RADIANCE: Cyber Vulnerabilities and Mitigations Related to Communication Protocols Found in Energy Delivery Systems

October 2019

SR Mix

GMLC-DE-AC07-05ID14517
PNNL-29313

GMLC-DE-AC07-05ID14517
PNNL-29313

RADIANCE: Cyber Vulnerabilities and Mitigations Related to Communication Protocols Found in Energy Delivery Systems

DOE Grid Modernization Laboratory Consortium Team

SR Mix[1]

October 2019

[1] Pacific Northwest National Laboratory

DISCLAIMER

PACIFIC NORTHWEST NATIONAL LABORATORY
operated by
BATTELLE
for the
UNITED STATES DEPARTMENT OF ENERGY
under Contract DE-AC05-76RL01830

Printed in the United States of America

Available to DOE and DOE contractors from the
Office of Scientific and Technical Information,
P.O. Box 62, Oak Ridge, TN 37831-0062;
ph: (865) 576-8401
fax: (865) 576-5728
email: reports@adonis.osti.gov

Available to the public from the National Technical Information Service
5301 Shawnee Rd., Alexandria, VA 22312
ph: (800) 553-NTIS (6847)
email: orders@ntis.gov <http://www.ntis.gov/about/form.aspx>
Online ordering: http://www.ntis.gov

Summary

Under its Grid Modernization Initiative, the U.S. Department of Energy (DOE), in collaboration with energy industry stakeholders, developed a multi-year research plan to support modernizing the electric grid. One of the foundational projects for accelerating modernization efforts is information and communications technology interoperability. A key element of this project has been the development of a methodology for engaging ecosystems related to grid integration to create roadmaps that advance the ease of integration of related smart technology.

This document provides an overview of cybersecurity issues and mitigations available for communications protocols used in energy delivery systems.

Acknowledgments

This work was supported by the Grid Modernization Initiative of the U.S. Department of Energy, under award or contract number DE-AC07-05ID14517, as part of its Grid Modernization Laboratory Consortium, a strategic partnership between DOE and the national laboratories to bring together leading experts, technologies, and resources to collaborate on the goal of modernizing the nation's grid.

This work was authored using funding provided by the U.S. Department of Energy Office of Energy Efficiency and Renewable Energy Water Project Technologies Office and the U.S. Department of Energy Office of Electricity. The views expressed in the document do not necessarily represent the views of the DOE or the U.S. Government. The U.S. Government, and the publisher, by accepting the article for publication, acknowledges that the U.S. Government retains a nonexclusive, paid-up, irrevocable, worldwide license to publish or reproduce the published form of this work, or allow others to do so, for U.S. Government purposes.

Acronyms and Abbreviations

AARE	application association response
AARQ	application association request
ACSE	association control service element
ASCII	American Standard Code for Information Interchange
AGA	American Gas Association
BITW	bump-in-the-wire
BPS	bits per second
CA	certificate authority
CIM	common information model
CIP	critical infrastructure protection
CLNP	Connectionless-mode Network Protocol
CRC	cyclic redundancy check
CRL	certificate revocation list
DER	distributed energy resource
DNP3	Distributed Network Protocol Version 3
DNP3 SA	Distributed Network Protocol Version 3 Secure Authentication
DOE	U.S. Department of Energy
DOS	denial-of-service
DPI	deep packet inspection
eLORAN	enhanced LOng RAnge Navigation
ESP	electronic security perimeter
FIPS	Federal Information Processing Standard
GDOI	Group Domain of Interpretation
GOOSE	Generalized Object Oriented Substation Event
GNSS	Global Navigation Satellite Systems
GPS	global positioning system
GTI	Gas Technology Institute
HSR	High-availability Seamless Redundancy
Hz	hertz
ICCP	Inter-control Center Communication Protocol
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IP	Internet Protocol
IPsec	Internet Protocol Security
IRIG-B	Inter-range Instrumentation Group – protocol “B”

