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

CIGRE US National Committee
2017 Grid of the Future Symposium

Cybersecurity Challenges of Implementing IEC 61850 for Automation Between the Smart Distribution Control Center and the Substation

J. M. COLE
Sargent & Lundy LLC
USA

M. LACOURT
Sargent & Lundy LLC
USA

R. ARNOLD
Sargent & Lundy LLC
USA

SUMMARY

Every time you turn on the news or pick up a newspaper, something is getting hacked. Businesses, banks, hospitals, governments, and other entities continue to get breached by attackers. Cybersecurity and the protection of sensitive data continue to be on everyone's mind, particularly the electric power industry especially in light of the recent Ukraine cyber-attack that happened on December 23, 2015. This "cyber-incident that hit the Ukraine Power Distribution Utilities' grid was considered as the first power interruption to take place from a well-planned, cyber-attack" [1]. This event caused interruptions to over 225,000 customers for up to six hours and left Ukraine's utility operators feeling helpless. This cyber-attack along with others has increased cybersecurity awareness but will it be enough to force utility regulators, policy makers and standards' developers to increase security protection for all power utilities, including distribution utilities? 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), this paper focuses on the resiliency of IEC-61850 along with NERC CIP's mandates and other standards according to 61850 and recommends key security enhancements to be implemented in order to reduce the overall attack surface.

KEYWORDS

Communication system security, IEC-61850, IP networks, Substation automation, Distribution Automation.

Joseph.M.Cole@SargentLundy.com

1. INTRODUCTION

"The North American Electric Corporation (NERC) created its Critical Infrastructure Protection (CIP) Standards under the jurisdiction of the Federal Energy Regulatory Commission (FERC) in order to prevent possible cyber-attacks to the Bulk Electric System (BES). NERC's primary mission enforces its CIP Standards upon generation and transmission utilities regulating them to harden their critical cyber assets (CCAs) that connect to a routable Internet Protocol (IP) against potential hacking vulnerabilities" [2]. NERC, along with others, have been studying the Ukraine attack in order to learn from this event and revisit its standards.

"The most recent NERC CIP Version 5 (V5) standards currently in affect do not include regulations for power distribution utilities. With no CIP standards or federal governing entities controlling the distribution utilities against cyber-attacks today, the greatest fear is that several power distribution utilities in the U.S. and Canada could be less secure and more vulnerable than Ukraine on December 23, 2015" [1]. NERC views the distribution power voltage levels as of no concern or to have "no impact" on the BES [1]. Due to the Ukraine attack, similar CIP mandates or state regulations could be enforced in the near future for distribution utilities.

Another obstacle facing distribution utilities, but also beneficial, is the need for more automation. For the past several years, distribution utilities have been performing substation and control center upgrades towards a copper-less environment by replacing several hardwired devices with higher performing, state-of-the-art microprocessor based devices that implement automation and utilize fiber optics communications for better, faster, and more reliable communications interfaces. With Smart Grid (SG) and Distributed Energy Resources (DER) taking center stage in the electric power industry, these functions are requiring higher bandwidth and more secure peer-to-peer communications. As more Smart devices are added with newer innovative technologies performing real-time operations, cyber resiliency continues to become a greater challenge due to the ever increasing cyber-attack surface.

Additionally, utility operators are constantly requiring more real-time operations data in order to better automate, manage, operate, control, monitor and test their power system. 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 reliable power, it's important to have a common high speed communications language protocol that is secure and that all devices understand. "The success of a Substation Automation System (SAS) relies on the use of an effective communication system to link the various protection, control, and monitoring elements within a substation" [3]. "Thus, the resulting overall power system must be an open interoperable and connected system to allow the necessary amount of access between participating parties like devices in the grid but also market stakeholders. Only then, a smart evolution of the power system is possible. An open system, in turn, needs standardization to fulfill several interoperability requirements and to be run in an efficient way. Without standardization e.g. in terms of data models and interfaces the costs for integration of components as well as applications would be enormous" [4].

