Unveiling the Operation and Configuration of a Real-World Bulk Substation Network

Keerthi Koneru[1(✉)], Juan Lozano[1], John Castellanos[2], Emmanuele Zambon[3], and Alvaro Cardenas[1]

[1] University of California, Santa Cruz, USA
{kekoneru,juclozan,alacarde}@ucsc.edu
[2] Hitachi Energy, Mannheim, Germany
john.castellanos@hitachienergy.com
[3] Eindhoven University of Technology, Eindhoven, Netherlands
e.zambon.n.mazzocato@tue.nl

Abstract. Electrical substations are distributed points where operators can monitor and control the power grid. In this paper, we perform the first in-depth study of the operation of a large (500 KV) real-world substation automation network. We provide a view of how these critical networks operate using packet captures and a Substation Configuration Description (SCD) file. We discuss the challenges we overcame to reconstruct a network with redundant paths, gateways, serial legacy devices, and sophisticated intelligent electronic devices (IEDs). Our work provides a deep-dive discussion of these critical networks in a real-world system and sheds light on their operation, configuration and security.

Keywords: Communication · GOOSE · IEC 61850 · IEC 62439-3 · Network measurement · Security · Passwords · Network Monitoring · Network architectures · PRP · Substation Automation · Substation · Substation Configuration Description (SCD) file

1 Introduction

In the last two decades, substations have undergone an automation revolution, changing from analog communications to modern networks and computers, including Intelligent Electronic Devices (IEDs). Furthermore, new standards focus on the fully automatic configuration of a substation. A Substation Automation System (SAS) comprises hardware and software components that monitor and control an electrical system locally and remotely. SAS replaces repetitive, tedious, and error-prone tasks with automated processes, enhancing system efficiency and productivity.

Despite the growing number of automated substations, the academic community has limited visibility into how these critical networks operate in the real world. This paper addresses this blind spot in our network measurement community. In particular, we analyze a pcap network capture and a substation configuration description (SCD) file from a large 500 kV substation. From these passive measurements, we aim to learn as

X. Hei et al. (Eds.): SmartSP 2024, LNICST 622, pp. 211–236, 2025.
https://doi.org/10.1007/978-3-031-93354-7_10

much as possible about the operation of these networks, the devices, their configuration, and their security.

Finally, automating network reconstruction is an important security step. In Operational Technology (OT) networks, the most common first step for securing a network is to perform asset inventory: systematically collecting, cataloging, and managing all technological devices in the OT network. Many legacy OT operators do not even know what is on their network. However, reconstructing a substation network presents challenges for their unique use of proxies, legacy serial devices, multicast messages, and redundant parallel networks. These complexities require us to develop a new framework to analyze substation datasets.

Our contributions include the following:

- We create a framework for analyzing substation networks through packet captures and substation configuration description (SCD) files, enabling a systematic approach to understand their operation.
- We reconstruct the substation network using passive measurements, providing insights into the network's structure, protocols, and devices. As far as we know, we are the first to give this detailed view of the operation of a real-world substation.
- During our study, we had to overcome several technical challenges to uncover the presence of proxies, redundant networks, legacy serial devices, devices subscribed to multicast messages, etc. Our results shed light on unexplored aspects of real-world substation networks.

2 Related Work

Table 1. List of papers showing the analysis of previous research on substation datasets.

	[15]	[7]	[24]	[14]	[20]	[37]	[36]	[5]	[19]	[8]	[10]	[18]	Our Work
Substation Network	●	●	●	●	●	●	●	●	●	●	●	●	●
DPI	-	-	-	-	-	-	●	●	●	-	-	●	●
Use of SCD Files	-	-	-	-	-	-	-	-	-	●	-	●	●
Real World data	-	-	-	-	-	-	-	-	-	-	●	-	●

Legend: ●: Feature considered by authors. DPI: Deep Packet Inspection. SCD: Substation Configuration Description

There is a growing literature studying the networks in electric substations. As we can see in Table 1, while researchers have an interest in understanding substation networks, most studies use synthetic data, either from testbeds or simulations.

We are only aware of three previous papers looking at real-world power grid networks [4,10,23,25]. Out of these papers, only Formby et al. [10] focuses on substation networks (and therefore, it is the only paper in our table). Formby et al. focused primarily on traffic analysis (timing and packet sizes) of various devices. In contrast, in

this paper, we use Deep Packet Inspection (DPI) and a substation configuration file to discover all the devices in the network and their specific roles and functions.

The remaining papers in the table use synthetic data from testbeds or simulations. Research efforts that look at the payload of the packets (DPI) include Konka et al. [17], which studies the headers and PDUs of Sample Values packets. Similarly, [5] and [18] analyzed Generic Object Oriented Substation Events (GOOSE) traffic, exploring statistical parameters and proposing anomaly detection methods. As far as we know, no previous work has used DPI to uncover legacy serial devices and proxies within substations.

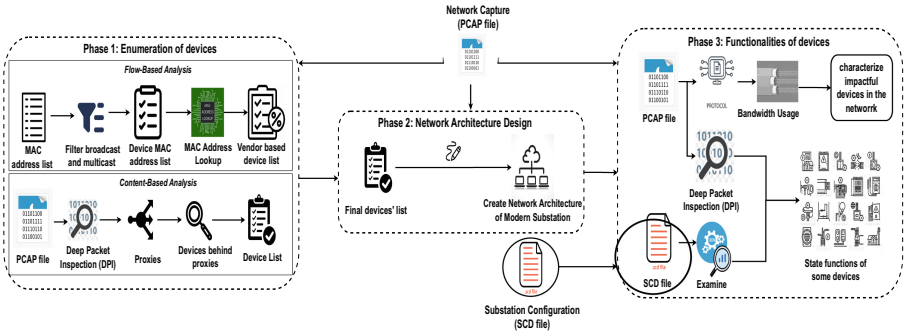

Fig. 1. Proposed framework to analyze substation networks.

Furthermore, we discovered several studies that actively utilized Substation Configuration Language (SCL) files for their research. These files are used for substation automation. For example, [8] developed a program capable of parsing SCL files and generating detailed reports on the identified components. Similarly, [13] proposed a methodology for estimating GOOSE and Sample Values (SV) traffic by extracting relevant information from SCL files. Also, [18] employed the SCL language to evaluate the domain of exchanged fields, incorporating it as supplementary data for their deep packet inspection analysis. We are unaware of any previous work using SCL files from real-world systems.

This paper uses a network trace from a real-world transmission substation and a configuration file for some of its devices. We then inspect the payloads to understand these networks' devices, services, and operations. In addition, the configuration files allow us to understand the producers and consumers of multicast information being sent in this network. Our final result is a more detailed description of an operational substation network in an academic publication. Our work fills a gap in the academic community in understanding real-world substation networks.

3 Substation Automation

Early substations had to convert several analog-to-digital signals at the local control room, requiring individual copper wires for each signal to traverse from the switchyard

to the control room. This arrangement led to frequent failures and incurred significant maintenance and operation costs.

In the 1990s, the transition from conventional protection and control systems to digital Substation Automation Systems (SASs) brought significant changes. The distinction between the conventional and digital substations lies in the location of the information digitization process. This conversion happens at the source in digital substations, allowing the transmission of digital data to the local control room via more reliable channels like optical fiber. Figure 2 illustrates the difference between conventional and digital substations.

Digital substations offer significant advantages, including increased safety by eliminating the electrical connection between high voltage equipment and protection/control panels, reduced cabling, maintenance, and installation time, utilization of advanced communication protocols (such as IEC 61850 and IEC 62351), and high reliability.

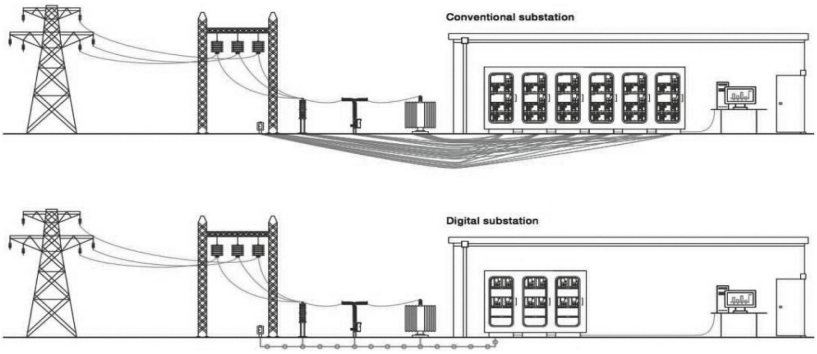

Fig. 2. Conventional Substation vs. Digital Substation: Digital Substations replace many copper wires with a single fiber-optic bus.

