Title

A Taxonomy of Industrial Control Protocols and Networks in the Power Grid

Journal

IEEE Communications Magazine, 61(6)

ISSN

0163-6804

Authors

Ortiz, Neil

Cardenas, Alvaro A

Wool, Avishai

Publication Date

2023-06-01

DOI

10.1109/mcom.001.2200574

Peer reviewed

A Taxonomy of Industrial Control Protocols and Networks in the Power Grid

Neil Ortiz, Alvaro A. Cardenas, and Avishai Wool

Abstract

Despite a growing interest in understanding the industrial control networks that monitor our critical infrastructures (such as the power grid), to date, these networks have been analyzed in isolation from each other and treated as monolithic networks without consideration of the differences. In this article, we use five industrial control protocols to showcase the diversity of applications and usage of these systems. We introduce a taxonomy of industrial protocols and a summary of their security challenges.

The authors introduce a taxonomy of industrial protocols and a summary of their security challenges.

Introduction

Power grids are complex systems with multiple networks and a variety of industrial protocols. Each network has distinct configurations tailored to the specific needs of the system. There are protocols for different communication purposes (synchronous and asynchronous, request/response and, unsolicited communications), and models (client/server or publisher/subscriber). Some protocols are designed for fast response to events, and others for carrying large amounts of data. Some networks transmit data long distances, and others keep it localized. While some are for monitoring stable-state events, others are for transient events. Considering this diversity, we have collected datasets from different operators in the power grid. In this article, we use our experience with these datasets to give a brief primer overview of the protocols, propose a taxonomy, and discuss their similarities and differences.

Related Works

In the past two decades, the Supervisory Control and Data Acquisition (SCADA) systems have migrated from serial communications to IP-based and Ethernet networks. However, there has been limited academic research on network traffic for industrial control systems (ICS), particularly for power grids. We identify two main limitations:

1. Analyzing emulated or simulated data is the most popular approach due to the difficulty of obtaining real-world data from operational power grids.
2. The academic community tends to analyze a single network using a single industrial protocol, which gives only a small representation of these critical networks.

Most of the interest in SCADA networks from the academic community focuses on security. Lin *et al.*[1], Stylianou *et al.* [2] and Bohara *et al.* [3] use simulated data and testbeds to model IEC 60870-5-104 (IEC 104), C37.118, and GOOSE traffic, respectively. Yet, simulations or testbeds do not represent real behaviors in the power grid network. As Lian and Nadjim-Tehani's study showed [4], emulated datasets are prone to simple and regular patterns.

Two papers using real-world data from an operational power grid include Mai *et al.* [5], and Formby *et al.* [6]. Mai analyzes and characterizes IEC 104 traffic from a real system during two consecutive years. They revealed topological changes from year to year and found important misconfigurations. However, their work focused on a single protocol. Formby *et al.* analyzed a real-world distribution substation that uses the DNP3 industrial control protocol. They analyzed the flow of traffic in the transport layer. This article focused on only one part of the protocol without considering its characteristics in the application layer.

In all these previous works, researchers tend to refer to SCADA protocols as a monolithic entity; they do not identify where each protocol fits in the ICS ecosystem. We aim to show that the traffic characteristics of each protocol are unique and serve distinct purposes. We believe a short article conveying this message can be helpful to researchers who want to enter this field and can help them position their SCADA network analysis in the context of related work.

Networks in the Power Grid

Power grids are systems used to generate, transmit, and distribute electricity over large geographical regions. There are three interconnected networks: generation, transmission, and distribution. They deliver the energy from remote generation plants to end-customers. The Bulk Power Grid (BPG) usually refers to large generation plants and the transmission systems. While BPG is a redundant grid covering a large geographical area, distribution systems are small radial (non-redundant) grids covering small geographical areas.

Network Endpoints

Electrical substations are distributed nodes in the power system which can be staffed or unattended. From control rooms, operators remotely monitor and maintain the system's safety by controlling power flow. Operational Technologies (OT) enable the communication between operators and substations. They consist of a variety

Neil Ortiz and Alvaro A. Cardenas are with the University of California Santa Cruz, USA; Avishai Wool is with Tel-Aviv University, Israel.