IEC-61850, created by the International Electro-technical Commission (IEC) Technical Committee 57 (TC57), has made several breakthroughs with continuous improvements and standard revisions over the years allowing for more robust peer-to-peer communications with intelligent electronic devices (IEDs) and other Smart devices between substations and control centers. "The major challenge faced by substation automation design engineers is to provide interoperability among the protection, control, and monitoring devices from the various manufacturers" [3]. IEC-61850 is capable of communicating with several multi-vendor devices within substations and control centers. "IEC-61850 based Smart substations have played a significant role in Smart Grid operation, becoming increasingly complex and interconnected as state-of-the-art information and communication technologies (ICT) are adopted. The increased complexity and interconnection of supervisory control and data acquisition (SCADA) systems have exposed them to a wide range of cybersecurity threats, which may lead to catastrophic physical damage" [5]. IEC-61850 is meeting today's DA challenges faced in Smart control centers

and substations, but is, however, becoming increasingly exposed to more cyber vulnerabilities both in the substation and Smart control center.

A "Smart Distribution Control Center (SDCC) is characterized by the function and operational capabilities of the center and is comprised of an increased reliance on data acquisition, software, and automation" [1]. With the SDCC being the heart and soul for operating and controlling the more modernized grid, cybersecurity challenges increase with the added number of connected cyber devices [1]. Figure 1 shows the SDCC along with functional operation blocks, derived from NIST's Guidelines for Smart Grid Cybersecurity [6]. Figure 1 also shows the typical operations of an SDCC enclosed within the dashed box. Communication links connecting each function block represents the physical flow of data that can occur within or outside the Smart control center to other applications. If IEC-61850 is being used for communications outside the SDCC or substation, what security measures should be taken to ensure safe and reliable operations of the SG?

This paper will review the latest NERC CIP-005-5 standards for the Electronic Security Perimeter (ESP) as it applies to cybersecurity enhancements for IEC-61850 protocol communications between the substation and SDCC, while comparing to other standards such as IEC-62351-1 and NIST-7628. Although CIP-005-5 does not apply to distribution utilities, this paper will emphasize possible security vulnerabilities using IEC-61850 protocol communications outside the substation for substation automation (SA), particularly SCADA systems, and recommend improvements to be performed for enhancing cyber resiliency for distribution utilities. Although there are other protocols used by utilities in SA, SG and DER, (e.g. DNP3, Modbus, etc.), this paper will concentrate on the IEC-61850 protocol.

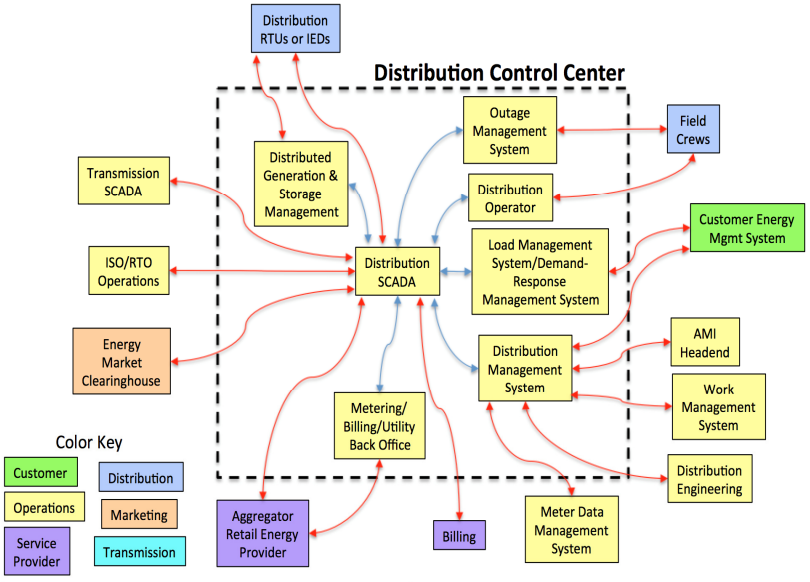

Figure 1: SDCC, Smart Grid Logical Reference Model [6]

2. MAIN BENEFITS OF IEC-61850

IEC-61850 has many benefits covering various industries. The list below shows the main benefits of IEC-61850 as used in the electric utility industry, particularly power distribution utilities as it relates to power distribution control centers and substations.

