Title
Digital Substations and IEC 61850: A Primer

Permalink
https://escholarship.org/uc/item/5kp7n3cn

Journal
IEEE Communications Magazine, 61(6)

ISSN
0163-6804

Authors
Lozano, Juan C
Koneru, Keerthi
Ortiz, Neil
et al.

Publication Date
2023-06-01

DOI
10.1109/mcom.001.2200568

Copyright Information

Peer reviewed

Digital Substations and IEC 61850: A Primer

Abstract—**Modern electrical substations are managed by intelligent electronic devices communicating through Ethernet-based networks. Because of the highly critical roles of substations, which include safety and protection, electronic devices need to be configured automatically through highly reliable and low-latency networks. This gives substation networks some requirements not addressed by previous industrial network standards. To address these unique challenges, IEC 61850 provides a collection of protocols and a model for the automatic configuration of digital substations. This article briefly overviews this standard and the security efforts to protect substations from attacks.**

I. Introduction

Electrical Substations are a core component of the power grid. They have distributed nodes where operators can monitor and control the flow of electric power, and maintain safety. An electrical substation is an indoor or outdoor facility and can be staffed or unattended. Electrical substations can step up or down electric lines' voltage and perform various control operations such as reactive power compensation. They are also essential for safety and protection by using switching and interrupting devices, known as Switchgear. Circuit breakers, load break switches, and disconnect switches and isolate a grid segment to protect maintenance workers and prevent accidents or equipment damage from overloaded lines. Fast isolation response minimizes hazardous conditions (e.g., when lightning strikes); therefore, these protection mechanisms must be automated. Substations house transformers, reactors, capacitors, circuit breakers, and other switchgear. In addition, a substation usually has a control room with relays, meters, alarm annunciator panels, and other communication equipment.

Before 1960, substations were controlled using large relay panels wired to each element in the switchyard, making it expensive and vulnerable to faults. Programmable Logic Controllers (PLCs) emerged in the 1960s replacing hardwired relay logic circuits, reducing maintenance costs, and deploying new systems. By the 1970s, Supervisory Control and Data Acquisition (SCADA) allowed remote control and supervision tasks while improving situational awareness. Serial SCADA protocols like Modbus and IEC101 emerged as communication standards for connecting a control room with substations or field equipment from different manufacturers. In the 80s and 90s, the adoption of Ethernet and TCP/IP-based networking brought a new range of protocols such as Modbus TCP, IEC 104, DNP3, and OPC for efficient data transmission and facilitate remote operation, maintenance, machine configuration, and interoperability across vendors.

While these industrial network protocols facilitated remote operation and interoperability, they were not tailored for the requirements and high-reliability challenges of emerging networks of embedded computers within a substation. To address the configuration and communication challenges of this *digital substations*, Industry worldwide led by IEC Technical Committee (TC) 57, focused on producing an industry consensus for a communications architecture tailored for the unique requirements of substation automation: integrated control, protection, data acquisition, and automatic configuration.

The IEC 61850 is the international standard for Ethernet-based communication in substations. In contrast to the previous scenario with several vendor-specific protocols and specific solutions even for each substation, IEC 61850 defines a universal data model and a universal language for substation configuration, the Substation Configuration Language (SCL), which includes a logical and abstract representation of the substation components, allowing a single interpretation of the information exchanged and the system architecture. This facilitates the interoperability of equipment in a substation. IEC 61850 also has several related standards that focus on reliability, time synchronization, and redundancy. In this article, we provide a short overview of this standard and its security requirements.

II. Digital Substations

In a classical substation, each electrical signal has to travel from the field device to the control room in an individual copper wire at the expense of constant failures, high maintenance, and operation costs. In contrast, in a digital substation, the conversion occurs at the process level, and the digital data travels to the local control room over reliable network links.

A. Substation Architecture

IEC61850 defines three levels of communications: Process, Bay, and Station, as seen in Figure 1. It also describes how these levels interact and the protocols they use.

The **process level** directly interacts with devices at the switchyard, such as sensors (current and voltage), actuators (circuit breakers), and Merging Units (MU).

The **bay level** is composed of Intelligent Electronic Devices (IEDs); these are control, and protection devices, which receive data from the process level and take local-control decisions. This level also connects the station with the process.