3.1 Substation Architecture

Substations are situated at various stages of the Power Grid, each with specific functions and equipment tailored to their location, such as generation, transmission, or distribution. Despite that diversity, a standardized substation architecture typically includes three levels based on function and location.

The three levels are: **process**, **bay**, and **station**-level.

Figure 3 shows different substation levels connected by process bus and station bus.

Process Level: The process level includes primary equipment like switching devices, circuit breakers, and instrument transformers. Information from measuring devices is transmitted through the process bus using the Sampled Values (SV) protocol, facilitating communication between Merging Units (MUs) and Intelligent Electronic Devices (IEDs) over Ethernet. IEDs at this level serve as sensors and actuators connected to the process bus through LAN technology. MUs synchronize time by receiving inputs from instrument transformers and circuit breaker auxiliary contacts.

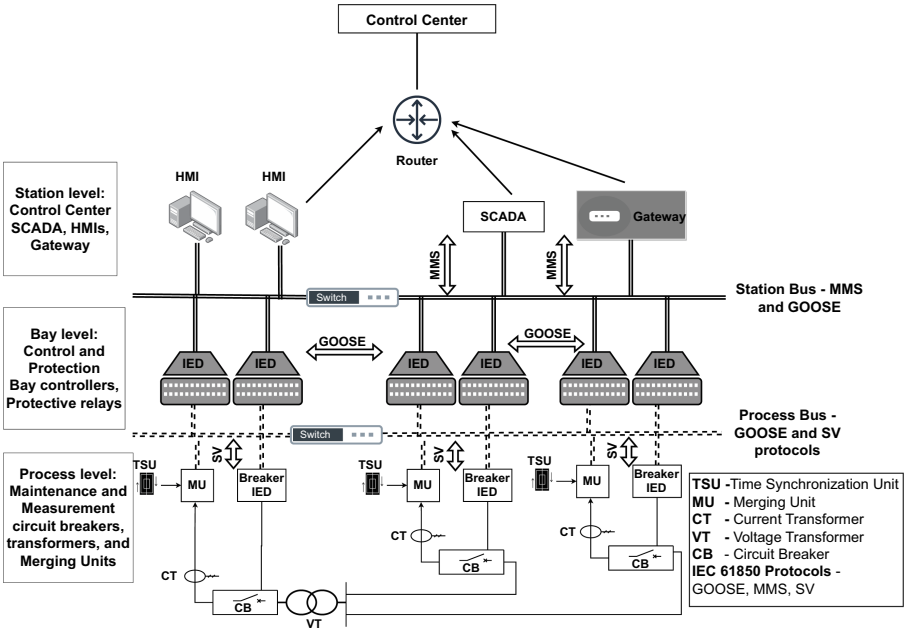

Fig. 3. Levels of a Substation Automation System.

Bay Level: The bay level consists of IEDs, which are microprocessor-based power system equipment with control and automation functions. These devices process sensor data and issue control commands to prevent failures. They utilize the GOOSE protocol for communication. Common IEDs include circuit breakers, protective relays, and PLCs.

Station Level: The station level in the control room includes Human-Machine Interfaces (HMI), SCADA systems, Fault Recorders, Alarms, and the Gateway to the remote control center. The client can read/write data, read configuration, and exchange files at this level.

Our network capture is at the interface between the Station level and the Bay level of the substation, so in the remainder of this paper, we focus on this supervisory network.

3.2 IEC 61850 in Substations

Improvements in automation and reliability need interoperability. The IEC 61850 standard by the Technical Committee Number 57 (TC57) Working Group 10 (WG10) has three main principles:

1. Defining a **unified information model.**
2. Usage of standard file (**substation configuration description**) with specific rules.
3. Defining a system-wide **communication protocol** to exchange data.

Information Model: The information model or data model of IEC 61850 includes a naming hierarchy (described in Appendix A.1) and specific data structures for any compliant device. Vendors should use the same concepts with the same name and a standard format to build their information. This feature reduces errors and format conversions.

Substation Configuration Description (SCD)
Integrating substation equipment in automation requires a standardized format to configure networking capabilities and improve performance. IEC 61850 Part 6 defines the Substation Configuration Description Language (SCL/SCD), using the XML schema, to describe IED functions and communication networks [13]. The detailed structure of the SCD file is described in Appendix A.2.

Communication Protocols
The IEC 61850 protocol stack ensures reliable communication between devices, promoting interoperability. It includes sub-protocols like Manufacturing Message Specification (MMS) over TCP/IP, while GOOSE and SV utilize Ethernet multicast for real-time data exchange. Ethernet multicast enables fast and prioritized data distribution to subscribers with low delays (within 3 ms or 20 ms).

GOOSE: We focus on GOOSE because our network capture includes this industrial protocol. GOOSE is a publish-subscribe communication service between IEDs [12]. It ensures fast and reliable distribution of binary status information through multicast services, enabling high performance and availability [11].

3.3 Parallel Redundancy Protocol (PRP)

Substations utilize redundancy measures to ensure uninterrupted operation and minimize downtime during failures or disruptions. In particular, the IEC released specifications for industrial-Ethernet communications under the IEC 62439 standard mandated by IEC 61850 [3].

PRP is a part of IEC 62439. PRP protocol provides redundancy by connecting devices to two independent Ethernet networks (LAN_A and LAN_B). This implementation allows Ethernet frames to reach their destination through an alternate port if one network fails. PRP also allows the connection of devices that do not support PRP (these devices will only see one Ethernet network). After we obtained our network capture, we first realized that all frames in the network were encapsulated in this PRP protocol. We will describe our analysis next.

4 Enumeration of Devices

Our data consists of a network capture (pcap file) of 14 continuous hours and a configuration file (SCD) from a large (500 KV) real-world substation automation network. Figure 1 shows our proposed framework for analyzing the pcap and configuration files from a substation.

The goal in the initial phase is to enumerate all the devices in the network. Our first attempt used flow-based analysis to discover unique MAC addresses. However, we later found that several devices in these networks are behind proxies, and to discover those, we need to perform a content-based analysis by looking at the payload of the packets.

Table 2. Taxonomy of devices based on vendors

Protocol	Device Vendor Name	# of Devices	Percentage
Ethernet Devices	ABB AUTOM	33	31.73%
	SIEMENS	10	9.61%
	IPCAS	10	9.61%
	ABB SWITZ	3	2.88%
	HP	5	4.8%
	AMETEK	4	3.84%
	RuggedCom	3	2.88%
	MegaSystem	3	2.88%
	Moxa Technologies Corp.	2	1.92%
	Advantech	2	1.92%
	CADAC	1	0.96%
	Reason Technologia SA	1	0.96%
	Dlink	1	0.96%
Serial Devices	SEL IED	9	8.65%
	Unknown Devices	16	15.38%
	Modem	1	0.96%

In the second phase, we build the network architecture by integrating the initial findings and the guidance of the IEC standard. In the final stage, we combine deep-packet inspection and SCD files to identify the functionality of most devices in the network.

This section focuses on the first phase, where we enumerate devices by network flow analysis and then by content-based analysis (to identify devices behind proxies).

4.1 Flow-Based Analysis

We found 97 unique MAC addresses in the network capture. Of them, 19 are broadcast/-multicast destinations for different Ethernet and IP protocols such as PRP, GOOSE, IPv4/IPv6 multicast, and broadcast. For the remaining 78 Ethernet devices, we used a MAC address look-up [32] to classify them based on their vendor name as shown in Table 2. From this table, we can see that most of the Ethernet devices are from just three vendors: ABB AUTOM (which refers to the industrial company ABB), SIEMENS (referring to the industrial company Siemens), and IPCAS (which as we will show later, is also from Siemens).