- Widely used protocol in Europe & US for protection & controls (PRC) and SA
- Eliminates hard wiring/uses less copper
- Provides cost savings for substation designs, installations, commissioning and operations
- Easier to implement/ease of use compared to other protocols
- Smooth data exchanges with multi-vendor devices
- Eliminates the need for special vendor proprietary protocol converters
- Provides reliable, high priority network messaging
- Capable of providing real-time data and control between control centers and substations
- Uses an object oriented data hierarchy

3. USING IEC-61850 FOR CRITICAL COMMUNICATIONS OUTSIDE THE SUBSTATION

Utility operators and power engineers are demanding much more real-time functionality from substation Smart devices. The substation local area network (LAN) has made it possible to communicate with local devices as well as remote devices outside the substation and that reside at the SDCC. "The station LAN connects all of the IEDs to one another and to a router or other device for communicating outside the substation onto a wide area network (WAN)" [7].

With NERC CIP's increased focus of protecting critical cyber assets (CCAs) from a cyber-attack, how secure are the LANs that distribution substation devices are connected to while performing IEC-61850 communications outside the ESP? When implementing substation and communications designs, "consideration should be made to ensure that failed or attacked networks affect as few devices as possible and designers need to choose IEDs that will continue to function if they reside on a failed or attacked network" [7]. Critical functions must be implemented, maintained and protected against an attack.

Since SCADA is one of the most common critical functions used for DA and SA, it communicates outside the substation to the SDCC's master SCADA system via the WAN, allowing operators to send real-time remote control commands. Today, many IEDs are performing real-time SCADA functions using IEC-61850 that only a few years ago were limited to Remote Terminal Units (RTUs) alone. Figure 2, shows a typical substation network with connected devices, such as IEDs, HMI, Merging Units (MUs), metering, etc., all capable of performing IEC-61850 communications within a substations' LAN and outside via a Gateway/WAN.

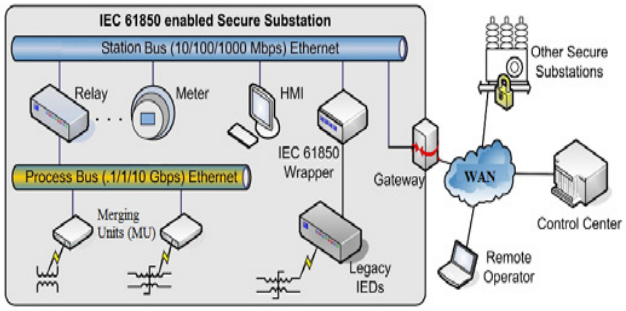

Figure 2: ***IEC-61850 Substation Architecture*** **[8]**

When using IEC-61850 protocol for critical control functions, what major security risks do 61850 communications pose for SCADA systems outside the substation's ESP? What enhancements need to be made to ensure 61850 is fail proof against future cyber threats?

4. SECURITY VULNERABILITIES FOR IEC-61850 COMMUNICATIONS BETWEEN THE SDCC AND SUBSTATIONS

IEC TC57 created a series of specifications and recommendations to address the security of communication protocols, which encompasses IEC-61850 among others. TS 62351-1 states:

"These protocols are now widely used in the electric power industry. However, they were developed before information security became a major issue for the industry, so no security measures were included in the original standards" [9].