The **station level** contains supervision and operation devices. It allows manual operation and configuration of the SCADA and Human Machine Interfaces (HMIs). It also connects the substation with a Remote-Control room (usually hundreds of km away) to enable a central operator or utility to manually change the status of devices and monitor the substation's operations.

To connect these levels, IEC 61850 defines two buses: The **process bus** and the **station bus**, illustrated in Figure 1, as the

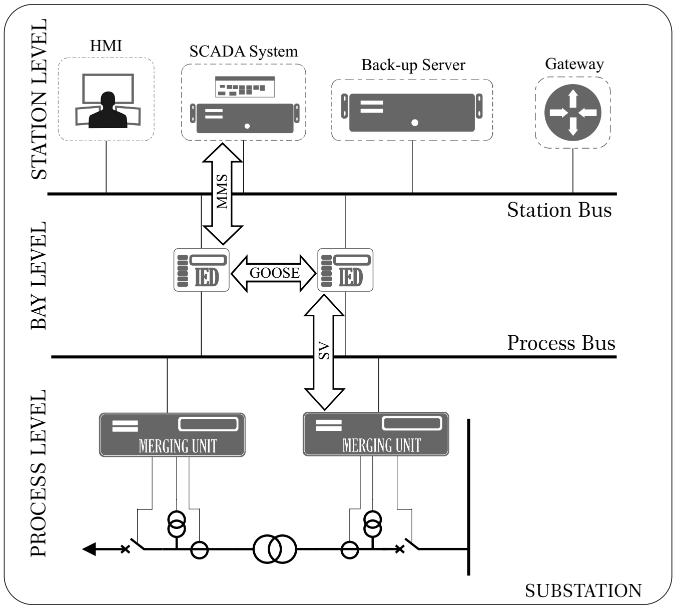

Fig. 1: Substation level representation and internal communication protocols

network interconnecting the process level with the bay level, and the station level with the bay level (respectively). These buses support three different network protocols supporting different communication requirements: from process to bay (SV), within the bay (GOOSE), and from bay to station (MMS).

III. Network Protocols

A. Manufacturing Messaging Specification (MMS)

The communications from bay-level devices to the control room use MMS. The control room can be physically close to the substation field equipment but may be remote. Therefore, to read the status of distant field equipment and to send commands translating to physical actions, we need a reliable connection supported by MMS.

The origin of MMS dated back to the 80s and was standardized in 2003 as ISO/IEC 9506-1 and ISO/IEC 9506-2. Later, the IEC 61850 adopted MMS to define the services to exchange messages in substations.Since MMS was designed independently from IEC 61850, its functions refer to services in a different spectrum or range. It is necessary to adapt or translate IEC 61850 definitions to the MMS equivalent service. MMS uses an association communication model, meaning that besides the underlying connections, there is an agreement on the information to be shared and the conditions to do so. MMS is the only industrial protocol in IEC 61850 over TCP/IP (the other protocols run directly over Ethernet or UPD/IP).

The transmission of messages can be either report or request/respond, depending on the data type. Typically, MMS uses spontaneous reports to transmit measurement data and request/respond to control data.

B. Generic Object-Oriented Substation Events (GOOSE)

The GOOSE protocol communicates emergency events (e.g., overcurrent), and requires a latency between 4 ms to 1 s. Like MMS, GOOSE uses datasets and reports called GOOSE Control Block (GoCB). Unlike MMS, GOOSE uses a subscriber/publisher model to communicate with IEDs. Its data transmission is periodic and via multicast packets, so several destinations can get the same information simultaneously.

The multicast uses a range of MAC addresses from 01-0c-cd-01-00-00 to 01-0c-cd-01-00-FF, which means that at most, 512 GOOSE flows can be in the network. Each IED receives the same data but chooses what data to consume by checking the MAC address and message ID.

GOOSE messages are associated with a VLAN to define message priority. This priority grants privilege over other messages, such as monitoring traces, allowing specific messages to arrive without delay. GOOSE inherits eight priorities from VLAN, from 0 to 7, where 7 is the lowest priority used by default for those devices without priority.

The protocol has two essential parameters: `Time Max` and `Time Min`. `Time Max` is the periodic time for sending messages when there are no events (nothing new to report), usually in seconds. `Time Min` defines the transmission-interval times when an event occurs, and the retransmission happens with an incremental factor of 2. Typically, its value is 1 or 5 ms; for example, in a trip event with `Time Min` of 1 ms, the event detection triggers immediately. The retransmission occurs 1 ms after, 2 ms later, 4 ms later, and so on until it reaches `Time Max`, followed by sending data at the same frequency.