4.2 Content-Based Analysis

During this step, we examined the payload of network traffic from each identified device in the flow-based analysis. Using deep packet inspection, we found the presence of two

types of proxies in the network: RedBoxes (referred to as AS1, AS2, AS3) from ABB SWITZ and Serial to Ethernet Gateways (referred to as M1, M2) from MoxaTech Corp.

Redundancy Boxes (RedBoxes): RedBoxes serve proxies that facilitate the connection of devices that do not support the PRP protocol (we will discuss this protocol in the next section).

Table 3 shows the summary of the devices behind each RedBox.

Serial to Ethernet (S2E) Gateways: After identifying the MAC address of these gateways (which we refer to as M1 and M2), we figured they connected legacy serial devices to the substation network. We analyzed the traffic through these gateways and discovered 26 additional devices behind M1 and M2. We will describe more details in Sect. 6.3.

We are now ready to switch to Phase 2: identifying how these devices are connected to the network.

5 Network Architecture

The first surprise we found when analyzing the pcap file was that all Ethernet frames were encapsulated (PRP enclosure trailer `0x88fb`) with a protocol we hadn't heard of before: PRP.

After finding the documentation about PRP, we discovered that this protocol is used for high reliability and availability. PRP provides full redundancy by connecting two Ethernet networks and using both to send all information. This level of redundancy makes sense in highly critical networks, where an alert about an unsafe condition (e.g., an overcurrent alert) needs to be propagated reliably to devices that can respond to this condition (e.g., opening a circuit breaker to prevent a fire).

The IEC standard classifies each device connected to the PRP network into three categories [8]:

- ***Doubly-Attached Nodes (DAN)*** - devices with two network interfaces and connected to both the LANs (LAN_A and LAN_B).
- ***Singly-Attached Nodes (SAN)*** - non-critical devices having a single network interface and only connect to one of the networks (either LAN_A or LAN_B) without requiring redundant communication [8].
- ***Redundancy Box (RedBox)*** - gateways for SAN devices without PRP support to connect to both networks. These devices, called VDANs, use RedBox messages that include the associated SAN's source MAC address. Figure 4 differentiates the RedBox Message from the normal DAN message.

From the above, devices that speak PRP are either DANs or RedBoxes.

Table 3. Devices connected to RedBoxes

RedBox	Devices Connected
AS1	No Devices
AS2	2 HP computers and 1 Advantech Industrial PC
AS3	1 HP computer and 1 Advantech Industrial PC

5.1 Network Architecture

We identified more than 50% of the devices as DANs, based on the PRP packets they send. Additionally, 2.8% of the devices incorporate RedBox Messages in their PRP packets. Behind the RedBoxes are five devices, accounting for 4.8% of the total devices. The network also includes two Serial to Ethernet Gateways, facilitating the connection of approximately 25% of the devices. And, 14.4% of the other SANs directly connect to the Ethernet switch without requiring a RedBox intermediary.

Figure 5 shows our inferred network architecture. In short, the critical devices in the network leverage the redundant PRP network, while less critical devices are only connected to one network interface. As we will see in the next phase, these critical devices are mostly IEDs, which are the devices that monitor and protect the substation equipment from accidents and failures.

6 Identifying Device Functionality

To identify device functionalities, we analyzed the protocols on the network.

Most (95%) of the network traffic consists of PRP, GOOSE, and TCP transmissions. PRP supervision packets comprise over 62% of the packets and 50% of the bandwidth, GOOSE contributes to more than 13% of packets and 31% of bandwidth, while TCP occupies 19% of packets and 15% of bandwidth.

This section details devices utilizing PRP, GOOSE, and TCP protocols.

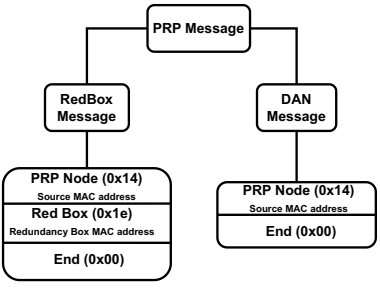

Fig. 4. Types of PRP packets

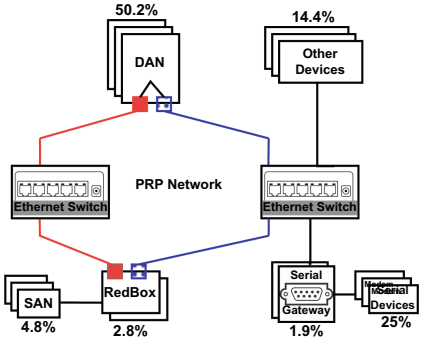

Fig. 5. Real-world substation network architecture

6.1 PRP

Most of the traffic in our network corresponds to heartbeat messages from the PRP protocol, so we are checking that the network is available. In more detail, DANs and RedBoxes regularly transmit PRP messages to notify other devices or network infrastructure that the originating device is still active and reachable, often known as "**heartbeat**" or "**keep-alive**" packets. These packets are small and multicast to a MAC address (`01:15:4e:00:01:00`), defined as PRP multicast address by an IEC standard [3].

The network capture shows that ABB AUTOM, SIEMENS, and IPCAS devices are DANs, and ABB SWITZ devices are RedBoxes with RedBox messages. All these devices are responsible for the PRP traffic.

Therefore, we confirm that all devices sending PRP traffic (connected to the redundant network) are industrial equipment that needs highly reliable communications [35]

6.2 GOOSE

After PRP traffic, GOOSE traffic is the second most prevalent in our network. GOOSE, a publish-subscribe protocol used by IEDs, facilitates the exchange of alarms, measurements, device statuses, or control commands via multicast frames. The IED standard [22] assigned the multicast addresses from `01:0c:cd:01:00:00` to `01:0c:cd:01:01:FF` to support this architecture.

We identify 28 devices publishing GOOSE messages to four multicast addresses in the network capture, as shown in Fig. 6. Among the 28 devices, 22 are manufactured by ABB AUTOM, four are SIEMENS, and two are IPCAS.

While we have identified a minimum of 28 IEDs in the network, we do not know what type of IEDs they are (e.g., a control switch, a protective relay, etc.) We also do not know if they communicate with one another: since this is a broadcast protocol, we cannot learn which devices consume the information sent by others. We need to analyze the SCD file we obtained to answer all these questions.

The goal of IEC 61850 is to facilitate substation automation, and SCD files are used to configure IEDs. Our SCD file contained information on all SIEMENS devices.

SCD File Analysis:

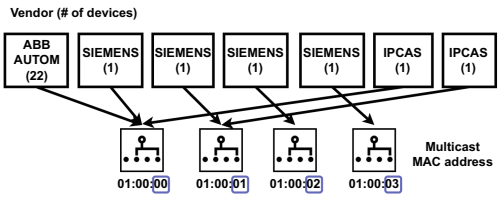

Fig. 6. PCAP analysis

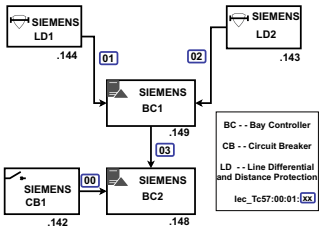

Fig. 7. SCD file analysis

The SCD file configures Fig. 10 SIEMENS devices, which correlates with the number of SIEMENS devices observed in our pcap file.

We identify IED types using the vendor's website [29]. For example, `6MD85` (shown in Listing 1.1) is listed as a SIEMENS Bay Controller. In the SCD file, we find three Bay Controllers (BC), two Circuit Breakers (CB), two Line Differential and Distance Protection (LD) devices, two Digital Fault Recorders (DFR), and a Busbar Protection device.