Digital Object Identifier: 10.1109/MCOM.001.2200574

The main players in the bulk power grid are the transmission owners and the system operators

of embedded devices and classical computers which measure, control, and monitor the physical processes in the substation and transmit the data to the control room. These devices/computers together with the control room, we label as endpoints in our taxonomy.

The following list summarizes the most common **endpoints** we have encountered in our study of power grid communications:

Control Room (CR) The control room, as the center of operations, orchestrates physical processes in the system, (such as power flow, voltage level, and frequency). They are computers collecting data from remote devices, (often referred to as "the SCADA"). They usually interface with other computers such as databases (a.k.a Historian) and Human Machine Interfaces (HMI) that operators can use to visualize the state of the physical process being managed.

Intelligent Electronic Device (IED) An IED is an embedded computer that receives data from sensors, i.e., measurement transformers, and sends commands to power equipment, e.g., circuit breakers directly. Relays and digital fault records are examples of IEDs. Engineers deploy IEDs within a substation and only communicate locally with other IEDs or computers inside the substation (e.g., an RTU or a local CR). Because of the safety-critical nature of their operation (e.g., automatically disconnecting an overloaded electric line before a fire starts), they need to operate over highly-reliable and low-latency local networks.

Remote Terminal Units (RTU) Similar to an IED a RTU is an embedded computer that collects data mainly from IEDs, and then delivers it to the CR. While IEDs are employed for communication within a substation, RTUs are used for external communication. RTUs have been the traditional endpoint for exchanging data between a CR and a substation, but some modern substations utilize **substation gateways** as endpoints.

Programmable Logic Controller (PLC) A PLC is another industrial computer used to automatically control a physical process. They are more widely used in industry, such as water, chemical, and manufacturing systems. While IEDs focus on protecting electrical equipment, PLCs focus on controlling power generation machines. They are also popular in commercial end-consumer applications.

Phasor Measurement Unit (PMU) A PMU is a sensor that collects voltage and current values and calculates their synchrophasor measurements. They operate at a very high-frequency and in a time-synchronized way. They can be a standalone device or incorporated into an IED. It is a relatively new technology that is much faster and more time accurate (to the order of one millisecond) compared with the traditional SCADA technologies. They are used in Wide-Area Monitoring Systems (WAMS) and in synchrophasor-base Wide-Area Monitoring Protection and Control (WAMPAC) applications.

Operators

Several companies operate the BPG and the distribution system, and each company runs one (or several) industrial networks to supervise the power grid. The main players in the bulk power grid are the transmission owners and the system operators.

Transmission Owners own assets in the transmission system, such as electrical towers and substations, along with the associated equipment, such as transformers and circuit breakers. They need industrial networks to connect their central control room(s) to remote substations.

System Operators orchestrate the operation of the power companies. In the U.S., system operators are called either Regional Transmission Operators (RTO) or Independent System Operators (ISO), depending on whether they oversee the power grid of several states (RTO) or one state only (ISO). The system operator needs a network to exchange information with multiple power system operators. In addition, the operator runs the Automatic Generation Control (AGC) algorithm to control the power output of electric generators within an area in response to the system frequency or tieline loading. Therefore the operator will need a network to communicate control commands from the CR to generation substations. Finally, they may also receive PMU data for wide area monitoring, and therefore will need a PMU network.

Distribution Owners (including electric utilities) own assets at the distribution level and manage several distribution substations, distribution lines, and the delivery to end consumers. They need industrial networks to receive data from substations and send control commands to them.

Consumers receive electric power from distribution utilities. While many consumers are residential, others are commercial or institutional consumers (e.g., a university campus) which supervise their electricity consumption among different buildings. They need a network connecting the CR to different PLCs in buildings.

Industrial Networks and Protocols

Figure 1 illustrates the relationships between some of the operators mentioned above. The bottom figure represents the physical layer of the BPG. Generation plants (in blue) are connected to the electrical transmission system. Each node in the physical layer is a substation. The top part of the figure pictures the cyber layer. It displays the connections of a variety of endpoints. The red node represents the CR of a main system operator. The system operator communicates with multiple endpoints, such as the CRs of Transmission Owners (blue nodes) and RTUs in substations (black nodes). The link between connections is illustrated with various colors to represent the different protocols used to communicate. For example, the ISO (main CR) uses the industrial protocol ICCP to exchange information with the CRs of Transmission owners (red links), IEC 104 to perform AGC in generation substations (green links), and IEEE C37.118 to receive information from PMUs (orange link).