C. Sample Values (SV)

SV samples analog sensor signals at a predefined frequency, and the bay-level equipment reconstructs the signal. SV also allows communications within the process level.

Like GOOSE, SV implements a publish-subscribe model and uses multicast for data transmission. It allows the subscriber to receive data as soon as it is connected.

SV ensures data transmission at a constant bandwidth, and also reports the device's status. Successful error detection requires a significant amount of transmitted information with good resolution. The UCA International Users Group published a guideline known as IEC 61850-9-2LE (Lite Edition) suggesting sample rates for analog values: 80 samples/cycle for protection and metering and 256 samples/period for power quality. It also suggests using one optical pulse per second for time synchronization. This recommendation, in the case of a power system frequency of 60 Hz, requires sending values every 208 μs, which might be a challenge for legacy or constrained devices.

D. HSR/PRP

Because protection devices need to communicate reliably, the use of IEC 62439 (Industrial Communication Networks - High availability Automation Networks), is mandated by IEC 61850. In particular, IEC 62439-3 Clause 4 and 5 defines the Parallel Redundancy Protocol (PRP) and the High-availability

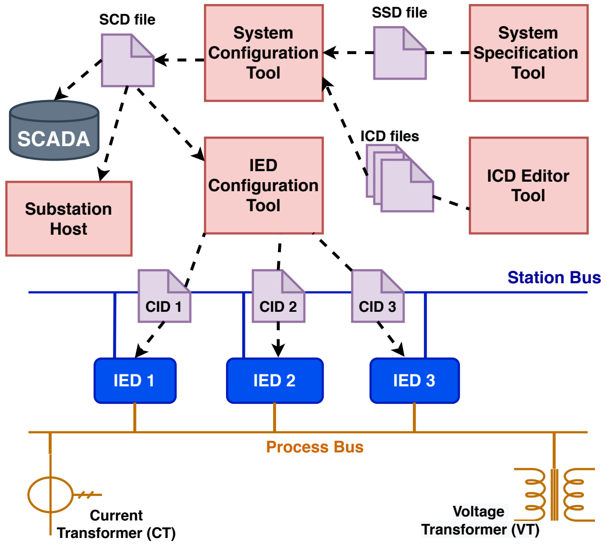

Fig. 2: Files involved in an IED configuration process

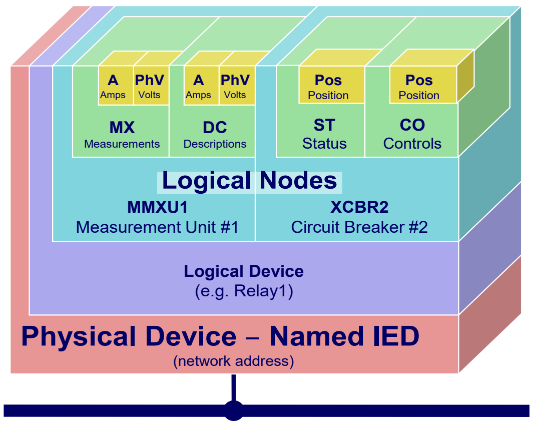

Fig. 3: Object-Oriented IED Data Model

Seamless Redundancy (HSR) protocol. Their goal is to use redundancy in Ethernet networks to improve their reliability.

In PRP, each node is connected to two parallel Local Area Networks (LANs). Each source node sends two copies of each packet, one on each network. When a destination node receives a packet, it accepts the first copy and discards the second copy, eliminating the duplicate. The downside of PRP is the network cost. The ring topology of HSR provides redundancy at a lower cost. The source node duplicates all the frames and sends them using two paths to their destination. If either one of the paths is broken due to link or node failure, the frames can still reach their destination while traveling in the other direction of the ring.

IV. Substation Configuration

MMS, GOOSE, and SV allow devices to provide their services according to their data model and configuration. A substation's configuration defines each element's functionality and interactions. The Substation Configuration Language (SCL) is a description language based on XML, that operators can use to define the topology and configuration of the network.

SCL files enable an interoperable exchange of configuration data between an IED Configuration Tool (ICT) and a System Configuration Tool (SCT) from different vendors. An SCT allows the creation, configuration, viewing, and editing of the substation. The ICT software reconfigures the IEC 61850 settings on an IED during installation or when the IED's requirements for some settings change.