To compensate for this shortcoming in IEC-61850, IEC-62351 was created. IEC-62351-1 defines four vulnerable areas of cyber system that require protection:

1. Human-Machine Interface
2. Software Applications in Computer Systems
3. Communications Transport Protocols
4. Communications Media [9]

Due to the remote nature of substations, it is necessary for the traffic to leave the secure Physical Security Perimeter (PSP) and ESP of the substation in order to travel to the PSP and ESP of the SDCC. During this time, it is critical that the vulnerable areas listed above be appropriately protected.

In order to keep the security protection reasonable, a security risk assessment is recommended for all assets. Although making every asset impenetrable may be ideal, in practice it is not practical or cost effective. The security risk assessment should weigh the costs installing and maintaining particular security measures against the cost or damage incurred due to a security breach. In terms of practical security, a one sized design does not fit all applications [9].

The two key recommendations made by IEC-62351 regarding control center to substation communications via IEC-61850 are authentication and encryption. The use of Transport Layer Security (TLS) is recommended to provide end-to-end protection. This will provide authentication and, in the case of Manufacturing Message Specification (MMS), encryption. It is not recommended to use encryption for Generic Object-Oriented Substation Events (GOOSE), Generic Substation Events (GSE), or Sampled Measured Values (SMV) due to the latency introduced into the packet transmission. IEC's recommendation for these is authentication only. These three message classes are not routable and are not intended to communicate beyond the substation LAN.

However, "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/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/blocking of breakers, causing denial of service (DOS) to customers or damage to substation equipment or hazard to personnel" [8]

4.1. NERC CIP REGULATORY COMPLIANCE FOR USING IEC-61850

The CIP V5 transition program offered a document on frequently asked questions (FAQ) in order to aid utilities on their previous CIP V5 upgrades. Shown in the FAQ below is item number 23 that discusses whether IEC-61850 is considered to be a routable protocol. Taken from NERC, it states:

"IEC 61850 is an Ethernet-based standard for the design of electrical substation automation and the abstract data models can be mapped to a number of protocols, including MMS (the underlying communication architecture for ICCP), GOOSE, and Web Services. IEC 61850 is not a data link or network layer protocol, thus declaring IEC 61850 to be a routable or non-routable protocol is not appropriate. Time-critical messages, such as GOOSE messages for direct inter-bay communication, typically run on a flat Layer 2 network without the need for Layer 3 IP addresses. Other non-time-critical messages, including MMS and web services, typically run on a Layer 3 network, such as TCP/IP, with addressing and routing. The registered entity should carefully evaluate the communication environment supporting the IEC 61850 data protocol to determine if routable communication exists. If the IEC 61850 data is being communicated over a TCP/IP network, then that network connectivity is considered routable and should be protected per the CIP Standards accordingly. Note: Low impact requirements exempt 61850 from its scope" [10].

Since CIP V5 considers 61850 as being exempt and not in scope for low impact or distribution utilities, this paper recommends adding security protection to IEC-61850 especially for external routable communications outside a distribution substation. The communications between the SDCC and substation consists of MMS and web services, both of which are routable communications. Even though 61850 can be packaged or tunneled through SONET systems before leaving the substation, NERC CIP-005-5 considers this as outside the scope or as non-routable and therefore not requiring protection. This paper recommends adding security for distribution utilities that use 61850 communications outside substations, whether routable or not and whether included in CIP-005-5 scope or not, in order to reduce the overall cyber-attack surface.

4.2. NIST STANDARD FOR USING IEC-61850

The NIST Guideline for Smart Grid Cyber Security, NISTIR 7628, has defined IEC 61850 as an insecure protocol [6]. This needs to be taken in to consideration when specifying the Operational

Technology (OT) architecture. The substation ESP ends at the substation firewall or demilitarized zone (DMZ) and the SDCC ESP ends at the SDCC firewall or DMZ. As such, the WAN in between is most vulnerable to outside intrusions. The gateway to the substation's ESP, as established in CIP-005-5, is classified as the Electronic Access Point (EAP). This is similar to and is usually the substation's firewall, which requires inbound and outbound access permissions/restrictions, including the reason for granting access, and denies all other access by default [11]. The EAP firewall will perform authentication, usually through an IP security protocol through a Virtual Private Network (VPN). TLS (the successor to Secure Shell - SSH) or SSH are also acceptable forms of security. By securing and monitoring inbound and outbound traffic, the risk of an outside attack is greatly reduced.