Protocols Description

Even though SCADA systems use a wide variety of communication protocols, this work focuses on only five: IEC 60870-5, ICCP, GOOSE, Modbus TCP, and IEEE C37.118. They are the specific protocols contained in a dataset that we collected from operating power grids. While our list is not exhaustive, we believe that these protocols represent a sample of the diversity in these networks and will suffice for the scope of our study.

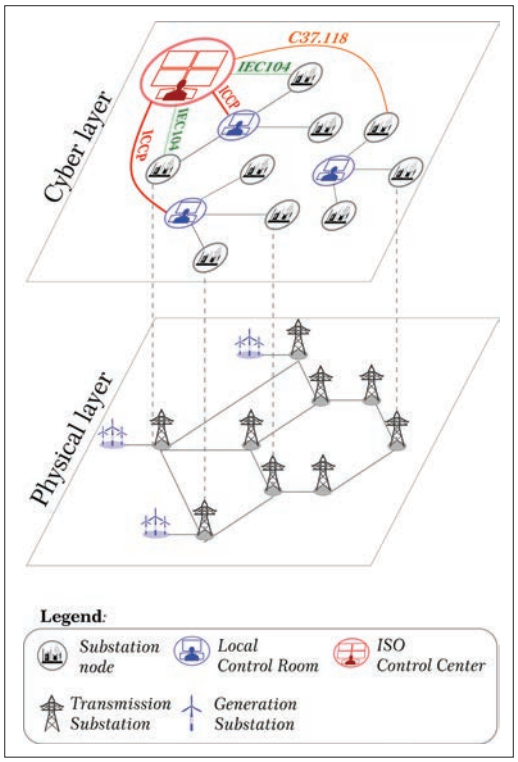

FIGURE 1. Cyber-Physical abstract representation of a Bulk Power Grid. Wide area monitoring depends on different protocols.

Figure 2 further illustrates how the dataset we obtained from different operators functions in the power grid. At generation level, the system operator uses IEC 104 (and its serial line equivalent IEC 101) to monitor the power grid and to send AGC control commands to generation substations. At the transmission level, ICCP facilitates data exchange between control centers. IEC 104 (and IEC 101) transmits regular SCADA data from substations to CRs and IEEE C37.118 transmits synchrophasor data to CRs of different transmission substations. Inside a substation, communications are standardized by IEC 61850. This standard includes multiple protocols, among them: MMS (communicates between CRs and IEDs), GOOSE (communicates between IEDs), and SV (communicates between IEDs and physical processes). On the distribution side, we see again the use of IEC 104 to connect the CR of electric utilities with distribution substations. Finally, at the end-customer level, a university CR uses Modbus TCP to supervise PLCs in different buildings on a campus network. As we can see, IEC 104 is a widely used protocol in the power system.

We will now give a brief overview of these protocols and will finish with our taxonomy and analysis.

IEC 60870-5 (101 AND 104)

When SCADA was first deployed, serial communication like Modbus and IEC 101 emerged as the communication standards. They served as a communication solution for exchanging data between equipment from different manufacturers. IEC 60970-5-101 (a.k.a IEC 101) enables telecontrol messages between CR and substations. This point-to-point serial communication uses a low bandwidth bit-serial communication to transmit data objects and services over geographically wide areas. It also supports multi-drop communication (several devices connected to a single serial channel) in a client/server model. In addition, it uses balanced and unbalanced communications (in balanced communications, any party can initiate data transfers) and data acquisition by polling, cyclic transmission, spontaneous event, and general interrogation.

Later, with Ethernet and TCP/IP-based networking, a new range of SCADA protocols appeared. Protocols such as Modbus TCP, IEC 104, and DNP3 facilitate remote operation, maintenance, machine configuration, and interoperability across vendors. IEC 104 is an application layer protocol that transmits over TCP/IP using a client/server model. This protocol permits synchronous and asynchronous messages (a.k.a spontaneous/periodic messages) for balanced/unbalanced communications. In addition, it allows timestamps and quality attributes in the messages.