There are two types of SCL files: Input and Output. Input files load the initial information of the devices and network to the System Configurator Tool (SCT). Output files download the configuration information to the IED, i.e., files from SCT include system configuration, SCADA system, etc., and files from ICT include specifics of IED configuration. Figure 2 illustrates the three stages of the configuration process of devices in a substation. In the first stage, the SCT collects SSD and ICD files to obtain the overall topology (electrical and communications) of the substation. The the second stage the SCT assigns a name and IP address to each IED, and creates SCD files with the respective protocols that devices will use (GOOSE, SV, MMS). In the final stage, the ICT generates Configured IED Description (CID) files that are uploaded to each IED.

V. Data Model

One of the advantages of implementing IEC 61850 is the interoperability of data used to describe devices and the information they use. The standard defines a hierarchical structure of nested elements as illustrated in Figure 3. The top-level elements are containers; each container encapsulates elements with more basic characteristics often decided by functionality or availability on the substation. Below, we provide a top-down data model approach.

Each IED is composed of the main Server container, allowing the device to accept connections from clients that are either Human-Computer Interfaces (HCI) or other IEDs. That server container is already an abstraction, but consider it a trivial container for the layer of logical devices.

Logical Device (LD): While the standard mentions that there should be at least one LD, vendors choose to create several LDs based on similar functions; for instance, the set of measurement components is clustered as an LD and protection elements into another LD. There are no unique criteria for such categorization.

Logical Node (LN): LNs should follow a mandatory nomenclature syntax and encoding names for every type. This is a four-length letter name whose first character indicates functionality as defined by IEC 61850-7-4.

Data Objects (DO): An LN is composed of Data Objects. Those elements have attributes that depend on the complexity of each component. A DO may be directly a basic data type, such as Integer, Boolean, or Char. Since elements of a substation have different complexities, e.g., measuring a DC Voltage requires fewer columns than measuring a three-phase voltage, the standard provides other data type builds. Clustering basic data types will create common data types; some common data types are TimeStamp, Array, and ReasonCode.

Data Attributes (DA): These are the core of the abstraction model; different configurations of these elements constitute DOs, and different LNs may use DOs that have the same DAs. For instance, discrete input variables have Value, Quality, Timestamp, and Description. A set of DAs, or Common Data Classes, can be categorized by their functionality, e.g., Measurands, Statues, Controls, and Analogue Settings.

Functional Constraints (FC): Functional Constraints modify the capabilities of DOs. For instance, a specific measuring field of the DO should be Read-only, then a Status FC should be applied to it; this adds semantic and service-oriented features.

VI. IEC 61850 Message Types and Performance Classes

IEC 61850 classifies messages into seven types and is subdivided into performance classes (P1, P2, P3), which define the transfer or processing times for types of messages as stated in part 5 of IEC 61850. (P2/P3) performance classes represent the most time-critical messages, demanding a total transmission time below the order of a quarter of a cycle.

The seven types are: **Type 1A** (P1) messages include releases and status changes that have a transmission time of 10 ms, whereas **Type 1A** (P2/P3) messages include trips and blockings with a transmission time of ≤3 ms. Other time-critical messages (**Type 1B**) include Start, Stop, Close, etc., with a transmission time varying from 20 ms (P2/P3) to 100 ms (P1). The first type is for protection and control and covers three performance classes: P1 - distribution bay, P2 - transmission bay, and P3 - transmission bay with high-performance synchronizing features and breaker differential.

Types 2, 3, 5 messages are less time-critical and are classified as P1 messages. **Type 2** contains normal 'state' information with the transmission time of ≤ 100 ms. **Type 3** messages comprise slow auto-control functions, the transmission of event records, and the general presentation of time-tagged system data with transmission time ≤ 500 ms. **Type 5** messages file transfer messages, where large data files of recording, information, or settings are transferred with a transmission time ≥ 1000 ms.

Type 4 messages are raw-data messages including cyclic/periodic sampling messages from instrument transformers. These are critical messages with a transmission time of 10 ms for the P1 class and ≤ 3 ms for the P2/P3 class. **Type 6** messages used to synchronize the internal clocks of IEDs in the system, and **Type 7** messages of a high degree of security used for transfer of control orders command messages with access control.