5. SECURITY CHALLENGES FOR IEC-61850 COMMUNICATIONS FROM THE SUBSTATION TO THE SDCC

Ideally, a substation to SDCC communication link is transported by a utility's closed private network or WAN directly from the substation to the SDCC, either via fiber, microwave, or a licensed and encrypted radio. Often times, utilities are not able to implement their very own private networks and frequently rely on outside entities for providing this communication path to the SDCC. This is due to limited budgets, lack of real estate ownership, right of way (ROW) access, and/or limitations of their telecommunications infrastructure. Outside entities can include neighboring utilities with spare dark fiber, telecommunications companies providing leased circuits, cellular or satellite wireless connections, or wavelength division multiplexing over shared networks with other entities, etc. How does the utility owner know the communication supplier values cybersecurity protection of its data as if it were their own?

6. RECOMMENDATIONS FOR ENHANCING IEC-61850 FOR CYBER RESILIENCY

The following list is a combined summary from NERC, IEC, and NIST of the recommended devices and technologies for cybersecurity enhancements of IEC-61850 and substation communications in general.

- TLS Encryption
- User/Device Multi-Factor Authentication
- Firewalls/Gateways/DMZs
- Intrusion Detection/Prevention Systems (IDS/IPS)

Encryption is recommended to be enabled between the end devices, where possible, for the most effective level of protection. A properly encrypted communication channel should be able to prevent eavesdropping by another entity or adversary.

The use of user and device authentication will further the resiliency of the communications link. Authentication will prevent unauthorized access or modification of information, and will hold the appropriate users accountable for breaches that may occur through their accounts [9].

These encryption and authentication services between the SDCC and substation can be provided by Ethernet firewalls, gateways, and DMZs installed at each location. These devices will define the ESP at the site to protect the smart devices contained within it. The firewalls should be configured to deny all unanticipated traffic by default.

To further the security and visibility of the communications link, an IDS/IPS should be installed. The IDS will monitor the network traffic and log unexpected device traffic.

Figure 3 below shows how a distribution substation LAN should look after adding the recommended security improvements for protection against future cyber threats, especially when using 61850 outside the substation.

7. CONCLUSION

With cyber threats on the rise and no foreseen end in sight, power distribution utilities should remain

focused on the latest threats and vulnerabilities along with their remedies. NERC, IEC, NIST, and other entities will increase their focus on enhancing regulations and standards for continuously improving cybersecurity protection in hopes of preventing another future Ukraine-like attack.

Although NERC today views distribution utility voltage levels as having no impact on the reliability of the BES and CIP-005-5 views the routable protocols that communicate outside the distribution's ESP as being out of scope, this could change in the near future. This paper reviewed other standards from IEC and NIST for examining the possible vulnerabilities when using IEC-61850 protocol for communications outside the substation. When 61850 is performing SA for SCADA control while communicating between the substation and the SDCC, all unencrypted data is at risk. Also the substation LAN is vulnerable if firewalls, gateways, IDS/IPS and DMZs are not implemented at each ESP penetration or EAP especially when the utility is relying on other entities for leased communications between the substation and the SDCC.