When SCADA was first deployed, serial communication like Modbus and IEC 101 emerged as the communication standards.

ICCP

Inter-Control Center Communications Protocol (ICCP) exchanges time-critical data over WANs among CRs. This data exchange includes real-time monitoring and control data, measurement data, accounting data, and operator messages. It is widely used to tie together groups of utility companies, typically a regional system operator with the transmission, and distribution utilities, and generators. For example, regional operators may coordinate the import and export of power between regions across major inter-ties. In addition, Operators can use ICCP to exchange information between applications within a single control center. i.e., data exchange between the control center's Energy Management System (EMS) and a historian or SCADA [7].

ICCP can operate over either an ISO-compliant transport layer or a TCP/IP transport layer (although TCP/IP over Ethernet is the most common). In addition, ICCP employs a client/server model and sits in the upper sub-layer of layer 7 in the OSI reference model. A CR can be both a client and a server. All data transfers originate with a request by a CR to another CR that owns and manages the data. Each ICCP server performs access control on all incoming client requests based on bilateral association agreements. ICCP uses another industrial protocol MMS (Manufacturing Message Specification), for the required messaging services.

GOOSE

The Generic Object Oriented Substation Events (GOOSE) is a communication protocol defined by the IEC 61850 standard [8]. The IEC 61850 is an international standard that defines communication protocols to provide interoperability between all types of IEDs in a substation. GOOSE exchanges protection-related events (commands, alarms, and status) across digital substation networks.

It is an event-based protocol. The main objective of GOOSE messaging is to provide a fast and reliable way to exchange data sets between two or more IEDs. GOOSE enables the user to group any data format (status, value) into a data set. It works directly over the Ethernet layer and follows a multicast communication model (a non-routable protocol that does not use IP addresses). To exchange data, GOOSE uses a publish/subscribe model [9].

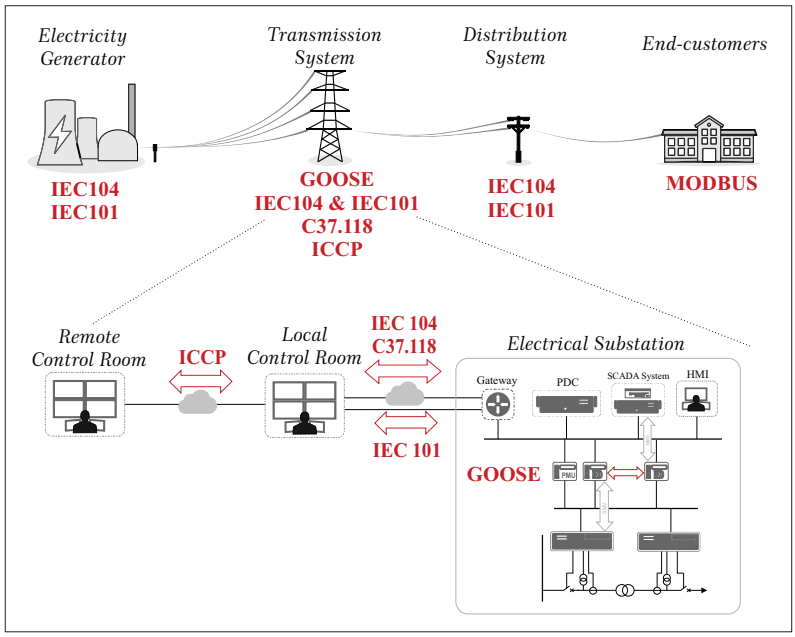

FIGURE 2. Protocols for different parts of the grid.

Modbus TCP

Modbus is one of the most common industrial protocols. It is easy to implement and maintain and has an open specification. There are several versions, including Modbus RTU for serial communication and Modbus TCP for TCP/IP communications. The version that we will reference in this work is Modbus TCP. Modbus TCP is a simple request/response protocol in a client/server model widely implemented in both WANs and LANs networks. Only the controller (client) can initiate communication with the remote unit (server). i.e., the controller device must routinely poll each RTU or PLC (agents) and look for changes in the data. This means that, since there is no way for an agent device to report an exception, an agent only sends a message if requested by its controller.