VII. Security

Most industrial protocols were designed with the implicit assumption of trusted insiders. The idea is that the industrial network is isolated and only trusted devices and people have access to it. Unfortunately, in practice, these assumptions are starting to break down. Airgapped networks can be bypassed, disgruntled employees can access industrial networks, and these networks are getting connected more and more often to corporate networks for business reasons.

To address these security challenges, the IEC TC 57 developed IEC 62351, a standard to provide security measures and solutions to all protocols, such as IEC 60870-5 (Control Center to Substations/SCADA 101-104), IEC 60870-6 (Connecting Control Centers, ICCP), IEC 61850 (within a substation), IEC 61970 (with the application program interfaces for energy management systems (EMS)), and IEC 61968 (inter-application integration at electric utilities - System interfaces for distribution management). Currently, the standard has 16 parts, of which three focus on the communication profiles of IEC 61850. And four other parts focus on the general security mechanisms common to all the TC 57 series. The details about the parts of the standard relevant to IEC 61850 are discussed below:

IEC 62351-3: ***Profiles including TCP/IP:*** This specifies the cybersecurity procedures to achieve confidentiality, integrity, and authentication at the transport layer for different SCADA and tele-control protocols that use TCP/IP. The primary implementation of this part of the standard is to use Transport Layer Security (TLS) as the underlying protocol to provide end-to-end transport security for power system automation protocols, together with X.509 certificates for the authentication of the device.

IEC 62351-4: ***Profiles including MMS and derivatives:*** This standard specifies security requirements for MMS messages both at the application and transport profiles. Two transport security (T-security) specifications, i.e., compatible and native, are given at the transport layer. Compatibility mode is exclusively for MMS using OSI stack implementation according to ISO 9506-2. In contrast, the native mode is relevant for MMS using the IP suite and IEC 61850-8-2 XMPP implementations. The T-security specification uses Transport Layer Security (TLS) protocol for TCP sessions.

At the application layer, two security specifications, namely peer-to-peer (or A-security) and End to End application security (E2E security), are specified by IEC 62351-4 standards. In A-security specification, the main goal is to provide authentication. Hence, it requires T-security at the transport layer, which makes the system secure. E2E security authentication achieves message integrity and confidentiality using public key signatures and symmetric encryption algorithms.

IEC 62351-6: ***Security for IEC 61850 (GOOSE and SV):*** The standard specifies that confidentiality of GOOSE and SV messages is not ensured due to the stringent timing requirement of 3ms. Digital signatures are a straightforward solution that provides authentication for GOOSE and SV messages. However, some studies argue that digital signatures are computationally expensive in the time required for these messages for embedded devices.

Message Authentication Codes (MAC) have been proposed to replace digital signatures for GOOSE and SV messages. While MACs are more efficient and can prevent outsiders from forging messages in these networks, they cannot prevent a compromised device from impersonating others. Other disadvantages of replacing digital signatures with MACs are the difficulty in providing a secured channel for shared keys and the inability to provide non-repudiation.

IEC 62351-7: ***Network and system management (NSM) data object models:*** This specifies the Network and system management for energy systems: it supports gathering information about the network through NSM data objects. These data objects aid in monitoring the health of the devices such as IEDs (Intelligent Electronic Devices), RTUs (Remote Terminal Units), DERs (Distributed Energy Resources) systems, and other systems that are important to power system operations. Intrusion detection systems use this information, but this standard part does not provide any specific guidance to identify attacks.

IEC 62351-8:***Role-based access control (RBAC):*** The main goal of this part is to separate authorization from authentication such that users have only the permissions needed to perform their duties. RBAC is not confined to human users; it applies to automated systems and software applications. This part details two types of access: 1) local (direct wired) access to the object by a human user, a local and automated computer agent, or a built-in HMI or panel. 2) remote (via dial-up or wireless media) access to the object by a human user or a remote automated computer agent, e.g., another object at another substation or a control center application. This part also defines a list of pre-defined roles (e.g., VIEWER, OPERATOR, etc.) and pre-defined rights (e.g., View, Read, Control, etc.) and provides more information on handling sessions.

IEC 62351-9: ***Cyber security key management for power system equipment:*** The main focus of this part of the standard is to provide key management techniques required for different algorithms specified in the other parts of IEC 62351 standards, such as 3, 4, and 6. Part 9 includes the generation, distribution, and handling of public key certificates and cryptographic keys.

