Security Through Simplicity in Digital Substations

Joe Casebolt

INTRODUCTION

Distributed digital substations extend the digital boundary from the traditional border of the control house out to the primary equipment in the substation yard. Performing the analog-to-digital conversion at the point of measurement and carrying the digital information over fiber-optic cabling can create a safer working environment and lower operational costs. By transferring the information digitally, dangerous voltages can be removed from the control house. Material costs can be minimized by replacing hundreds of feet of copper lines with a single fiber-optic cable, which also reduces the physical footprint with smaller trench requirements. Labor costs can be reduced via less trench work, fewer wiring termination points, and a reduction in maintenance activity.

Figure 1 shows a traditional substation design. Modern installations like the one shown in Figure 2 rely on communications technologies and purpose-built devices to digitize the data and distribute it from the point of measurement to the electronic devices in the control house that perform the protection, control, and monitoring. IEC 61850 and SEL's Time-Domain Link Technology (TiDL™) are two options available for these kinds of communications services. This paper provides a brief overview of the two technologies and assesses the cybersecurity posture of each.

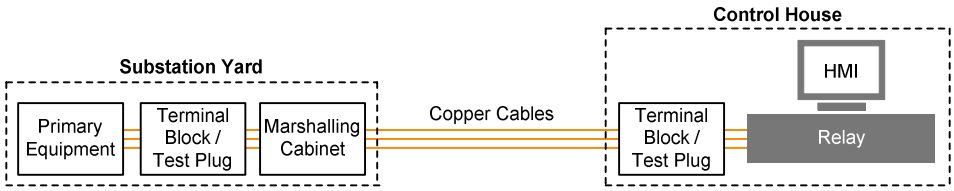

Figure 1 Traditional Substation Design

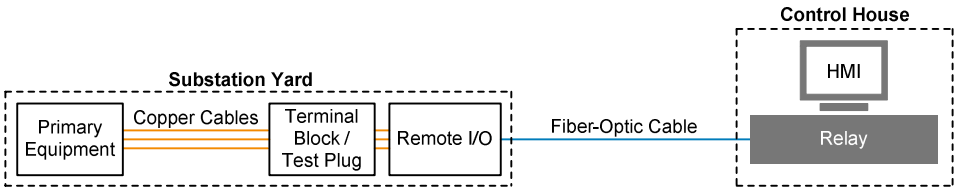

Figure 2 Modern Digital Substation Design

TECHNOLOGY OVERVIEW

Distributed digital substations require the communication of three basic types of information:

- Time – system time synchronization.
- Discrete I/O – discrete I/O measurement and control.
- AC inputs – ac instrument transformer measurements.

TiDL and IEC 61850 take distinctly different approaches to the network architecture and the communications methods to share information. TiDL uses private point-to-point connections to each device, whereas IEC 61850 uses a switched Ethernet network. In addition to the network architecture difference, the two technologies have different protocols to communicate the three basic types of information, as shown in Table 1.

Table 1 Communications Methods

Technology	Time	Discrete I/O	AC Inputs
IEC 61850	Not defined (Precision Time Protocol [PTP] identified as preferred method)	Generic Object-Oriented Substation Event (GOOSE)	Sampled Values (SV)
TiDL	EtherCAT®[1]	EtherCAT	EtherCAT

A TiDL solution uses a direct, point-to-point link between the relay and the remote I/O unit, as shown in Figure 3.

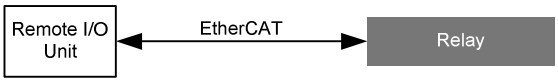

Figure 3 TiDL System With Single I/O Connection

When multiple I/O units are needed, each gets an isolated point-to-point connection, as shown in Figure 4.

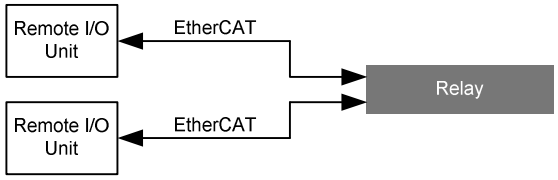

Figure 4 TiDL System With Multiple I/O Connections

An IEC 61850 solution uses the same types of devices but also includes an Ethernet switch and some method to distribute time to all of the devices in the network (a PTP solution is shown in Figure 5).