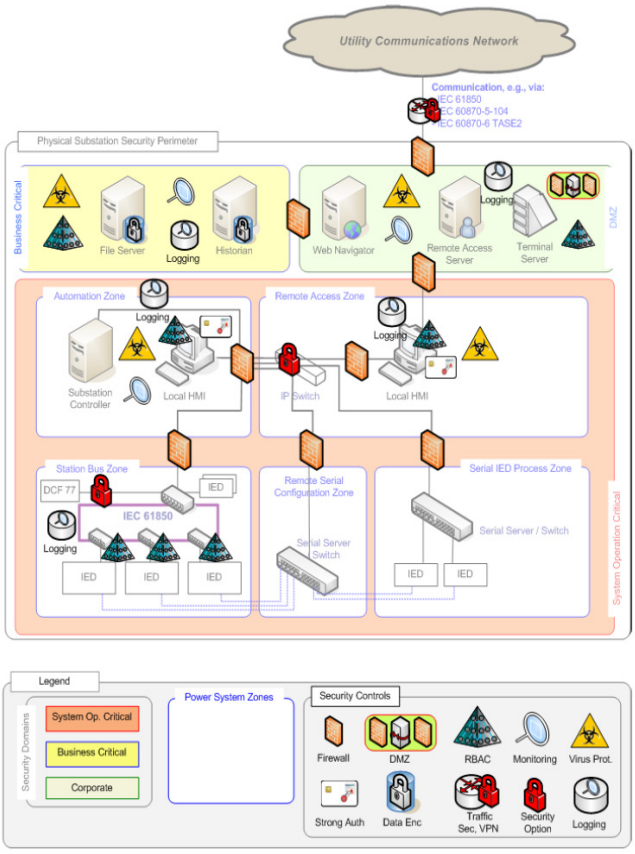

Figure 3*: IEC-62351 Recommended Substation Protections* **[12]**

Along with installing gateways, DMZs and IDS/IPS, this paper also recommended implementing multi-factor authentication and encryption for all 61850 communications outside the ESP through the WAN to the SDCC. Although applying these added security functions can be very costly, the cost of doing nothing, if attacked, can be considered as immeasurable.

With IEC-61850 being one of the global standards and most widely used communication protocols of the future in SG and other automated functions, cybersecurity enhancements for 61850 must continue in order to reduce the overall attack surface as 61850's usage increases in the ever changing modernized grid.

BIBLIOGRAPHY

[1] J. Cole and N. Wallace, "Applying NERC CIP Standards to Power Distribution Utility Control Centers to Enhance Cybersecurity within a SMART and Automated Environment." (CIGRE 2016).

[2] J. Cole, "Challenges of implementing substation hardware upgrades for NERC CIP version 5 compliance to enhance cybersecurity." (210 IEEE, Power Engineering Society Transmission & Distribution Conference, pp 1-5).

[3] T. Sidhu, M. Kanabar, and P. Parikh, "Implementation Issues with IEC 61850 Based Substation Automation Systems." (Fifteenth National Power Conference, IIT Bombay, 2008).

[4] S. Lehnhoff, W. Mahnke, S. Rohjans, and M. Uslar, "IEC 61850 based OPC UAS Communication – The Future of Smart Grid Automation." (17th Power Systems Computation Conference, Stockholm, Sweden, August 2011).

[5] Y. Yang, K. McLaughlin, L. Gao, S. Sezer, Y. Yuan, Y. Gong, "Intrusion Detection System for IED 61850 based Smart Substations." (IEEE, 2016).
[6] NIST 7628 "Guidelines for Smart Grid Cyber Security v1.0." 2010. [Online]. Available: http://www.nist.gov/smartgrid/upload/nistir-7628_total.pdf
[7] D. Dolezilek, "IEC 61850: What You Need to Know About Functionality and Practical Implementation." (SEL Journal of Reliable Power, Oct 2010).
[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] Power systems management and associated information exchange – Data and communication security Part 1: Communication network and system security – Introduction to security issues. (IEC TS 62351-1, 2007).
[10] NERC CIP Standards, CIP V5 Transition Program, 2014. [Online]. Available: http://www.nerc.com/pa/CI/tpv5impmntnstdy/CIPV5_FAQs_Consolidated_Oct2015_Oct_13_2015.pdf. page 8.
[11] NERC CIP Standards, CIP Version 5, 2013. [Online]. Available: http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx.
[12] Power systems management and associated information exchange – Data and communications security – Part 10: Security architecture guidelines. (IEC TR 62351-10, 2012).