IS	International Standard (a type of IEC publication)
ISA	International Society of Automation
ISO	International Standards Organization
LAN	local area network
LRC	longitudinal redundancy check
MIB	management information block
MMS	manufacturing messaging specification
NERC	North American Electric Reliability Corporation
NIST	National Institute of Standards and Technology
NTP	Network Time Protocol
OCSP	Online Certificate Status Protocol
OSI	open systems interconnection
PKI	public key infrastructure
PMU	phasor measurement unit
PNNL	Pacific Northwest National Laboratory
PRP	Parallel Redundancy Protocol
PTP	Precision Time Protocol
R-GOOSE	Routable Generalized Object Oriented Substation Event
R-SV	routable sampled values
RADIANCE	Resilient Alaskan Distribution system Improvements using Automation, Network analysis, Control, and Energy storage
RBAC	role-based access control
RFC	request for comments
RTU	remote terminal unit
SCADA	supervisory control and data acquisition
SDN	software defined network
SEL	Schweitzer Engineering Laboratories
SNTP	Simple Network Time Protocol
SOE	sequence of events
SP	Special Publication (a type of NIST publication)
SSCP	Secure SCADA Communications Protocol
SSP-21	Secure SCADA Protocol for the 21st Century
SSPP	Secure SCADA Protection Protocol
SV	sampled values
TCP	Transmission Control Protocol
TP4	Transmission Protocol 4
TR	Technical Report (a type of IEC publication)
TS	Technical Specification (a type of IEC publication)

TLS	Transport Layer Security
UDP	User Datagram Protocol
VLAN	virtual local area network
VPN	virtual private network
WAN	wide area network
WWVB	A NIST radio station located near Fort Collins, Colorado
XML	eXtensible Markup Language

Contents

Introduction

Nearly all communications used for telemetry and control in an electric power system are based on legacy protocols that were developed long before cybersecurity was a concern. The primary focus of these protocols was integrity of the message. As a result, most of the protocols in use do not have the capability to natively protect the communication messages from observation, provide authentication of the sending or receiving node, or provide integrity against intentionally modified packets.

While some protocols, such as Distributed Network Protocol Version 3 (DNP3), standardized by the Institute of Electrical and Electronics Engineers (IEEE) as IEEE Std. 1858, have added secure features to the protocol to provide authentication services for communications, other protocols such as Secure Modbus[1] have adopted "wrapper" technologies to secure the protocol payload with minimal impact to the underlying protocol.

Additional techniques may be applied to secure the underlying protocol. These techniques include protocol-agnostic wrappers like Secure SCADA Communications Protocol (SSCP), standardized as IEEE Std. 1711.2; use of IPsec tunneling for IP versions of protocols; and standard approaches defined in the International Elecrotechnial Commission (IEC) standard IEC 62351, Security Standards for the Power System Information Infrastructure.

The impact of the North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) standards for North American electric utilities has had an impact on several security implementations, particularly the requirement to inspect all traffic that crosses a security boundary, i.e., a NERC CIP Electronic Security Perimeter (ESP).

This report consists of two major portions. The first is a brief overview of the protocols commonly found in energy delivery systems. The second is an overview of currently documented and implemented mitigations to protect those protocols from attack.

A section on time synchronization protocols is also included, since many of the mitigations rely on accurate and coordinated time in order to work effectively. Most telemetry and control protocols do not require accurate time at field end of the communication link. The exception to this is if the central stations have a "sequence of events" (SOE) application that attempts to correlate the exact order of device status changes at multiple locations. A discussion of SOE is beyond the scope of this report.