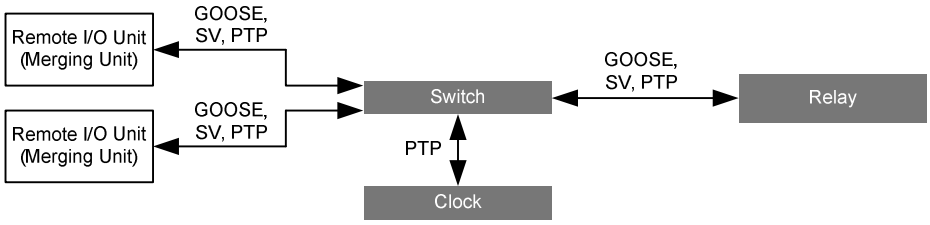

Figure 5 Simplified IEC 61850 Solution

[1] EtherCAT® is registered trademark and patented technology, licensed by Beckhoff Automation GmbH, Germany.

CYBERSECURITY ASSESSMENT

Cryptography

The TiDL and IEC 61850 systems are located and communicate within the physical security perimeter (PSP) and the electronic security perimeter (ESP). This reduces the need for cryptographically secure communications. While cryptography bolsters the robustness of a digital substation solution and can be used to establish machine-to-machine trust, neither technology has cryptographic security (encryption and authentication) built into its protocols.

Simplicity

Security tends to degrade as systems get more complex or more interconnected. The TiDL technology's simplicity creates a stronger security posture versus the IEC 61850 solution by reducing the number of device types that can be targeted, inherently restricting external accessibility, limiting the number of protocols that can potentially be exploited, and eliminating the need for an external time source.

Devices

Each device in the network is a potential target for attack. Reducing the number of device types to be managed and secured reduces the overall attack surface. Each device type in the system needs its own security evaluation. Both solutions employ relays and remote I/O units, but the IEC 61850 solution also introduces switches and clocks that require their own management and security assessments.

Accessibility

Both technologies communicate using Layer 2 of the Open Systems Interconnection (OSI) model. Because TiDL operates using a point-to-point architecture, media access control (MAC) addressing is not enforced, and entities on an EtherCAT network are not required to (and seldom do) have unique hardware MAC addresses. This precludes TiDL systems from being connected to networks that use switches, thereby limiting communications accessibility to physical access only. The IEC 61850 solution uses standard Ethernet MAC addressing for switched networks. To limit accessibility through the switches, the solution requires that ports and access to the ports be managed through policies, network design, and engineering discipline.

A common IEC 61850 architecture to limit accessibility isolates the process bus communications from the station bus communications, as shown in Figure 6.

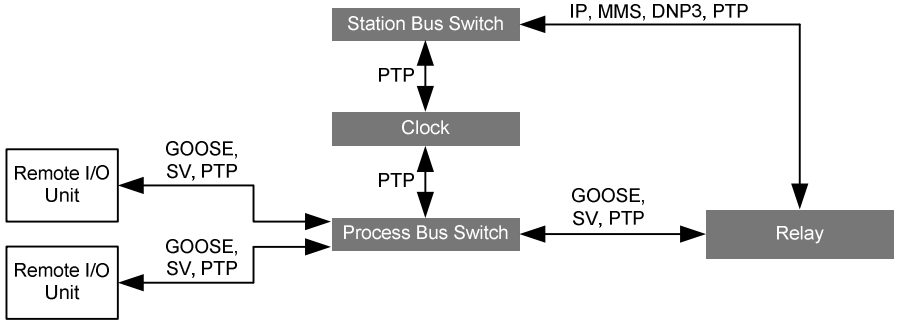

Figure 6 Separate Process Bus and Station Bus Topology

Station bus communications commonly contain Layer 3 communications that extend outside the PSP and ESP. These systems are engineered so that communications to remote I/O units through the station bus switch are prohibited.

Protocols

The TiDL solution employs a single protocol: EtherCAT. The EtherCAT protocol is designated for private, sole-purposed use where other protocols do not exist on the network. This makes the messaging deterministic by design because EtherCAT frames are the only frames on the network. The IEC 61850 solution includes three independent protocols. Simple systems restricted to using GOOSE, SV, and PTP can guarantee data delivery based on the low bandwidth requirements. Larger, generic Ethernet networks require system integrators to study bandwidth allocation and engineer dependability into the solution.

Time Distribution

In a TiDL system, time is distributed using the EtherCAT protocol. The time used to synchronize TiDL systems is a relative system time distributed by the relay, not an absolute time. It is not affected by external natural influences (e.g., solar flares) or potentially malicious influences (e.g., GPS spoofing) that may affect the system's ability to operate reliably.