In the remainder of this paper, these devices are named BC1, BC2, BC3, CB1, CB2, LD1, LD2, DFR1, DFR2, and BB.

```
<IED iedName="BC2" type="6MD85" manufacturer="SIEMENS" .......>
    <LDevice desc="Signals" ....>
        <LN lnClass="GGIO" inst="2" desc="Goose">
            <Inputs>
                <ExtRef desc="Pos" iedName="BC1" ldInst="..."
                    lnClass="XCBR" lnInst="1" ... />
                <ExtRef desc="SPS4" iedName="CB1" ldInst="UD1"
                    lnClass="USER" lnInst="4" ... />
            </Inputs>
        </LN>
    </LDevice>
</IED>
```

Listing 1.1. Sample of Input signal. Subscriber: BC2. Publishers: BC1 and CB1

In addition to identifying devices, the SCD file provides information on which devices subscribe to GOOSE messages. While the pcap file can only indicate the devices that publish GOOSE messages, it does not provide information on devices that read them. We can determine which devices read GOOSE messages by examining the `<Inputs>` label in the SCD file, as shown in Listing 1.1. For example, we identify that the label inside the bay controller (BC2) instructs it to read messages from another bay controller (BC1) and circuit breaker (CB1) using the `iedName`. Through this analysis, we discovered that out of the ten devices, only two devices, namely the two Bay Controllers (BC1 and BC2), subscribe to GOOSE messages.

- ***BC1***: subscribes to two Line Differentials (***LD1 and LD2***).
- ***BC2***: subscribes to a bay controller and Circuit Breaker (***BC1 and CB1***).

This indicates that these BCs actively receive and process the GOOSE messages published by other devices within the network, as shown in Fig. 7.

Furthermore, suppose we want to learn the physical meaning of the messages they subscribe to. In that case, we can look at `lnclass`, which means Logical node class (defines the functionality of configured device), and `desc`, which means the description of the message configured.

The configuration of devices in the SCD file can have two types of Logical Nodes (LNs): (1) Standard and (2) User-Defined. The standard LNs define well-known functionalities such as Circuit Breaker (XCBR), Control Switch (CSWI), etc. The user-defined LNs (Generic Process I/O, GGIO) declare a functionality that the user gives and uses only when the functionality does not exist in standard or under catastrophic conditions.

Initially, we anticipated that all SCD files would adhere to well-known device configurations. However, we discovered that most functionalities in our SCD file were user-defined, which added complexity to our analysis as we had to establish connections between different device descriptions.

The standard configuration allows for the direct identification of input messages. For instance, in Listing 1.1, the input message from BC1 corresponds to the "Circuit breaker position" (denoted by XCBR for circuit breaker and Pos for Position). Conversely, to identify the message from CB1 (which utilizes a user-defined LN), we had to delve into CB1's configuration, search through all logical nodes for user-defined entries, and correlate them with the provided values in `Inputs` label to determine that it represents a "Busbar Interlocking Signal."

Unfortunately, the configuration of LD1 and LD2 also utilizes user-defined LNs. After an extensive search, we found BC1 subscribes to the "Busbar Interlocking Signal" and "Ground Interlocking Signal" messages from the Line Differentials. Table 4 lists the publisher and subscriber IEDs, the subscribed messages, and the corresponding Logical nodes. Below, we highlight the importance of these subscribed messages:

1. ***Busbar Interlocking*** is a control mechanism ensuring the safe operation of electrical busbars by coordinating device actions and maintaining network integrity and stability. It prevents faults, voltage transients, and excessive currents using predetermined rules or logic.
2. ***Ground Interlocking*** is a special case of busbar interlocking, where the busbar connects to the ground as an essential safety measure to protect personnel, equipment, etc.
3. ***Position of Circuit Breaker*** provides the status of the circuit breaker, whether ON/OFF or Transient. These inputs allow devices within the network to take appropriate actions, such as initiating protective measures or signaling other devices.

Using user-defined LNs complicates the configuration and poses challenges for modification during failures or outages. The SCD file analysis revealed unnecessary activation of user-defined LNs without utilizing their equivalent standard LNs, further adding complexity to the configuration.

Table 4. GOOSE input messages between IEDs

Subscriber	Publisher	Input	LN used
BC2	CB1	Busbar Interlocking (ON/OFF)	User Defined
BC2	BC1	Circuit break. Position (ON/OFF/Transient)	XCBR
BC1	LD1	Busbar and Ground Interlocking (ON/OFF)	User Defined
BC1	LD2	Busbar and Ground Interlocking (ON/OFF)	User Defined

In summary, our 14-hour GOOSE traffic analysis yields three key insights:

– The unchanged payload and timing of GOOSE messages indicate no critical events, affirming stable power grid conditions.

– All SIEMENS devices utilizing GOOSE are IEDs, suggesting that devices from vendors like ABB AUTOM and IPCAS could also be IEDs, totaling 53 in the network.
– The substation's configuration deviates from typical standards, likely due to vendors promoting proprietary setups that do not conform to a unified SCD file or standard LNs.

6.3 TCP

We finalize the analysis of this section by looking at TCP flows in our network, as they represent the third most popular traffic in the capture.

Almost all TCP traffic (99.95% of TCP flows) results from encapsulating serial communications to the serial devices behind the Serial to Ethernet proxy. The remaining TCP traffic includes 0.034% of TELNET packets and 0.011% of HTTP packets.

Serial to Ethernet (S2E): From the TCP traffic header, the S2E communication appears to be only with two devices, Moxatech Serial to Ethernet Gateways (M1 and M2). But, these devices expose multiple serial links [1].

Looking at the payload of the packets sending data as serial transmission (a stream of data bits sequentially transmitted), we find they are point-to-point `RS-232` serial links. It implies only one device connects to the gateway per serial link or ***one device per TCP destination port***.

The list of communicating ports for M1 are ***950-956; 959-960; 966-972; 975-976***, and M2 are ***950-953; 966-969***.

Looking at the different port numbers, we discover that behind the two S2E gateways are 26 devices, specifically, 18 connected to M1 and eight to M2.

We analyzed the payload of traffic sent to each port to identify the devices behind these ports. We find ASCII characters sent to 11 different ports.

For example, TCP packets sent from H1 to one of the M1 ports contained ASCII characters such as `Q`, `U`, `IT`, and `..` Analyzing these characters, we identified keywords like QUIT, ACCESS, OTTER, SHOWSET, etc. Looking online for these keywords, we find that they correspond to commands in the Schweitzer Engineering Laboratories (SEL) protocol [27], which is utilized by SEL IEDs. We find that nine devices were receiving these commands, indicating the presence of 9 SEL IEDs behind M1.

Two additional devices are receiving ASCII characters. The other device we could identify is a modem, as it receives `AT` commands that control the operation of a modem [31]. We could not identify the remaining device receiving ASCII characters, which include non-word characters like `@416DCF05S8A\r\n`.

We analyzed traffic from 11 devices out of the 26 S2E-connected devices. Among the remaining devices, 13 received data in an unidentified binary protocol, and two received only Acknowledgment (ACK) packets from H1.

We also notice that this substation employs **default passwords** (`OTTER`) to access these SEL IEDs [27] (detailed in Appendix A.3). This shows that the operators assume that any device inside the substation is trusted. This might be a reasonable assumption if the network is strongly segmented (or air-gapped) from external networks. Still, it

does raise some security concerns, as any device in the network can connect to these SEL IEDs and may be able to change their configuration.

In summary, our analysis of the serial communications reveals nine SEL IEDs, one modem, and 16 unknown devices behind M1 and M2.

TELNET: We will now finish our analysis of TCP flows by studying the other application layer protocols. In the network capture, we find 167 TELNET packets sent to four AMETEK devices (AME 1-4). TELNET is a text-based communication protocol, and in the pcap, we find the TELNET commands sent sequentially to each of the AMETEK devices in the order shown below:

→ 1 command of `SHOW DATE`
→ 30 commands of `SHOW TIME`
→ 1 command of `LIST RECORD`
→ (*if record exists*) sends a single packet with a group of commands for each record (`BATCH EXECUTE`; `SHOW RECORD <X>`; `SHOW MCCONFIG <X>`; `SHOW PROFILE <X>`; `SHOW FAULTDATA <X>`), where `<X>` represents record
→ 1 packet of `LIST RECORD`

We infer from these commands that the AMETEK devices may be fault recorders or a type of historian or database used to keep records of faults.

