal currents, or failure to trip in the presence of fault currents. One of the major possible attack surfaces under the IEC-61850 substation architecture is the process bus, where the measurement data along with other process related control commands are communicated. Since the protection relays and IEDs operate based on the measurement data from the process bus, a successful data injection attack at the process bus can result in nuisance tripping and blocking of breakers, causing denial of service (DOS) to customers or damage to substation equipment or hazard to personnel” [7, 8]

Possible Cybersecurity Vulnerabilities with Using IEC-61850 for SCADA Control

There are several areas within an IEC-61850 SCADA system that require additional attention regarding security.

The (1) first area to address is physical security of the system components. Without adequate physical security controls, the IEC-61850 SCADA system is perhaps even more vulnerable than a traditional SCADA system due to more intelligent electronic devices (IEDs) in use with more complex configurations, as well as the use of Ethernet networking for communications.

The (2) next consideration for a IEC-61850 SCADA system is the need for an Ethernet network, which for many substations in North America will bring additional NERC CIP External Routable Connectivity requirements into scope. These requirements will add additional processes and cost to the IEC-61850 SCADA system.

Another (3) significant security issue for the IEC-61850 SCADA system is device access control. In many cases, the focus of cyber security for SCADA systems has been on the network and application layers. There is an assumption that the IEDs and other sensors are secure (uncompromised), accurate, and authenticated which may not be the case. Another (4) issue is the organizational silos of multiple functional areas affected by process sensors including cyber security, safety, alarm management and device management organizations [9].

The IEC-61850 communications protocols depend on Ethernet to perform properly, but rogue or unauthorized devices on the Ethernet network may introduce significant traffic and create a denial-of-service condition for protection messaging. Virtual LAN (VLAN) membership and/or multicast filtering is an important device access control and traffic management tool that is useful in IEC-61850 due to the nature of GOOSE messaging and the publisher-subscriber model.

(5) User access control is also an important security control. Many utilities have user access controls that are unique to the Operational Technology (OT) network. Remote engineering access is also common in modern SCADA systems to increase efficiency and automation. Proper authentication and authorization is critical for maintaining configuration and change management for SCADA systems.

Cyber Security Recommendations when Using IEC-61850 within a Substation Environment

Physical access control to the control house should be standard procedure for all substations, but additional physical access controls inside the control house include locking cabinets for the Ethernet switches to prevent adding devices to the switch or changing cable connections on the physical switchports. The Human Machine Interface (HMI) is another potential access point with significant risk, so adding physical access control to the HMI (lockable rack or cabinet) is also recommended.

Ethernet port security should be configured on the Ethernet switches to only allow known devices to connect to each switch. This is typically done through the port security settings.

Another similar control can be done with the virtual LAN (VLAN) configuration. For GOOSE messaging, the best performance is achieved when devices that subscribe to GOOSE messages are members of a "GOOSE VLAN" that only shares Ethernet frames with members of that VLAN. Use the VLAN Membership functions to control which devices belong to the VLAN. The same functionality can be done with multicast filtering – only allowing GOOSE MAC addresses to be shared as a multicast frame.

For all IEDs and SCADA, disable all unused ports, services, and unnecessary local user accounts and change the default passwords on the required device accounts. Use strong passwords for all accounts, especially local user accounts that have elevated privileges. Use centralized authentication services such as RADIUS, LDAP or Active Directory for all user accounts on devices that support such services.

All remote access should use an intermediate system with multi-factor authentication and encryption of network traffic between the remote host and the intermediate system. The intermediate system acts as a proxy to limit direct access to IEDs from external hosts and protect the IEDs from possible vulnerabilities on the remote host.

At the transport layer, all applicable controls that are required for externally routable communications are also required for IEC-61850. In particular, a stateful inspection firewall that understands the Manufacturing Message Specification (MMS) protocol for transporting information from an RTU to an Energy Management System (EMS) or Distribution Management System (DMS) would be prudent for detecting malicious traffic masquerading as MMS information.

The NIST Guidelines for Smart Grid Cybersecurity provide a comprehensive reference for substation and SCADA design engineers that want to develop a security program for all aspects of power substation design and implementations [10].

Recommendations for Improving Cyber Resiliency when using IEC-61850 in SCADA Designs

Due to the importance of the network infrastructure in an IEC-61850 SCADA system, the ability for the network to recover from a failed component is very important. There are several design choices and enhancements that can improve the resilience of the network.

The (1) first mechanism that can be used is Rapid Spanning Tree Protocol (RSTP). With a wise choice of topology and implementing advanced features, the convergence time of RSTP when losing a link between two switches will be less than one second. Larger networks may increase the convergence time due to the need for all switches to receive bridge protocol data unit frames. For many SCADA solutions, this is an acceptable solution since traditional SCADA systems that use a client-server model can withstand a recovery time in the hundreds of milliseconds [11].