The performance of the IEC 61850 solution depends on absolute time synchronization among the devices in the network. This places high criticality on how time is distributed within the system. The operation of the protection, control, and monitoring functions depends on the quality, reliability, and availability of the time distribution. IEC 61850 does not dictate these time requirements, only that the data be accurately time-stamped.

Port Services

Minimizing services and capabilities on device ports reduces the attack surface of a solution. Only services contributing to the digital substation solution should be available on device ports. For TiDL, EtherCAT is the only service available on the ports because of its dedicated-network requirements. Typically, an IEC 61850-enabled port is a generic Ethernet port capable of multiple services. Many manufacturers allow services on these ports to be programmatically disabled. If supported, doing so is a recommended security best practice.

NERC CIP Governance

Users commissioning digital substation communications technologies in North America must understand how these solutions affect their North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP) compliance. Both TiDL and IEC 61850 bring new digital communications and devices into the equation. At this time, Version 5 of the NERC CIP standard is in effect. Version 5 recognizes a distinction between protocols that operate at Layer 3 (IP addressing layer) or above and those that operate at Layer 2. In NERC CIP, devices are categorized as being with or without External Routable Communication (ERC). "Routable communication" refers to protocols using Layer 3 and above that are bidirectional. "External" refers to communications connections outside of the ESP. A device that communicates at Layer 3 or higher with bidirectional routable protocols outside of a substation's ESP is categorized as being with ERC. Such devices are subjected to many additional requirements (user access, authentication, patch management, and logging requirements, to name a few).

For TiDL, the remote I/O devices are inherently categorized as being without ERC. For the IEC 61850 solution, a device's ERC status depends on the protocols it supports as well as its Ethernet switches and the other connections made to them. If a switch has connections outside the ESP that allow for Layer 3 or above protocols, then the IEC 61850 remote I/O devices may be considered to be with ERC. However, whether they are or not is beyond the scope of this paper, as the determination depends on the use of electronic access points and whether interactive remote access with those remote nodes is possible. It is recommended that Layer 2 traffic used in IEC 61850 solutions be isolated from other networks in the substation. This can be accomplished by using physically separated switches (process bus versus station bus) or by using software-defined networking (SDN) technologies.

Any additional communications connectivity to the remote I/O units, in both the TiDL and IEC 61850 solutions, requires a separate NERC CIP compliance evaluation.

Cybersecurity Summary

Table 2 provides a summary of the cybersecurity factors for evaluating these two digital substation solutions.

Table 2 Technology Comparison

Technology Attribute	TiDL	IEC 61850
Network topology	Point-to-point Ethernet	Switched Ethernet
OSI model layer	Layer 2	Layer 2
Built-in security (encryption and authentication)	No	No
802.1*x*-compatible MAC addressing	No	Yes
Remote I/O modules with ERC	No	Manufacturer and application dependent
Number of protocols	1	3
Support for other protocols on network	No	Yes
Number of device types	2	4
Dependable time distribution	Inherent	Engineered
Inherent frame determinism	Yes	No

CONCLUSIONS

More devices, more connections, and more protocols mean more engineering, more potential for mistakes, more access points for attack, more testing, more patches, and an overall diminished security posture. The TiDL solution's simplicity and dedicated network stand out in this cybersecurity evaluation. IEC 61850 solutions can be secured by controlling access via separated networks and by emerging technologies such as SDN that ensure dedicated bandwidth and reliability. With a variety of solutions emerging for the digital substation, the main takeaway is that mission-critical systems cannot be built with a generic communications network. A protection system solution must assume full responsibility for all aspects of its operation.

BIOGRAPHY

Joe Casebolt is a research and development manager for the automation controller product lines at Schweitzer Engineering Laboratories, Inc. (SEL). He graduated with a B.S. in computer engineering from the University of Idaho in 2001. He joined SEL in 2001, and his experience includes embedded system design, cybersecurity, protocols, and control and automation solutions. Joe currently holds several patents in the area of digital signal processing and communications.

SCHWEITZER ENGINEERING LABORATORIES, INC.
2350 NE Hopkins Court • Pullman, WA 99163-5603 USA
Tel: +1.509.332.1890 • Fax: +1.509.332.7990
www.selinc.com • info@selinc.com

LWP0021-01

SEL White Paper LWP0021-01 Date Code 20161122