HTTP: 54 HTTP packets sent from H1 to a CADAC device include a combination of GET requests and POST status messages. Listing 1.2 shows the sample of a GET request:

```
GET /data/fault/....,....,...,FLN,RPV311,AlstomGrid,....,fault.
    zic HTTP/1.1\r\n
```

Listing 1.2. `GET` Sample

We find the model number `RPV311, AlstomGrid` from the GET request. Looking online, we find that it is a Digital Fault Recorder **DFR** (a type of IED) with Fault Location and Phase Measurement Unit (PMU) [30]. The Alstom-Grid RPV311 DFR captures and stores high-speed electrical waveform data during fault events.

6.4 Final Network Characterization

Besides the mentioned core devices, miscellaneous devices in the network play smaller roles. We now summarize our findings.

HP Computers (H2, H3, H4, H5): We discovered four additional HP computers in the network, apart from H1. These computers perform network broadcasts such as NetBIOS, LLMNR, DHCPv6, SSDP, IGMP, and Sentinel LDK UDP broadcasts. Sentinel LDK packets indicate the usage of proprietary software.

The payloads of NetBIOS host announcements reveal that these computers use Windows 7 or Windows Server 2008 operating systems, suggesting their roles as workstations. These workstations serve multiple purposes, including HMIs, alarm systems, control and monitoring devices, and enabling remote management and supervision of substation processes and equipment.

During analysis, H4 consistently exhibited packets with bad checksums due to checksum offloading (the network card allows hardware to calculate the checksum, causing random values in captured traffic). This behavior only affects the host capturing the network traffic and does not impact the transmitted packets, which identifies H4 as the computer responsible for capturing the traffic.

Industrial PC (IPC): We find two Industrial PCs from vendor Advantech. IPC is a specialized computer system designed to operate in harsh and demanding industrial environments. We only see NetBIOS and Sentinel LDK UDP broadcasts sent from this host. They use the Windows XP operating system from the NetBIOS host announcements.

MegaSystems Devices: We find three devices from the vendor MegaSystem Technologies in the network. The online information [2] reveals that these devices are UPS management cards that offer remote monitoring and control of a UPS by connecting it to the network.

RuggedComm Devices: In the network traffic, we find three RuggedComm Devices. They are robust industrial communication equipment designed for harsh environments and include networking components for reliable communication. One of these devices only receives NTP from a RedBox, and by observing the payload, we find it acts as an NTP client. The second one broadcasts STP, and the other sends ARP. We cannot identify the other two even after inspecting their payloads.

7 Timing Analysis

The preceding research [21], the GOOSE protocol's timing mechanisms for the same network capture was examined. This analysis shed light on the distribution and timing variations of data packets by focusing on the inter-arrival times and bandwidth utilization. The main findings include:

- Identifying a network behavior characterized by traffic segmentation into four clusters according to their packet inter-arrival spans - intervals of 2, 3.3, 5, and 10 s, respectively.
- Our clustering approach demonstrated a network exhibiting periodicity and latency, reinforcing the network's capability to maintain stability and communication patterns among connected devices over durations, as evidenced across a 14-hour monitoring timeframe.

Expanding upon these findings, in this research, we investigated the timing analysis of TCP traffic, contrasting it with the periodic nature of the previously studied PRP and GOOSE traffic, which covered the entirety of the 14-hour observation period. During the TCP traffic analysis, we observed packet dissections occurring within brief time

frames, suggesting a different operational dynamic compared to the transmissions of PRP and GOOSE packets.

To analyze this hypothesis, we implemented a "change detection" statistic on the amount of TCP packets we saw over a period of time. In particular, we implement the nonparametric CUmulative SUM (CUSUM) on the number of packets transmitted per second in the network traffic. We used Algorithm 1 to analyze this data, and Table 5 describes parameters used in the CUSUM algorithm.

Algorithm 1. Nonparametric CUSUM

```
procedure CUSUM(ΔP_t, t, τ)
    S_0 ← 0
    for t in ΔP_t do
        if t > 0 then
            S_t = S_t + S_{t-1} − δ                ▷ true ⟹ δ = 1
        else
            S_t = ΔP_t
        end
    if S_t ≥ τ then                                ▷ τ = median of S_t series
        The traffic includes data packets.
    else
        The traffic includes no data packets.
    end
```

Table 5. Parameters of CUSUM algorithm

Parameter	Description
t	Time in seconds
S_0, S_t	CUSUM value at $t = 0$ and $t = t$, respectively
ΔP_t	Difference in the number of transmitted packets between t and $t + 1$
τ	Threshold to classify packets transmitting data (constant)

The results, as shown in Fig. 8, indicate a clear storm of TCP activity in a limited time window. In particular, we find that this flurry of TCP activity started at around 7600 s (nearly 2 h) after the capture began and lasted for a maximum of 428 s (7.13 min). We also found that the time gap between the commands sent to the same device is less than 30 ms, which suggests that all the TCP traffic we analyzed was automated or pre-configured execution of scheduled jobs or tasks.

In addition to the big flurry of activity, we also see some smaller activity spread throughout the data capture. These smaller peaks correspond to a single connection to

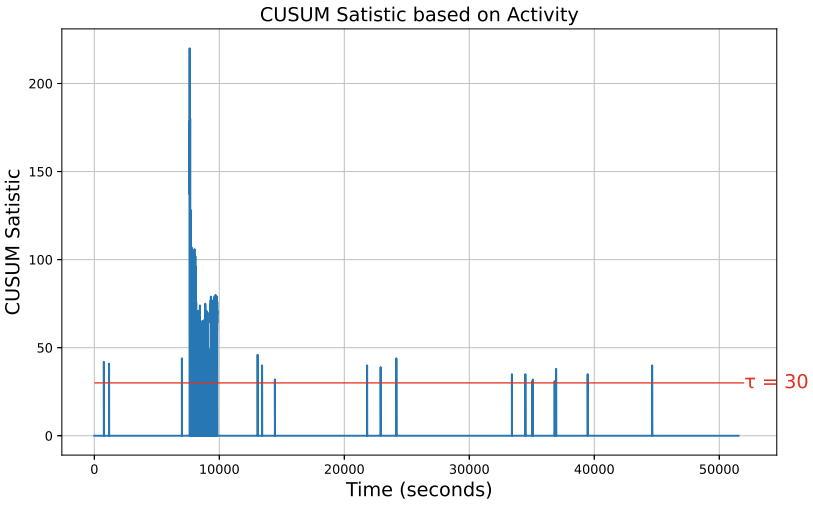

Fig. 8. Timing analysis of TCP protocol - CUSUM statistic

port 969 of gateway M2. Unfortunately, this is one of the few devices we could not identify.

8 Discussion

To finalize our analysis, we now illustrate the full substation network in Figure 9.

In summary, the real-world substation network analysis reveals:

- The vast majority of packets in the network correspond to keep alive (heartbeat) messages from two protocols: PRP and GOOSE. This shows that most of the traffic is used to check the network's status and to ensure that all devices are ready to act in case of an emergency event (e.g., an overcurrent).
- This leads us to the second observation: having long periods without events inside a real-world substation appears to be common.
- GOOSE traffic is broadcasted in the network, so classical flow analysis cannot identify destinations (or consumers of information). To obtain that information, we need SCD files.
- The configuration of the substation network does not follow standard procedures, such as using a single SCD file for all IEDs in the network or using standard LNs.
- The substation operates under a "trusted insider" assumption. This assumption may make sense if the network is fully segmented from the operational network and uses a private network. However, the modern trend in security is to assume "zero trust" networks (which means eliminating default trust assumptions, requiring verification for every access request regardless of location). So, we believe substations need to start following this zero trust configuration in the future to make them more resilient to potential future attacks.