IEC 62351-10: ***Security architecture guidelines:*** This document describes essential security architecture guidelines specifying indispensable components, functions, and their relationship. It also covers the integration of those security elements into the general power system to deploy security at different stages.

IEC 62351-11: ***Security for XML documents:*** It determines the procedures to secure XML documents present on a substation, e.g. SCL files, it uses already known W3C standards specifying ways to encapsulate the XML file, Access control to sections of the document and signatures.

While this security standard provides a baseline of security best practices, it does not discuss advanced security practices or discussions on trade-offs. We, therefore, turn to recent academic research on the security of IEC 61850.

TABLE I: Summary of the taxonomy of related work on security in Substation Automated Systems.

	[1] Biswas *et al.*	[2] Quincozes *et al.*	[3] Rezabek *et al.*	[4] Yang *et al.*	[5] Rrushi *et al.*	[6] Yahya *et al.*	[7] Mashima *et al.*	[8] Youseff *et al.*	[9] Tan *et al.*	[10] Reda *et al.*	[11] Lopez *et al.*	[12] Xu *et al.*	[13] Hussain *et al.*	[14] Volkova *et al.*	[15] Aftab *et al.*
Security															
Intrusion Detection	-	●	-	●	●	●	-	-	●	-	●	-	-	-	-
Attacks	●	-	-	-	-	-	-	-	●	●	-	-	-	●	●
Use of IEC62351	-	-	-	-	-	-	-	●	-	-	-	-	●	●	●
Performance Cost	-	-	●	-	●	-	-	-	●	-	-	◐	●	●	-
Honeypot	-	-	-	-	-	-	●	-	-	-	-	-	-	-	-
Protocol Focus*															
MMS	-	●	-	●	◐	-	●	●	●	-	●	-	-	●	●
GOOSE	●	●	-	●	◐	-	●	●	-	●	-	-	●	●	●
Sampled Values	-	●	-	◐	-	-	-	●	-	-	-	-	●	●	●
PTP	-	-	●	-	-	-	-	-	-	-	-	-	-	-	◐
HSR/PRP	-	-	-	-	-	-	-	-	-	-	-	●	-	-	-
Implementation															
Simulation	●	-	●	-	-	-	●	-	●	●	●	●	-	-	-
Testbed	-	-	-	●	●	●	-	-	-	-	-	-	-	-	-
Survey	-	●	-	-	-	-	-	-	-	-	-	-	●	●	●
Real world data	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-

Legend: ●: feature considered by authors, ◐: feature is not explicitly stated or exhibits ambiguity.

A. Academic Research

Table shows our taxonomy and survey of recent results about the security of IEC 61850.

As we can see from the table, attacks and how to detect these attacks (intrusion detection) have been the most popular areas of research. There are three approaches for Intrusion Detection Systems (IDS): Signature-based IDS (looks for known bad), Specification-based IDS (looks for activity outside the specification), and Anomaly-based IDS (looks for anomalous activities). Anomaly detection was and continues to be one of the most popular academic research directions [5], and tools used to detect anomalies include stochastic activity networks and Support Vector Machines (SVMs).

Recently, however, more work has been focusing on Specification-based IDS [4], [6], [9]. Some use MMS protocol specification, physical states, and protocol interactions. Yang includes SCL to create a white list of communications among IEDs and also uses the maximum number of Report control blocks for each IED. Recall that SCL files specify Datasets and Reports; the former are subsets consisting of Data Objects selected by the user, and the latter allows configuration to determine sending times of the datasets. Reports are user-defined triggers, choosing from a change in a value when a value is updated by a user, periodically, or after connection recovery.

Datasets and Reports let an honest observer know the amount of information that should be flowing given the Report settings. When communication patterns in the substation violate any of the configured datasets or reports, an alert is raised by the IDS. Similarly, Lopez extracts information from the SCL files to understand the rules that govern the specific substation and make the Intrusion Detection System *substation aware.* [11]

The other popular topic focuses on attacks. These range from attacks against **Availability** by exploiting vulnerable implementations with malformed packets [10]; attacks against **integrity** by illustrating man-in-the-middle (MiTM) attacks on MMS, replay and tampering of messages on GOOSE, and message injection [14]; finally, attacks against **confidentiality** focus on eavesdropping due to non-encrypted transmissions [1], [10] while others propose mechanisms to make transmissions more secure by using authenticated encryption algorithms AES [13].