Finally, unlike IEC 104, Modbus does not have timestamp or quality attributes in its packets. Furthermore, its format packets do not include an attribute for data object descriptions. e.g., whether a register value represents a voltage value or a power measurement.

IEEE C37.118

The IEEE C37.118-2 is a widely used standard for PMUs sending synchronized phasor measurements (synchrophasor). A PMU computes the synchrophasor data. It transform electrical measurements for the current/voltage waveform at a given instant to a magnitude and phase angle. PMU implementations use WAMS network technologies for transmitting sysnchrophasor across large geographical areas due to its low latency requirements suitable for real-time supervision. Synchrophasor data is typically timestamped using Global Positioning System (GPS) time as a universal time source for higher accuracy. It is used in applications for dynamic observability, such as islanding detection, voltage stability monitoring, oscillation monitoring, and detection and wide-area frequency monitoring [10].

Taxonomy

We will now discuss our proposed taxonomy features.

Communications

We identify three main models of communication which differ according to the specific needs of the network and the relationship between peers. The three models are client/server, publisher-subscriber, and peer-to-peer.

A client/server model is used mainly for supervision purposes. The client is the centralized SCADA system located in the CR, and the servers are the supervising devices in the field (such as RTUs, PMUs, and PLCs). The CR is always the initiator of communications and the field devices, answer only to the main server, so their relationship is hierarchical.

All the data is gathered at a particular point (CR), which means that the architecture of the network is centralized.

The publisher-subscriber is commonly used at the substation level, mainly for protection purposes. The publisher is the element that transmits data, and the subscribers are the consumers of that data. In this model, data is broadcast among all the devices and accepted only by those that need it. This is a many-to-many communication type. Unlike the client/server model in which the devices that request data differ from the field devices, the devices in the publisher-subscriber model are typically the same and perform similar functions (usually IEDs), i.e., there is no hierarchical relationship. Since data is broadcast, the publisher does not need to know who is using the information and, the subscriber does not require the origin of the data. In this way, the electrical substation reduces delivery latency, and the connection complexity is decreased to a single point. As a result, protection schemes in a substation can be operated without delay. When an IED detects a fault, it broadcasts the alarm without concern about the destination address or connection problems.

The last communication model is the peer-to-peer model, where two or more peers pool their data in a decentralized system. Peers are CRs that communicate with each other directly without any intermediary and share the status (measurement data) of their substations. Usually, there is no hierarchical relationship. Each CR possesses the same capabilities: it can initiate communication and function as a client or a server (via a request-response message). Since the primary purpose is data monitoring between CRs, data speed and reliability are not the priority, unlike in the publish-subscribe model.

Connectivity, E2E ID, and Port

The industrial protocols we have analyzed have a variety of communication links. They range from Local Area Networks (LANs) to monitor and control devices relatively close to each other (including serial communication in IEC 101) to IP-based WANs used to monitor and control remote units. Therefore, we define the following features:

1. Connectivity denotes the type of connections the devices have; for example, IEC 101 is a serial link, IEC 104 uses WAN and GOOSE uses LAN.

Protocol	Communications	Connectivity	E2E ID	Port	Monitoring	Object-oriented	Traffic Endpoints
IEC 101	C/S	Serial	Link address	—	P, SP		RTU-CR
IEC 104	C/S	WAN	IP	TCP/2404	P, SP		RTU-CR
ICCP	P2P	WAN	IP	TCP/102	R/R, P	✓	CR-CR
MODBUS	C/S	LAN	IP	TCP/502	R/R		PLC-CR
C37.118	C/S	WAN	IP	TCP/4712 UDP/4713	R/R, P		PMU-CR
GOOSE	PubSub	LAN	MAC	—	P, SP	✓	IED-IED

TABLE 1. Communications: Client/Server (C/S), Publish/Subscribe (PubSub), peer-to-peer (P2P). Mode: Request/Respond (R/R), Periodic (P), Spontaneous (SP).