(2) When using GOOSE messaging on the station bus or sampled values on the process bus for IEC-61850, the availability requirements for communications are significantly higher. For sampled values, a "bumpless" recovery time is a requirement. This requirement leads most SCADA system designers to specify one of the mechanisms defined in the IEC 62439-3 Standard – parallel redundancy protocol (PRP) or High-Availability Seamless Redundancy (HSR).

PRP provides two separate LAN connections per participating device. Any message that the device publishes is mirrored to both networks. Subscribing devices accept the first message and discard the second message. If one network link fails, the message is still seen by subscribers. One key aspect – the two networks must remain separate in order for the PRP design to work properly.

(3) HSR has a similar design except the topology for the network is a single ring, with messages published on each interface to transverse the rings in opposite directions. If a link between two members of the ring is broken, the message will still be received by all subscribers.

PRP requires two separate LAN systems and is seen as typically costing more for implementation. HSR in its simplest form requires no Ethernet switches – just communications cables between the members to facilitate the ring. However, HSR Ethernet frames are not compatible with standard Ethernet frames, so HSR is normally limited to related devices, such as all protective relays for a bus or feeder. For larger substation networks, a combination of HSR rings tied together with PRP networks is a good way to maximize the benefits of both architectures [12].

Conclusion

Since power delivery systems are considered as the main backbone of the US energy infrastructure, this is considered as a national security issue, especially in light of the past cyberattacks on Ukraine's and Venezuela's power grids'. A reliable and robust power system "is the cornerstone of our advanced digital economy and is essential for critical operations in transportation, water, communications, finance, food, agriculture, emergency services, and more." [4] As cyber threats continue to rise with no foreseen end in sight, the vulnerabilities with smart and critical substations must be mitigated to prevent future attacks. With the IEC-61850 protocol being one of the global standards and most widely used communication protocols of the future in SG, SA, DA, and use with SCADA systems, cybersecurity enhancements must continue to improve for IEC-61850 in order to reduce the attack threat as IEC-61850's usage with SCADA systems increases with upgrading to the modernized grid. [5]

This paper exposes the main vulnerabilities and provides recommended security considerations to follow in order to prevent and help rule out cyber vulnerabilities when using IEC-61850 as the main communications protocol with a station's SCADA system and other smart devices.

BIBLIOGRAPHY

[1] R. Arnold, J.M. Cole, and M. LaCourt, “Cybersecurity Challenges of Implementing IEC-61850 for Automation Between the Smart Distribution Control Center and the Substation,” CIGRE US National Committee, 2017 Grid of the Future Symposium, Cleveland, OH, October 22-24, 2017.

[2] T&D World, “Venezuela Plugs In Again after 19-Hour Outage,” Smart Utility/Outage Management, March 13, 2019. https://www.tdworld.com/outage-management/venezuela-plugs-again-after-19-hour-outage

[3] Wikipedia, “Critical Infrastructure Protection,” www.wikipedia.com.

[4] U.S. Department of Energy., “Multiyear Plan for Energy Sector Cybersecurity,” March 2018, www.energy.gov.

[5] J.M. Cole, “Is Your Legacy SCADA System Secure?” 3 Phase Associates – White Paper, October 7, 2018. https://3phaseassociates.com/is-your-legacy-scada-system-secure/

[6] Georgescu, Vlad-Cristian, "Optimized SCADA systems for electrical substations," pages 1-4. 2013 Conference: Advanced Topics in Electrical Engineering (ATEE).

[7] A. Aksoy, J. Bridges, J.M. Cole, F. Napier, “Methods for Reducing Cybersecurity Vulnerabilities of Power Substations Using Multi-Vendor Smart Devices in a Smart Grid Environment,” CIGRE US National Committee, 2017 Grid of the Future Symposium, Cleveland, OH, October 22-24, 2017.

[8] R. Macwan, C. Drew, P. Panumpabi, A. Valdes, N. Vaidya, P. Sauer, “Collaborative Defense Against Data Injection Attack in IEC61850 Based Smart Substations.” (Information Trust Institute).

[9] J. Weiss, “A Grim Gap: Cybersecurity of Level 1 Field Devices and lack of appropriate OT Expertise,” ControlGlobal, https://www.controlglobal.com/blogs/unfettered/a-grim-gap-cybersecurity-of-level-1-field-devices-and-lack-of-appropriate-ot-expertise/

[10] National Institute of Standards and Technology, “Guidelines for Smart Grid Cybersecurity,” NISTIR 7628 Revision 1, September 2014. https://nvlpubs.nist.gov/nistpubs/ir/2014/NIST.IR.7628r1.pdf

[11] R. Hunt and B. Popescu, “Comparison of PRP and HSR Networks for Protection and Control Applications,” Western Protective Relay Conference, Spokane, WA, October 20-22, 2015.

[12] E. Huang, “Deploying Integrated and Scalable Ethernet Redundancy with PRP/HSR,” Moxa, Inc., 2015.