[1] See http://modbus.org/docs/Modbus-SecurityPR-10-2018.pdf, referenced 10/8/2019

Vulnerabilities

When discussing vulnerabilities, it is useful to understand the traditional approach to describing security – the co-called C-I-A triad, standing for *Confidentiality*, *Integrity*, and *Availability*:

Federal Information Processing Standard (FIPS) publication FIPS-199, *Standards for Security Categorization of Federal Information and Information Systems*[2], defines the terms based on the language in 44 United States Code Section 3542 as follows:

- Confidentiality: "preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information." A loss of confidentiality is the unauthorized disclosure of information.
- Integrity: "guarding against improper information modification or destruction and includes ensuring information nonrepudiation and authenticity." A loss of integrity is the unauthorized modification or destruction of information. Integrity is typically used in the context of a communication channel to preserve the integrity of data in transit.
- Availability: "ensuring timely and reliable access to and use of information." A loss of availability is the disruption of access to or use of information or an information system.

In essence, the terms can be thought of as performing the following functions for a communication network:

- Confidentiality – protecting the message from being observed (or interpreted)
- Integrity – ensuring that the message that arrives at a destination is the same as the one sent
- Availability – ensuring that when a message is sent, it arrives within the expected timeframe

For a telemetry and control system, confidentiality is generally a low priority, since the telemetry is associated with measurements of physical systems that can be otherwise obtained, and control commands will have observable effects on the same physical systems. Therefore, the other two aspects, integrity and availability, have higher importance.

Availability cannot generally be increased through protocol modifications; rather, the use of redundant communication processors and redundant diversely routed communication paths are often deployed. In a local-area network (LAN), redundancy can be implemented using either Parallel Redundancy Protocol (PRP), or High-availability Seamless Redundancy (HSR), both defined by standard IEC 62439-3. Both of these protocols use different methods to send the same data packet into the network twice and have processing at the receiving end to detect and ignore the redundant packet if received.

Networks can also contain engineered resiliency through the use of software defined networking (SDN) with rapid link detection and re-routing recovery to minimize the impact of a failed link in the LAN infrastructure. Similar techniques can be applied for wide-area networks, although not with the same speeds as on an SDN LAN.

Availability can also be impacted by a number of denial-of-service (DOS) attacks that can either overload the communications bandwidth, preventing legitimate traffic from traversing the network, or by overloading the compute or memory resource capabilities of the receiving node.

[2] National Institute of Standards and Technology (NIST): Federal information Processing Standard 199: Standards for Security Categorization of Federal Information and Information Systems, February 2004. Available online: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf

Integrity of the message is the focus of most of the security mitigations available for telemetry and control protocols. The significant integrity attacks that are mitigated generally fall into the following categories:

- *Impersonation of a valid requesting or sending node*. Nearly all non-secure telemetry and control protocols will respond to any validly formed and received message regardless of what node sends the command. This can result in a rogue device requesting data or issuing commands. Adding authentication to the message will allow the recipient to determine if the message was sent by a legitimate source.

- *Modification of the message while in transit*. Most telemetry and control protocols are relatively simple, and the protocol formats are well known. It is relatively simple to intercept a message in transit, modify it, and retransmit the modified message, a technique known as a "man-in-the-middle" attack. Even protocols with simple "error correction" codes are vulnerable to these attacks, since the attacker can simply regenerate the error correcting code that corresponds to the modified message. Using a cryptographically secured error correction code that cannot be re-generated by the attacker will allow the recipient to determine that the message has been modified in transit and ignore it.

- *Replay of a valid command.* An attacker could monitor the traffic, gather and store an example of a command (for example, a breaker trip command), and save it for later. Then, when the attacker desires to open the same breaker, they could retransmit the command, a technique known as a replay attack. If the command includes authentication and "simple" integrity fields, the recipient will not be able to determine it is from a rogue device since it appears to have been submitted from an authorized source, and it was not modified in transit. For these reasons, both the authorization and integrity processing can implement methods to prevent the packet from being interpreted as valid. The authentication process may change keys, limiting the lifetime of the authentication signature, and the integrity process may include a sequence number or timestamp to allow the receiving node to determine that the message is a replay and can be ignored.