GOOSE is a different protocol from the others on the table. It is the only one that uses the Publisher/Subscriber model; this makes it more efficient for protection purposes.

2. E2E ID defines the End-to-End identifier in the communication link. For example, IEC 104 communicates via IP addresses, while GOOSE via MAC addresses.
3. The Port number identifies the port and the associated transport protocol used by the standard.

TCP/IP is the most common protocol found in the Network layer, noteworthy for its reliable data transmission. Less common but also important, UDP is ideal for fast communication over long distances (WAN) while Ethernet is ideal for fast communication over short distances (LAN). This is especially important for control and protection purposes. For example, PMU can use UDP for high data transmission between substations, and an IED can utilize GOOSE to transmit over Ethernet within the substations for rapid event responses.

Monitoring

We identified three ways that the control server monitors the status of devices and how the devices receive information from peers:

Spontaneous: These are events that the agent can send without receiving any previous request from the controller. The time report depends on when a value exceeds a pre-configured threshold or, in the case of status values, when they change. e.g., the networks that use IEC 104 widely use this type of transmission to reduce strain on the network.

Periodic: In this case, an agent reports value data at a fixed interval of time according to the configuration. The agents do not require an acknowledgment from the recipient, and the flow of communication can be in one direction. For example, C37.118 devices are mostly periodic, and only the controller communicates with the agent for configuration.

Request-Response: For these, only the controller can initiate communication and it must routinely poll each agent to look for changes. Agents do not report exceptions and never send a message unless their controller requests it. This is the only transmission mode used by Modbus. It has equal traffic flow in both directions.

Object-Oriented

The design of object-oriented protocols is comparatively new. Their purpose is to address the complexity and interoperability of network devices by creating objects described as data attributes and operational services. Each object is an independent entity that can be replaced without affecting the whole system. For instance, a substation has measurement, control, and protection devices, each with its data type, functionalities, and services. Without a simplified means of communication, there would be no easy method of interoperability between devices.

Endpoints

Finally, we come to the endpoints of each network. They are labeled starting with the endpoint that sends out most of the information. For example, RTU-CR means that the endpoints of this network are RTUs and CRs and that RTU sends out the bulk of its data to the CR (although the CR can also send data to the RTU).

Discussion

Table 1 shows our proposed taxonomy. As we can see, there are no two protocols alike. First, among our datasets, IEC 101 represents the only serial protocol in the list. It is representative of legacy SCADA systems that use modems or other serial connections to communicate remotely.

Among the protocols that use communication networks, the client/server model is predominant. This means that most of the communication within the grid is end-to-end.

With one exception, TCP/IP is the preferred transport protocol because packets can be re-transmitted if lost en-route. This is especially important for WAN, where the reception of packets is critical for control commands. The one time TCP is not utilized, it is substituted with IEEE C37.118. Since this is a protocol predominantly designed for high-granularity monitoring purposes, it can use UDP for fast transmission without the need to acknowledge packets. IEEE C37.118 is a data hose over UDP, and the server receives as much of it as possible.

GOOSE is a different protocol from the others on the table. It is the only one that uses the Publisher/Subscriber model; this makes it more efficient for protection purposes. It is also the only protocol not using TCP (it runs directly on top of Ethernet).

As regards monitoring, most communications can be either periodic (asynchronous) or request/response (asynchronous).

Finally, we can see that protocols that use object-oriented paradigms are not widely used in the power grid; they are instead chosen for a particular section of the grid. In our case, they are used for the short but fast packet transmission inside substations (GOOSE) and the long distances but heavy data volume between control rooms (ICCP).

To illustrate some of these differences, we obtained real-world data from operating power