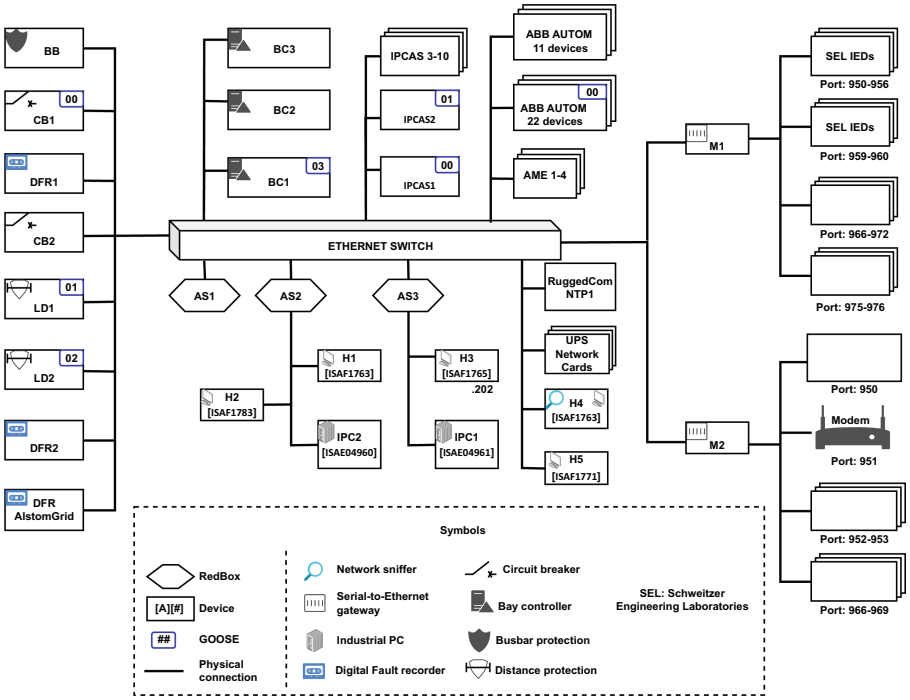

Fig. 9. Reconstructed substation network.

Our network analysis offers a unique perspective by investigating the coexistence of legacy devices and cutting-edge IEDs, setting us apart from existing literature. While previous research tends to focus exclusively on either IEC 61850 protocols [5,17,18] or legacy serial communication [6], our study examines both simultaneously. For instance, Chang et al. highlight the presence of IEDs and an HMI in station bus configuration, stating that *"The IEC61850 station bus interconnects 17 multifunction IEDs and the station HMI gateway unit through two independent LANs in a double-star configuration"* [8]. Similarly, other researchers acknowledge that *"IEDs connect the process bus and station bus"* [7,18,36]. However, our analysis uncovers that the real-world substation is more intricate, involving additional devices.

We draw attention to the existence of proxies and serial devices, which have not been discussed in previous research studies about substation networks.

We also highlight our effort to use data from actual measurements and perform a detailed architecture of the substation. As far as we are aware, Formby et al. [10] is the only other research paper discussing data from an operational substation; however, Formby provides only traffic flow analysis and does not attempt to enumerate all devices and protocols used in these networks, giving us only a glimpse of what their substations look like.

Our inspection of GOOSE packets revealed individual timestamp values for each IED, highlighting the reliance on external synchronization sources. Time synchroniza-

tion is crucial in substation networks, as failures can lead to artificial phase shifts and potential tripping [28]. The IEC 61850-7-5 standard emphasizes the need for careful consideration of time synchronization [26] to prevent undesired consequences.

Furthermore, our analysis of the SCD file provided valuable insights into the substation's configuration. We discovered that the substation relied on segmented SCD files, which can challenge managing and updating the design. Previous research, such as Wang et al. [34], has proposed management and control modules for more accessible configuration file updates. Still, segmented files add another layer of complexity to this task.

Additionally, our analysis of the SCD file revealed the use of generic user-defined Logical Nodes (GGIO) in the substation. While GGIOs provide flexibility in cases where the IEC 61850 standard lacks a standardized structure, they come at the cost of losing functional descriptions. This deviation from specialized logical nodes and reliance on GGIOs can impact the interoperability and traceability of information over time, as noted by Kaneda et al. [16].

It is also worth mentioning that besides industrial protocols, some devices, such as SEL IEDs, utilize proprietary protocols over serial communications. We are not aware of other papers discussing this use in substations. The existence of these devices and unencrypted protocols may also raise many security concerns. One such finding is the use of default passwords, like `OTTER`, to access these IEDs, despite the option for users to modify them according to the manuals [27]. This neglect of changing default passwords can allow unauthorized personnel to access these devices. The attacks against the power grid in Ukraine are a stark reminder that sophisticated adversaries are now targeting the power grid [9].

Impacts of Findings and Future Design Strategies for Substation Networks: From our analysis, we have summarized some of the implications and suggestions for future design strategies below:

1. ***Redundant Paths on Network Reliability and Efficiency:*** The study's findings on redundant paths, mainly through protocols like PRP, significantly boost network reliability and fault tolerance. With advanced monitoring and management systems, careful planning and implementation of redundant paths can optimize reliability while minimizing efficiency overhead.
2. ***IEDs and their evolution in future substation designs***: The study highlights the role of IEDs in substation automation and the critical need for cybersecurity in safeguarding vital infrastructure. As substation automation progresses, IEDs become essential for enhancing system intelligence, efficiency, and resilience. Future IEDs may integrate advanced cybersecurity features, such as secure communication protocols and encryption, to counter cyber threats effectively.
3. ***Identified vulnerabilities and recommendations for cybersecurity:*** The analysis revealed several vulnerabilities in the substation network's cybersecurity posture, including:
   - Lack of encryption for sensitive communication channels, leaving data vulnerable to interception and tampering.
   - Inadequate access control measures, allowing access to critical devices and systems multiple times unlimitedly.

To address these vulnerabilities and enhance cybersecurity:
- Implement end-to-end encryption for critical communication channels to protect data confidentiality and integrity.
- Enforce strong access control policies, including restricting any unauthorized access.
- Regularly update firmware and software on network devices to patch known vulnerabilities and mitigate security risks.
- Deploy intrusion detection and prevention systems to monitor network traffic for anomalies.

4. ***Enhancement of Network Understanding through SCD File Analysis and Challenges Encountered:*** By analyzing the SCD file, we can:
   - Identify network devices, functionalities, and interconnections based on the standardized IEC 61850 data model.
   - Validate device configurations and communication mappings against the intended network design and operational requirements.
   - Document network configurations and settings for maintenance, troubleshooting, and future upgrades.

   However, challenges encountered in using the SCD file include:
   - Complexity in parsing and interpreting the XML-based format of the SCD file, requiring specialized tools or scripts for analysis.
   - Inconsistencies or discrepancies between the SCD file and the network configuration necessitate manual verification and validation.
   - Limited support for proprietary extensions or vendor-specific configurations, leading to incomplete or inaccurate network representations.

   Despite these challenges, the SCD file remains valuable for understanding substation networks and facilitating effective network management and optimization.

9 Conclusion

As far as we know, in this paper, we provide the most detailed view of an operational substation network. We also present a novel framework for analyzing and understanding such networks by analyzing packet captures and utilizing an SCD file.

Our study found topics not commonly discussed in the industrial control network literature, such as the use of redundant Ethernet networks to guarantee reliability, the existence of several proxies (Red Boxes and Serial to Ethernet Converters), and the coexistence of legacy serial IEDs with modern IEDs following the GOOSE protocol. Most of the devices in the network were IEDs (63), emphasizing the critical role of these devices in substation automation.

We hope this study motivates future work to characterize and understand these critical networks, and perform ongoing asset inventory to identfy devices that need protection, as well as to identify any new malicious endpoint added to the network.

Acknowledgments. This work was partially supported by the Air Force Office of Scientific Research under award number FA9550-24-1-0015, by the NSF CPS program under CNS-1929410 and by the INTERSECT project, Grant No. NWA.1162.18.301, funded by the Netherlands Organisation for Scientific Research (NWO).

A Concepts of Substation

A.1 Information Model

The IEC 61850 standard defines a hierarchical information model as shown in Fig. 10 that includes:

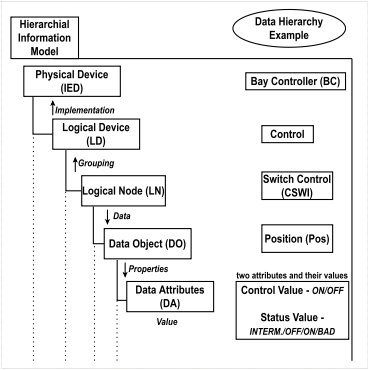

Fig. 10. Hierarchial Information Model

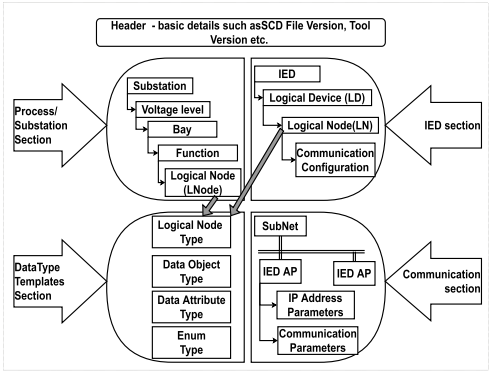

Fig. 11. SCD File Template

IED (or) Physical Device: This is the device connected to the network directly.