Telemetry and Control Protocols

Legacy Protocols

Most energy delivery systems built prior to the mid 1990s used proprietary and vendor-developed (largely vendor-specific) communication protocols that were designed as point-to-point, or point-to-multi-point links to run over analog telephone networks and considered the line quality of the telephone network for error detection (and in limited cases recovery from certain errors introduced by line noise). These protocols are generally referred to as “serial” protocols, and don’t have the additional protocol layers for routing and session management found in modern communications networks. Appendix A contains a partial list of protocols found in energy delivery systems, including legacy and currently used protocols.

In energy delivery systems, particularly those used in electric power, telemetry and control are accomplished by the use of remote terminal units (RTU), also called outstations, traditionally located on low-speed analog voice-grade telephone lines communicating with centralized control centers (central stations). These RTU communication links were often multi-drop (i.e., multiple RTUs shared a communication line) and were capable of transmission speeds between 110 bits per second (BPS) and 1200 BPS.

The prime concern of the time on voice-grade analog lines was bit flips due to line noise and interference, so error detection and potentially error correction codes, such as cyclic redundancy checks (CRC), were specified to detect one- or two-bit errors introduced by noise on the line, and force a retransmit, assuming the noise was transient, and the next communication would be clean. These error detection codes are sufficient for unintentionally and randomly introduced errors but modifying the data packet and re-generating the error correcting codes is a trivial exercise and is often automated in communication test sets that are used to simulate either the central station or outstation during testing.

There is also almost no authentication for an outstation to determine if the packet received is from the correct central station or for the central station to determine if the correct outstation sent the response. Outstations were programmed to act on any validly formed command received (as long as the error detection codes validated) as if it were from the central station. This behavior was intentional to allow for the test sets mentioned before to participate in telemetry and control checkout processes.

Some legacy protocols are based on 8-bit (or 16-bit) communication units; others use non-standard communication unit sizes (such as the 31-bit format used by the Conitel protocol), making them difficult to process using commodity hardware and software currently available. This can make mitigations difficult.

The equipment used in many legacy applications also includes embedded modem technology in the outstation devices, making access to a “digital” bit stream problematic.

Currently Used Protocols

Most currently used protocols are developed by a consensus process, many of which are overseen by standards development organizations, such as the International Electrotechnical Commission (IEC), the Institute of Electrical and Electronics Engineers (IEEE), the International Society of Automation (ISA), and the International Standards Organization (ISO). They are also designed to operate off other network infrastructures most typically using the Internet Protocol (IP) for routing, and either the Transmission Control protocol (TCP) or the User Datagram Protocol (UDP) for communication session management.

In some cases, ISO protocols are used, such as Connectionless-mode Network Protocol (CLNP) for routing and Transmission Protocol 4 (TP4) for session control.

The current protocols used for RTU communication use the same central station and outstation concept, although in some cases such as transmission line protection and control, the central station function (i.e., the initiator of a scan request or control) can be located at a field site.

Modbus

The Modbus protocol was developed in 1979 to allow programmable logic controllers (PLCs) to communicate with each other. Modbus exists in three major variants:

- Modbus/RTU – a compact binary protocol that allows efficient data transfer over low-speed serial (OSI layer 2) networks. It provides message integrity by the use of a cyclic redundancy check (CRC) checksum as an error check mechanism to ensure the data has not been modified due to electromagnetic interference on the communication channel. It does not protect the data from intentional modification.

- Modbus/ASCII – similar to Modbus/RTU, but the payload is transmitted as ASCII characters rather than binary representations. This allows a printing terminal to be used to monitor traffic without any additional processing. Modbus/ASCII uses a longitudinal redundancy check (LRC) checksum in the same manner as Modbus/RTU uses the CRC.