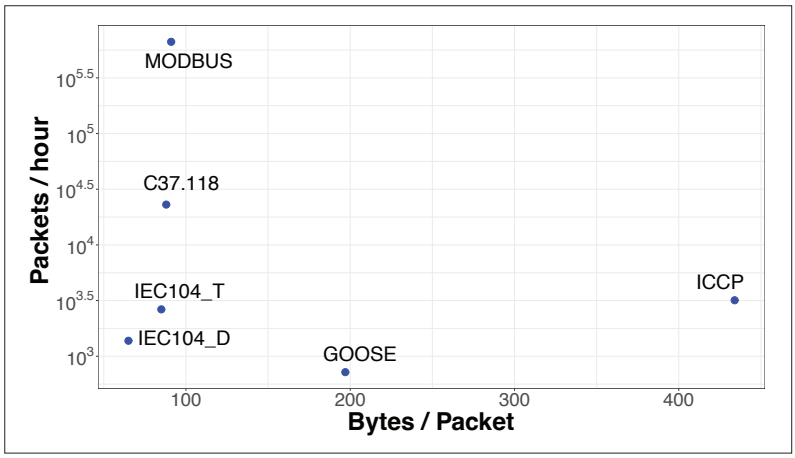

FIGURE 3. Packets/hour vs packet size.

grids in different infrastructures, including a System Operator, a Transmission Owner, a Distribution Owner, and a University Campus (Consumer). They were primarily collected in each facility's control network (SCADA network of the CR) with the exception of GOOSE, which was captured in a substation. The datasets are packet traces stored in a pcap format. They contain unencrypted data from steady-stable operations (no system disturbance/events or attacks registered) including control and measurement data.

Figure 3 shows our preliminary analysis of our datasets, showing clear clusters of activities. In trying to understand these clusters, we argue that the physical distance between the endpoints affects the amount of data that needs to be transmitted. The Modbus TCP protocol used in a university campus and the GOOSE protocol used in the substation are LANs where all devices sit within a few dozen meters of each other. In contrast, the rest of the protocols operate over WANs, spanning hundreds of kilometers between devices. GOOSE shows relatively lower data transmission, however, and this is because, during our packet capture, there was no emergency event (e.g., line overload). Therefore, there was no need to send packets at higher rates.

We also see small packets (less than 100 bytes) but with a rapid transmission rate (C37.118). This reflects the high-frequency data collection from PMUs. On the other extreme, there are protocols with large packet sizes and moderate transmission rates (e.g., ICCP). This reflects that CRs have much data to share (they collect data from a wide area, while substations only collect data from one point in the network).

Conversely, IEC 104_T (IEC 104 used in the transmission system) and IE104_D (IEC 104 used in the distribution system) carry information from a single substation (per connection). Modbus has the highest transmission rate, nearly two orders of magnitude greater than the rest. This rate of transfer was a configuration decision of the university campus.

Security

All the traffic packet captures we obtained for the analysis of this article showed unauthenticated and unencrypted connections. This is because the system uses private networks leased by telecom providers. In addition, some of the networks are LANs, and the protocols are not routable. In principle, they are not accessible by anyone outside the respective organizations; however, they still have two risks. First, as the Stuxnet attack showed, air-gapped networks are not fully resilient. And second, these private networks still operate with a trusted insider assumption. A disgruntled employee can do much damage if they have access to these systems.

Recently, there have been ongoing efforts to close the security gap in various protocols, for example, with the standard IEC 62351. This standard, published in 2008, was defined to provide power systems with applicable end-to-end mechanisms to secure communication networks (encryption and authentication), key management, network security monitoring, and role-based access control. The implementation of these standards in real-world networks has encountered some challenges. For example, the specification of the GOOSE standard to be able to send messages every 1 ms places heavy constraints on encryption and authentication.

Some proprietary protocols also enable security by default. While all the industrial protocols discussed so far are standardized and do not support encryption and authentication natively, the latest version of the proprietary Siemens S7 protocol has authenticated communications [11, 12].

Maintaining session semantics can also help prevent session hijacking. Without session semantics, spoofed messages will be accepted as legitimate; these could be fake sensor readings or fake actuator commands. Protocols that do not keep session semantics, such as GOOSE, can be more vulnerable to these attacks, especially those over TCP (session semantics increases the cost for attackers). But unless we have authentication, sessions can still be hijacked [13].

Finally, protocol-based publish/subscribe architectures like GOOSE and even bus protocols like CAN (which runs the network of ECUs in vehicles) do not have a source or destination identifiers. Devices look at the message ID of interest from broadcast messages in the network. Any compromised node in these networks can send messages with IDs that generally belong to others [14].