Logical Device (LD): The LDs are logical containers organizing the information of an IED, splitting it into different categories. Vendors categorize their information using logical device names such as PROT(protection), CTRL (control), REC (recorder), etc.

Logical Node (LN): The LNs are the functions or components that automate the system.

They are named by four letters; the first indicates their category. For example, LN CSWI stands for Control Switch.

Data Object (DO): Each LN includes a set of mandatory and optional data objects to fulfill their actions. The data objects represent status information, position, measurements, set points, controllable points, or descriptive information.

Data Attribute (DA): Each Data Object includes a group of data attributes that define the properties of the object. For example, properties such as Control Value, Status Value, timestamp, etc.

A.2 Substation Configuration Description

Integration of substation equipment is a complex task in the automation process. Using a standardized format to configure various IEDs' networking capabilities, equipment functionality, is vital in improving the performance Hence, Part 6 of the IEC 61850 standard defines the Substation Configuration description Language (SCL/SCD) that describes functions of IED and its communication network using extensive markup language (XML) schema [13]. Figure 11 shows a substation's template of an SCD file. Every SCD file template contains five main sections [33], defined as follows:

- ***Header:*** It helps to identify the version of the IED configurator used to create the SCD file.
- ***Substation:*** It defines the substation's name and its different entities, including various devices, interconnections, and other functionalities that help identify electrical connections and functions.
- ***Communication:*** This section describes the communication network of IEDs and the protocols they can use. For example, if an IED uses GOOSE, it is configured using a sub-element `GSE`.
- ***IED:*** This section describes the complete configuration (functions, access points, logical devices, logical nodes, data objects, inputs, and other information) of the connected IED. This section also helps to identify the interconnection between the logical nodes of multiple IEDs.
- ***DataType Templates:*** It provides a standardized structure for defining various communication data formats and characteristics. These templates ensure consistency and interoperability between devices and systems.

A.3 SEL Device Functionality in the Real-World Network

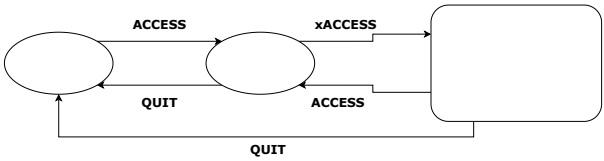

Fig. 12. Transition between different access levels in SEL devices

There are seven access levels in SEL devices. The ACCESS command is sent to enter any access level. If password protection is enabled, then it prompts for the password. The default password for access level 1 is OTTER, and access level 2 is TAIL. In access level 1, we can read the data and status information; in access level 2, we can also write the data. Access level B performs breaker control and shows breaker data. Access levels P, A, and O show protection settings, automation settings, and output settings, respectively, along with the functions of access level B. In the deep packet inspection, we only find commands from three access levels (access level 0, access level 1, and a single command from access level 2). These commands provide read access to different information. If an access level 2 command is used, we can write data to these devices from host machines [27]. Figure 12 shows the transition between different access levels in SEL devices.

The QUIT command sends the system to Access level 0 from any given level. Users utilize this command after communicating with the device to prevent unauthorized access.

The HISTORY command summarizes up to 40 previous events. Each summary shows the date, time, event type, fault location, active setting group, and targets.

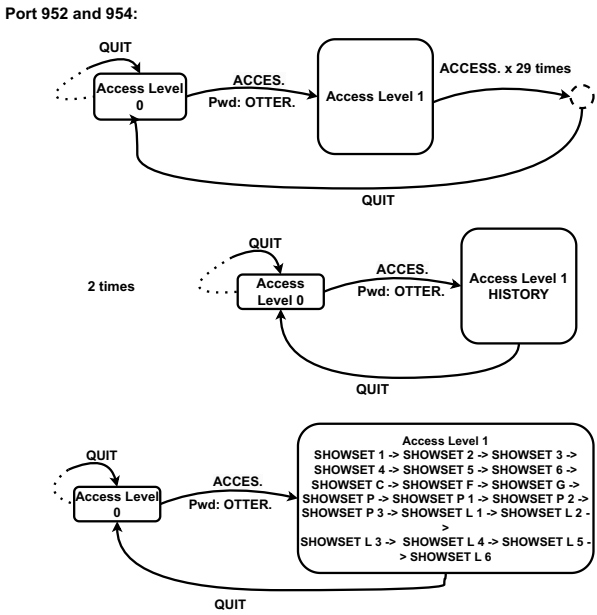

Fig. 13. State machine of commands to ports M1:952 and M1:954

The SHOWSET command displays the device settings for the selected group. One should use the command SET at access level 2 to perform update/write operations on these settings. Table 6 shows different SHOWSET commands. SHOWSET with 'A' displays all the inactive settings.

The STATUS command allows inspection of self-test status. The device executes the STATUS command whenever the self-test software enters a warning or failure state.

The TIME command displays and sets the internal clock.

We now summarize the commands we see and their destination:

– Commands to SEL Devices:
  - ***M1:950***: `QUIT`.
  - ***M1:951***: `QUIT, ACCESS/OTTER, ACCESS, SHOWSET, HISTORY`
  - ***M1:952, 954***: `QUIT, ACCESS/OTTER, ACCESS`(multiples times in a row), `HISTORY, SHOWSET 1-6, SHOWSET C, SHOWSET F, SHOWSET G,`
    `SHOWSET P, SHOWSET P 1-3, SHOWSET L 1-6.`
  - ***M1:[953, 955, 956, 960]***: `QUIT, ACCESS/OTTER, ACCESS` (multiple times in a row), `HISTORY, SHOWSET`
  - ***M1:959***: `QUIT, ACCESS/OTTER, HISTORY, SHOWSET, DATE, TIME` (multiple times in a row).

Most of these commands happen repeatedly. For example, in Fig. 13, which represents the state machine of commands sent to ports 952 and 954 of M1, H1 sends

Table 6. Command summary of SEL devices

Command	Description
Access Level 0	
ACCESS	enters level 1; password OTTER
Access Level 1	
2ACCESS	enters level 2; password TAIL
HISTORY	DATE, TIME, etc., for the last 40 events
QUIT	returns control to Access Level 0
SHOWSET n	active group settings for Group n
SHOWSET C	calibration settings
SHOWSET G	global settings
SHOWSET L	active logic settings
SHOWSET P	active port settings
STATUS	self-test status
TIME	Shows or sets time
Access Level 2	
SHOWSET F	future re-calibration settings

`ACCESS` command 29 times, despite reaching access level 1. It is followed by `QUIT` and returns to access level 0. It again enters access to level 1 and requests the settings of these devices connected to 953 and 954.