- Modbus/TCP – a Modbus variant that transmits Modbus packets over a TCP/IP network. It is also known as Modbus/IP. Several variants exist, including one that does not include a native checksum, rather relying on the TCP/IP layers to provide message integrity. Another variant includes the checksum, allowing the same Modbus application software to operate over IP networks as well as serial networks. Modbus typically uses TCP as a layer 4 protocol, but some uses of UDP have been attempted (Modbus/UDP).

Since traditional Modbus transmits its payload as plaintext (i.e., it is not encrypted), and the payload is protected only from line noise interference by a CRC or LRC, payload messages can be intercepted and modified in transit by a technique known as a man-in-the-middle attack. Similarly, since there is no authentication specified in the protocol, any Modbus client or receiver will accept and respond to any valid Modbus message received, even if the message was transmitted by a rogue Modbus server.

DNP3

The Distributed Network Protocol V3 (DNP3) protocol (also known as IEEE Std. 1815) was developed in 1993 based on the partially complete IEC 60870-5 protocol available at the time. DNP3 was designed to be reliable (i.e., immune from communication line noise introduced by electromagnetic interference), but was not designed to be immune from intentional attack (i.e., malicious modification of the payload during transmission). DNP3 was initially developed as a serial protocol using low-speed voice-grade analog communication links. Later, a version of the protocol was developed that was suitable for transmission over IP networks, known as DNP/IP.

Like Modbus, traditional DNP3 has no mechanism to protect its payload data from observation or malicious modification in transit.

ICCP

The Inter-control Center Communications Protocol (ICCP) (also known as IEC Standard 60870-6, Telecontrol Application Service Element 2 [TASE.2]), is used primarily to exchange data between control centers. It was initially implemented using ISO protocols for routing and session control but is most often implemented on TCP/IP in North American implementations.

Prior to the development of ICCP in the early 1990's data exchange between different utility control centers was accomplished using proprietary or custom links between control centers, often supplied by different vendors. When ICCP was introduced, it allowed each control center (and vendor) to develop a standardized data exchange interface designed to be interoperable with other implementations. Current implementations of ICCP are generally interoperable with each other for most commonly used features. However, configuration of individual data exchanges within an ICCP network can be very cumbersome and time-consuming, often taking weeks to months to design, debug, and test prior to being placed into production.

Like most legacy protocols, ICCP was not originally designed with security features built in.

IEC 61850

IEC 61850 is modern substation automation protocol defined primarily for use within a substation, but with extensions that allow it to be used to coordinate control actions between substations and initiate control actions from a control center to a substation.

IEC 61850 requires that the data used is time stamped, so an accurate and precise time source is required. Generally, sub-millisecond time precision is required for sampled values.

Generic Object Oriented Substation Events (GOOSE) Messages

IEC 61850 uses a communication mechanism referred to as Generic Object Oriented Substation Events (GOOSE) to send data in a high-speed and reliable manner. Typically, GOOSE messages are expected to be transmitted and received in 4 milliseconds or less. GOOSE messages are typically transmitted as OSI layer 2 multicast messages on Ethernet networks, and the transmission mechanism includes a retry algorithm to ensure that an individual GOOSE message is not lost. GOOSE messages contain state and sequence numbers to ensure that the same action is not performed if the message is successfully received multiple times.

GOOSE messages may also be transmitted over routed (i.e., IP) wide-area networks, using a packet format known as routed goose, or R-GOOSE. Due to the long-distance and non-deterministic nature of wide-area networks (as opposed to well-engineered local Ethernet networks), the 4 millisecond timeframe of GOOSE cannot be guaranteed, but for specialized and purpose-built networks, end-to-end performance of 22.9 milliseconds has been observed[3].

Sampled Values (SV)

IEC 61850 uses a communications mechanism known either as sampled values (SV) or sample measured values to emulate a continuous analog measurement as would be seen in a traditional environment.