Conclusions

As this initial discussion shows, industrial control protocols differ considerably from each other. They have distinct properties, communicate with a variety of endpoints through different types of networks. This has implications for network design as well as security deployments. We hope this article provides an initial background for interested researchers in this area, and motivates them to appreciate the difference in protocols and their implications in the SCADA networks.

Acknowledgments

This research was partially supported by NSF CNS-1931573 and by the NSF-BSF award 1929406.

References

[1] C.-Y. Lin, S. Nadjm-Tehrani, and M. Asplund, "Timing-Based Anomaly Detection in Scada Networks," *Critical Information Infrastructures Security*, Cham: Springer International Publishing, 2018, pp. 48–59.
[2] L. Stylianou *et al.*, "A Behavioral Model to Detect Data Manipulation Attacks of Synchrophasor Measurements,"

2021 IEEE PES Innovative Smart Grid Technologies Europe, Espoo, Finland: IEEE, Oct. 2021, pp. 1–6.
[3] A. Bohara *et al.*, "Ed4gap: Efficient Detection for Goose-Based Poisoning Attacks on IEC 61850 Substations," *2020 IEEE Int'l. Conf. Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm)*, Tempe, AZ, nov 2020, pp. 1–7.
[4] C.-Y. Lin and S. Nadjm-Tehrani, "A Comparative Analysis of Emulated and Real IEC-104 Spontaneous Traffic in Power System Networks," *Cyber-Physical Security for Critical Infrastructures Protection*, Cham: Springer International Publishing, 2021, pp. 207–223.
[5] K. Mai *et al.*, "Uncharted Networks: A First Measurement study of the Bulk Power System," *Proc. ACM Internet Measurement Conf.*, Virtual Event USA: ACM, oct 2020, pp. 201–13.
[6] D. Formby, A. Walid, and R. Beyah, "A Case Study in Power Substation Network Dynamics," *Proc. ACM Meas. Anal. Comput. Syst.*, vol. 1, no. 1, June 2017.
[7] S. Mohagheghi, J. Stoupis, and Z. Wang, "Communication Protocols and Networks for Power Systems-Current Status and Future Trends," *2009 IEEE/PES Power Systems Conference and Exposition*, Mar. 2009, pp. 1–9.
[8] I. E. Commission, T. C. 57, and I. E. Commission, Communication Networks and Systems for Power Utility Automation. Part 8-1, 2011, oCLC: 914242803.
[9] J. Hoyos, M. Dehus, and T. X. Brown, "Exploiting the Goose Protocol: A Practical Attack on Cyber-Infrastructure," *2012 IEEE Globecom Wksps.*, Anaheim, CA, USA: IEEE, Dec. 2012, pp. 1508–13.
[10] M. U. Usman and M. O. Faruque, "Applications of Synchrophasor Technologies in Power Systems," *J. Modern Power Systems and Clean Energy*, vol. 7, no. 2, Mar. 2019, pp. 211–26.
[11] A. Kleinman and A. Wool, "Accurate Modeling of the Siemens s7 Scada Protocol for Intrusion Detection and Digital Forensics," *J. Digital Forensics, Security and Law: JDFSL*, vol. 9, no. 2, 2014, pp. 37–50.
[12] E. Biham *et al.*, "Rogue7: Rogue Engineering-Station Attacks on S7 Simatic PLCs," p. 21.
[13] A. Kleinmann *et al.*, "Stealthy Deception Attacks Against Scada Systems," *Computer Security*, Cham: Springer International Publishing, 2018, pp. 93–109.
[14] T. Dagan and A. Wool, "Parrot, A Software-Only Anti-Spoofing Defense System for the CAN Bus," p. 10.

Biographies

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 [SM] (alacarde@ucsc.edu) 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.

Avishai Wool [SM] (avishai@tauex.tau.ac.il) received a B.Sc. (honors) degree in mathematics and computer science from at Tel Aviv University, in 1986 and the MSc (1992) and Ph.D. (1997) degrees from the Weizmann Institute Science, both in computer science. He is an associate professor at the School of Electrical Engineering Tel Aviv University. He is also the deputy-director of the Interdisciplinary Cyber Research Center, TAU. His research interest includes computer, network card, RFID systems, side-channel, cryptanalysis, and firewall technology.