Some authors review all the IEC 62351 standard security mechanisms when implemented with IEC 61850 [8], [14]. [14] concludes that there have been insufficient tests on the performance impact of IEC 62351 security applied to IEC 61850 systems and notes that complete integration is underspecified; other authors have gone further, [13] discovered that using AES Digital Signatures on GOOSE and SV as mandated by IEC 62351 does not meet time requirements of IEC 61850.

Honeypots for 61850 haven't received much attention from the research community, but recently Mashima et al. [7] explored this idea. They created a smart grid testbed that implements open source, virtualization, and back-end simulation (the physical process is simulated using Mininet for IEDs and a module called SoftGrid). In addition to the bay-level network, the authors recreate a control center including a Historian, SCADA, firewalls, and an externally connected PC. Most of their components are virtualized except the Historian, SCADA HMI, and VPN Server. The work is a first approximation and may be enhanced by fingerprinting of IED devices.

We found relevant a set of survey papers that include security for digital substations and discuss previously known protocol vulnerabilities and the proposed solutions, also analyzing their performance impact. In this branch, the work of Quincozes et al., surveys Intrusion Detection Systems in Automated Electrical Substations, pointing out the early stage of preventive measures for IDS [2]. Other documents dig into IEC 62351, and its performance cost in a comprehensive way covering MMS, GOOSE, and SV [13], [14]; additionally, Aftab et al. discuss Time Synchronization and performance based on the message type. [15]

Finally, as seen from the table, most papers validate their findings using simulators such as PowerWorld, PowerFactory, or SoftGrid IEDs. Other works use Testbeds; [5] uses SEL-421 IEDs acting as diverse components.

However, as seen from the table, no previous study has analyzed their security with real-world data. This is not surprising because the power industry is more conservative and does not like to share data for security reasons. We argue that we need to understand the operation of real-world systems better to understand if our security solutions match real-world systems. Another open area of research is the design, implementation, and enforcement of granular access control policies. As outlined above, the standard provides some basic access control rules, such as defining data types as `read only`. Enforcing and guaranteeing that these properties are maintained is an open challenge. Finally, we have not seen any discussion in the standards and research papers about post-quantum algorithms for 61850. Several post-quantum algorithms are being analyzed and standardized to replace RSA and Elliptic Curves algorithms. Discussing their applicability to 61850 is another open research direction.

VIII. Conclusion

In this article, we presented a primer on substation automation, IEC 61850, and related standards that describe the data model, protocols, configuration, and interoperability of substation equipment. Our goal is to present a short introduction to help newcomers to the field. We then discussed the main cybersecurity trends from industry and academia.

Overall, while we have made progress in defining security protections from industry, and intrusion detection in academia, work on attack recovery is limited. We believe that researchers should work on developing automated and semi-automated tools to help operators recover from attacks and bring systems back to operation after an incident. We also found that most of the research work focuses on simulations or testbeds, however, there is no research on security with real-world datasets or real-world systems. We understand that performing cybersecurity experiments in an operational substation is highly risky; however, obtaining datasets from real-world configurations is a first step that we encourage researchers to pursue. This way, we can validate cybersecurity methods with realistic configurations from operational systems.

References

[1] Qingbo Zhu Yuan Li Daisuke Mashima Binbin Chen Partha P. Biswas, Heng Chuan Tan. A Synthesized Dataset for Cybersecurity Study of IEC 61850 based Substation. In *2019 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm)*, pages 1–7, 2019.

[2] Silvio E. Quincozes, Célio Albuquerque, Diego Passos, and Daniel Mossé. A survey on intrusion detection and prevention systems in digital substations. *Computer Networks*, 184:107679, 2021.

[3] Filip Rezabek, Max Helm, Tizian Leonhardt, and Georg Carle. PTP Security Measures and their Impact on Synchronization Accuracy. In *2022 18th International Conference on Network and Service Management (CNSM)*, pages 109–117, 2022.

[4] Yi Yang, Hai-Qing Xu, Lei Gao, Yu-Bo Yuan, Kieran McLaughlin, and Sakir Sezer. Multidimensional Intrusion Detection system for IEC 61850-Based SCADA Networks. *IEEE Transactions on Power Delivery*, 32(2):1068–1078, 2017.