[3] See https://cdn.selinc.com/assets/Literature/Publications/Technical%20Papers/6425_CaseStudyMission_DD_20100126_Web.pdf?v=20151124-215956 (retrieved 10/19/2019)

Analog signals from instrument transformers measuring current and voltage are processed by a device called a merging unit to sample the analog signals as often as 4000 samples per second for a grid frequency of 50Hz and 4800 samples per second for 60 Hz with one sample per communication frame; or 12,800 samples per second at 50 Hz and 15,360 samples per second at 60 Hz with 8 samples per communication frame.

Sampled values, like R-GOOSE messages, can be transmitted over routed wide-area links using a packet format known as routed sampled values (R-SV).

Manufacturing Message Specification (MMS)

IEC 61850 uses the Manufacturing Message Specification (MMS) (also known as ISO/IEC 9506) as a client/server protocol to allow power system operators to monitor, manage, and control IEC 61850 devices. MMS is an alternative to DNP3 in an IEC 61850 environment for telemetry and control commands.

C37.118

The IEEE C38.118 protocol is used to transmit streaming synchrophasor (also known as Phasor Measurement Unit or PMU) data. It is a monitoring-only protocol that does not support any form of control. Synchrophasor data is transmitted as data streams, similar to sampled values, but typically at speeds of 30, 60, or 120 samples per second for 60Hz systems (or 25, 50, or 100 samples per second at 50Hz). While sampled values are intended (mostly) to stay within a substation perimeter, synchrophasor measurements are intended to be transmitted to control centers, thus the lower sample rate. Synchrophasor data streams can also be merged, down-sampled, and stored in historical archives.

Synchrophasor data is time stamped and requires an accurate and precise time source in order to time stamp the data before it is transmitted using the C37.118 protocol. Time stamping the data when it is initially transmitted allows applications to correlate data associated with events even if the data arrives at the application at different rates, or with different latencies. Devices that produce and transmit synchrophasor data using the C37.118 protocol either must have access to a network-based time source or must contain an internal precise time source (such as a satellite clock receiver).

Security Standards and Guidelines

The major international standard that specifies technical guidance for securing communications is the IEC 62351 family of standards. Other standards and guidance documents from the IEC, the International Standards Organization (ISO), and the US National Institute for Standards and Technology (NIST) are more focused on managerial and procedural controls for securing individual computer nodes, designing computer networks, and developing policies for use of compute and networking resources.

IEC 62351

IEC 62351 (*Power systems management and associated information exchange*) is a family of international standards developed to describe standard approaches to securing other protocols.

IEC 62351 specifically describes the handling of security for IEC 60870-5 (SCADA communications), IEC 60870-6 (inter-control center communications protocol - ICCP), IEC 61850 (substation automation), IEC 61970 (common information model - CIM) exchanges, and IEC 61968 (distribution system information model). It is primarily concerned with securing communications but includes sections on authentication of users/devices and security architecture.

IEC 60870-5 is not widely used in North America; rather most electric power SCADA communications use DNP3 (in either traditional [serial] mode, or in network [TCP/IP] mode). Secure versions of the DNP protocol are available, using the Secure Authentication features of DNP3 rather than IEC 62351.

IEC 62351 is primarily used in North America to secure IEC 61850 for substation automation.

IEC issues publications as either International Standards which contain mandatory requirements in a finalized form, Technical Specifications (TS) which are similar to International Standards, but the content has either not been fully developed or fully approved, or Technical Reports (TR) which contain no mandatory requirements. Only TS and TR are noted in the designation of the standard; International Standard status is assumed if not indicated.

IEC 62361 is comprised of at least 11 standards in various stages of approval or development.

- IEC/TS 62351-1: *Power systems management and associated information exchange - Data and communications security - Part 1: Communication network and system security - Introduction to security issues* contains an introduction to the IEC 62351 standard family.
- IEC/TS 62351-2: *Power systems management and associated information exchange - Data and communications security - Part 2: Glossary of terms* contains a glossary of terms used by the IEC 62351 family of standards.
- IEC 62351-3: *Power systems management and associated information exchange - Data and communications security - Part 3: Communication network and system security - Profiles including TCP/IP* specifies security profiles for protocols running on top of TCP/IP, including the use of Transport Layer Security (TLS) for encryption, node authentication using X.509 certificates, and message authentication.
- IEC 62351-4: *Power systems management and associated information exchange - Data and communications security - Part 4: Profiles including MMS* specifies security profiles for the use of the manufacturing message specification (MMS), primarily IEC 60870-6 ICCP and IEC 61850

substation automation, and specifies authentication methods for MMS communications and using TLS.