References

1. Which TCP/UDP ports do i need to open to access my mgate gateway remotely? https://www.moxa.com/en/support/product-support/product-faq/which-tcp-udp-ports-to-open-to-access-mgate-gateway-remotely. Accessed 05 May 2022
2. Megatec product list (1998-2004). http://www.megatec.com.tw/Product_list.htm. Accessed 05 May 2022
3. Araujo, J., Lázaro, J., Astarloa, A., Zuloaga, A., García, A.: PRP and HSR version 1 (IEC 62439-3 ed.2), improvements and a prototype implementation. In: IECON 2013 - 39th Annual Conference of the IEEE Industrial Electronics Society, pp. 4410–4415 (2013). https://doi.org/10.1109/IECON.2013.6699845
4. Barbier, G., Conti, M., Tippenhauer, N.O., Turrin, F.: Assessing the use of insecure ICS protocols via IXP network traffic analysis. In: 2021 International Conference on Computer Communications and Networks (ICCCN), pp. 1–9 (2021). https://doi.org/10.1109/ICCCN52240.2021.9522219
5. Biswas, P.P., Tan, H.C., Zhu, Q., Li, Y., Mashima, D., Chen, B.: 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), pp. 1–7 (2019). https://doi.org/10.1109/SmartGridComm.2019.8909783

6. Boakye-Boateng, K., Siahaan, I.S.R., Al Muktadir, A.H., Xu, D., Ghorbani, A.A.: Sniffing serial-based substation devices: a complement to security-centric data collection. In: 2021 IEEE PES Innovative Smart Grid Technologies Europe (ISGT Europe), pp. 1–6 (2021). https://doi.org/10.1109/ISGTEurope52324.2021.9640212
7. Buhagiar, T., Cayuela, J.P., Procopiou, A., Richards, S., Ramlachan, R.: Smart substation for the French power grid. In: 69th Annual Conference for Protective Relay Engineers (CPRE). IEEE (2016). https://doi.org/10.1109/CPRE.2016.7914915
8. Chang, J., Vincent, B., Reynen, M.: Protection and control system upgrade based on IEC-61850 and PRP. In: 2014 67th Annual Conference for Protective Relay Engineers, pp. 496–517 (2014)
9. CyberSecurity & Infrastructure Security Agency: Cyber-attack against Ukrainian critical infrastructure (2021). https://www.cisa.gov/news-events/ics-alerts/ir-alert-h-16-056-01/
10. Formby, D., Walid, A., Beyah, R.: A case study in power substation network dynamics. SIGMETRICS Perform. Eval. Rev. **45**(1), 66 (2017). https://doi.org/10.1145/3143314.3078525
11. Hoga, C., Wong, G.: Utilities and industries gain benefits as IEC 61850-implementation gains speed. In: 2005 IEEE Power Engineering Society Inaugural Conference and Exposition in Africa, pp. 176–179 (2005)
12. Huang, W.: Learn IEC 61850 configuration in 30 minutes. In: 2018 71st Annual Conference for Protective Relay Engineers (CPRE), pp. 1–5 (2018). https://doi.org/10.1109/CPRE.2018.8349803
13. Ingalalli, A., Silpa, K.S., Gore, R.: SCD based IEC 61850 traffic estimation for substation automation networks. In: 2017 22nd IEEE International Conference on Emerging Technologies and Factory Automation (ETFA), pp. 1–8 (2017). https://doi.org/10.1109/ETFA.2017.8247596
14. Juárez, J., Rodríguez-Morcillo, C., Rodríguez-Mondéjar, J.A.: Simulation of IEC 61850-based substations under omnet++. In: SIMUTOOLS 2012, ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), Brussels, BEL, pp. 319–326 (2012)
15. Kanabar, M.G., Sidhu, T.S.: Performance of IEC 61850-9-2 process bus and corrective measure for digital relaying. IEEE Trans. Power Deliv. **26**(2), 725–735 (2010)
16. Kaneda, K., Tamura, S., Fujiyama, N., Arata, Y., Ito, H.: Iec61850 based substation automation system. In: 2008 Joint International Conference on Power System Technology and IEEE Power India Conference, pp. 1–8 (2008). https://doi.org/10.1109/ICPST.2008.4745296
17. Konka, J.W., Arthur, C.M., Garcia, F.J., Atkinson, R.C.: Traffic generation of IEC 61850 sampled values. In: 2011 IEEE First International Workshop on Smart Grid Modeling and Simulation (SGMS), pp. 43–48. IEEE (2011)
18. Kwon, Y., Lee, S., King, R., Lim, J.I., Kim, H.K.: Behavior analysis and anomaly detection for a digital substation on cyber-physical system. Electronics **8**(3) (2019). https://doi.org/10.3390/electronics8030326
19. León, H., Montez, C., Stemmer, M., Vasques, F.: Simulation models for IEC 61850 communication in electrical substations using goose and SMV time-critical messages. In: 2016 IEEE World Conference on Factory Communication Systems (WFCS), pp. 1–8 (2016). https://doi.org/10.1109/WFCS.2016.7496500
20. León, H., Montez, C., Valle, O., Vasques, F.: Real-time analysis of time-critical messages in IEC 61850 electrical substation communication systems. Energies **12**(12) (2019). https://doi.org/10.3390/en12122272
21. Lozano, J., Koneru, K., Castellanos, J.H., Cardenas, A.A.: Timing analysis of goose in a real-world substation. In: 2022 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm), pp. 160–165 (2022). https://doi.org/10.1109/SmartGridComm52983.2022.9961030

22. Mackiewicz, C.R.: Technical overview and benefits of the IEC 61850 standard for substation automation. https://api.semanticscholar.org/CorpusID:17966971
23. Mai, K., Qin, X., Ortiz, N., Molina, J., Cardenas, A.A.: Uncharted networks: a first measurement study of the bulk power system. In: Proceedings of the ACM Internet Measurement Conference, IMC 2020, pp. 201–213. Association for Computing Machinery, New York (2020). https://doi.org/10.1145/3419394.3423630
24. Nivethan, J., Papa, M., Hawrylak, P.: Modeling and simulation of electric power substation employing an IEC 61850 network. In: Proceedings of the 9th Annual Cyber and Information Security Research Conference, CISR 2014, pp. 89–92. Association for Computing Machinery, New York (2014). https://doi.org/10.1145/2602087.2602096
25. Ortiz, N., Rosso, M., Zambon, E., den Hartog, J., Cardenas, A.A.: From power to water: dissecting SCADA networks across different critical infrastructures. In: International Conference on Passive and Active Network Measurement, pp. 3–31. Springer (2024)
26. Ozansoy, C.R., Zayegh, A., Kalam, A.: Time synchronisation in a IEC 61850 based substation automation system. In: 2008 Australasian Universities Power Engineering Conference, pp. 1–7 (2008)
27. Schweitzer Engineering Laboratories: Changing the default passwords; table 4.3 sel-421 relay access levels; figure 4.5 access level structure - sel -421 user manual (2012). https://www.manualslib.com/manual/1645670/Sel-Sel-421.html. Accessed 13 May 2022
28. Shrestha, A., Silveira, M., Yellajosula, J., Mutha, S.K.: Understanding the impacts of time synchronization and network issues on protection in digital secondary systems. In: PAC World Global Conference 2021 (2021)
29. Siemens AG: Siemens SIPROTEC 5 Portfolio. https://new.siemens.com/global/en/products/energy/energy-automation-and-smart-grid/protection-relays-and-control/siprotec-5.html. Accessed 05 May 2022
30. GG Solutions: Reason RPV311. https://www.dsgenterprisesltd.com/product/ge-reason-rpv311-digital-recorder/
31. TW Solutions: At commands reference guide. https://www.sparkfun.com/datasheets/CellularModules/AT_Commands_Reference_Guide_r0.pdf. Accessed 05 May 2022
32. Stiller, N.: Mac address lookup (2019). https://www.macvendorlookup.com/
33. Wang, J., Wang, Z.: Research and implementation of virtual circuit test tool for smart substations. Procedia Comput. Sci. **183**, 197–204 (2021)
34. Wang, L., Huang, J., Zhang, C.: Design and development of SCD file management and control system for serving substation reconstruction and expansion projects. In: 2022 IEEE 10th Joint International Information Technology and Artificial Intelligence Conference (ITAIC), vol. 10, pp. 1782–1790 (2022). https://doi.org/10.1109/ITAIC54216.2022.9836958
35. Weibel, H.: Tutorial on parallel redundancy protocol (PRP) (2003). http://caxapa.ru/thumbs/767218/tutorial-on-prp.pdf
36. Wong, T.J., Das, N.: Modelling and analysis of IEC 61850 for end-to-end delay characteristics with various packet sizes in modern power substation systems. In: 5th Brunei International Conference on Engineering and Technology (BICET 2014), pp. 1–6 (2014). https://doi.org/10.1049/cp.2014.1073
37. Zhao, J., et al.: A network scheme for process bus in smart substations without using external synchronization. Int. J. Electr. Power Energy Syst. **64**, 579–587 (2015). https://doi.org/10.1016/j.ijepes.2014.07.066. https://www.sciencedirect.com/science/article/pii/S0142061514005018