[5] Julian L. Rrushi and Roy H. Campbell. Detecting attacks in power plant interfacing substations through probabilistic validation of attack effect bindings. In *S4: SCADA Security Scientific Symposium*, 2008.

[6] Mohammad Yahya, Nasir Sharaf, Julian L. Rrushi, Ho Ming Tay, Bing Liu, and Kai Xu. Physics reasoning for intrusion detection in industrial networks. In *2020 Second IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA)*, pages 273–283, 2020.

[7] Daisuke Mashima, Derek Kok, Wei Lin, Muhammad Hazwan, and Alvin Cheng. On design and enhancement of smart grid honeypot system for practical collection of threat intelligence. In *13th USENIX Workshop on Cyber Security Experimentation and Test (CSET 20)*. USENIX Association, August 2020.

[8] Tarek A Youssef, mohamed El Hariri, Nicole Bugay, and Osama A Mohammed. IEC 61850: Technology Standards and Cyber-Security Threats. In *2016 IEEE 16th International Conference on Environment and Electrical Engineering (EEEIC)*, pages 1–6, 2016.

[9] Heng Chuan Tan, Vyshnavi Mohanraj, Binbin Chen, Daisuke Mashima, Shing Kham Shing Nan, and Aobo Yang. An IEC 61850 MMS Traffic Parser for Customizable and Efficient Intrusion Detection. In *2021 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm)*, pages 194–200, 2021.

[10] Pejman Peidaee Adnan Anwar Abdun Mahmood Akhtar Kalam Haftu Tasew Reda, Biplob Ray and Nahina Islam. Vulnerability and impact analysis of the IEC 61850 GOOSE protocol in the smart grid. *Sensors*, 2021.

[11] Jose Antonio Lopez, Iñaki Angulo, and Saturnino Martinez. Substation-aware. an intrusion detection system for the IEC 61850 protocol. In *Proceedings of the 17th International Conference on Availability, Reliability and Security*, pages 1–7, 2022.

[12] Luoyun Xu, Haiyu Li, and Linwei Chen. Modeling and performance analysis of data flow for HSR and PRP under fault conditions. In *2018 IEEE Power Energy Society General Meeting (PESGM)*, pages 1–5, 2018.

[13] Taha Selim Ustun S. M. Suhail Hussain and Akhtar Kalam. A review of IEC 62351 security mechanisms for IEC 61850 message exchanges. *IEEE Transactions on Industrial Informatics*, 2020.

[14] Anna Volkova, Michael Niedermeier, Robert Basmadjian, and Hermann de Meer. Security challenges in control network protocols: A survey. *IEEE Communications Surveys Tutorials*, 21(1):619–639, 2019.

[15] Ikbal Ali Taha Selim Ustun Mohd. Asim Aftab, S.M. Suhail Hussain. IEC 61850 based substation automation system: A survey. *Electrical Power and Energy Systems*, 2020.

Juan C. Lozano (juclozan@ucsc.edu) a Ph.D. candidate in Computer Science at the University of California, Santa Cruz, received an M.S. (2016) and B.S. (2010) degree from the Universidad Nacional de Colombia, his interests cover Intrusion Detection Systems for Cyber-physical systems for Industrial Control Systems and Medical Devices, aiming for adaptive techniques on diverse scenarios.

Keerthi Koneru (kekoneru@ucsc.edu) is pursuing her Ph.D. and is a graduate student researcher at the University of California, Santa Cruz. She received her M. S. in Computer Science from Sam Houston State University (2016), in Texas. Her recent research focuses on network security and deep packet inspection of substation protocols such as IEC 61850. Part of her work also includes network analysis on Internet of Things (IoT) devices such as smart cameras and baby monitors.

Neil Ortiz (nortizsi@ucsc.edu) is pursuing his Ph.D. and is a graduate student researcher at the University of California, Santa Cruz. His interests cover Network Security and Intrusion Detection Systems. His research focuses on identifying the successful practices and lessons learned by countries subject to persistent attacks on their critical infrastructures.

Alvaro A. Cardenas (alacarde@ucsc.edu) (SM, IEEE) received a B.S. degree from the Universidad de Los Andes (2000), Colombia, and the M.S. (2002) and Ph.D. (2006) degrees from the University of Maryland, College Park. He is currently an Associate Professor with the Department of Computer Science and Engineering at the University of California at Santa Cruz. His research interests include cyber-physical systems and IoT security and privacy, network intrusion detection, and wireless networks.