- IEC/TS 62351-5: *Power systems management and associated information exchange - Data and communications security - Part 5: Security for IEC 60870-5 and derivatives* specifies security profiles for IEC 60870-5 (SCADA telemetry and control communications similar to DNP3).
- IEC/TS 62351-6: *Power systems management and associated information exchange - Data and communications security - Part 6: Security for IEC 61850* specifies security profiles for IEC 61850, including mandating the use of virtual local area networks (VLANs) for GOOSE message traffic.
- IEC 62351-7: *Power systems management and associated information exchange - Data and communication security - Part 7: Network and system management (NSM) data object models* specifies a management information base (MIB) specific to the power industry for use by network and system management tools.
- IEC/TS 62351-8: *Power systems management and associated information exchange - Data and communications security - Part 8: Role-based access control* specifies requirements for role-based access control (RBAC).
- IEC 62351-9: *Power systems management and associated information exchange - Data and communications security - Part 9: Cyber security key management for power system equipment* specifies profiles and uses of key management, including appropriate use of passwords and encryption keys, cryptographic systems lifecycle management, methods for using asymmetric cryptography (i.e., public/private key and a public key infrastructure [PKI] for key management), and management of PKI itself and other support mechanisms.
- IEC/TR 62351-10: *Power systems management and associated information exchange - Data and communications security - Part 10: Security architecture guidelines* is a technical report describing security architecture guidelines for power systems.
- IEC 62351-11: *Power systems management and associated information exchange - Data and communications security - Part 11: Security for XML documents* defines profiles for securing extensible markup language (XML) files, including using X.509 certificates for XML file signature authenticity and optional data encryption.
- IEC/TR 62351-12*: Power systems management and associated information exchange - Data and communications security - Part 12: Resilience and security recommendations for power systems with distributed energy resources (DER) cyber-physical systems* discusses cybersecurity recommendations and engineering/operational strategies for improving the resilience of power systems with interconnected Distributed Energy Resources (DER) systems.
- IEC/TR 62351-13*: Power systems management and associated information exchange - Data and communications security - Part 13: Guidelines on security topics to be covered in standards and specifications* provides guidelines on what security topics could or should be covered in standards and specifications (IEC or otherwise) that are to be used in the power industry.
- IEC/TR 62351-90-1: *Power systems management and associated information exchange - Data and communications security - Part 90-1: Guidelines for handling role-based access control in power systems* is a technical report for handling of access control of users and automated agents to data objects in power systems by means of role-based access control (RBAC) as defined in IEC/TS 62351-8.
- IEC/TR 62351-90-2: *Power systems management and associated information exchange – Data and communications security – Part 90-2: Deep packet inspection of encrypted communications* is a

technical report that addresses the need to perform Deep Packet Inspection (DPI) on communication channels secured by various other IEC 62351 standards.

- IEC/TS 62351-100-1*: Power systems management and associated information exchange - Data and communications security - Part 100-1: Conformance test cases for IEC TS 62351-5 and IEC TS 60870-5-7* describes test cases for conformance and interoperability testing of IEC/TS 62351-5 and IEC/TS 60870-5-7 to secure IEC 60870-5-101- and IEC 6870-5-104-based communications.

Additionally, the following IEC 62351 standards are in early stages of development:

- IEC 62351-14: *Power systems management and associated information exchange - Data and communications security - Part 14: Cyber security event logging*
- IEC/TS 62351-100-3: *Power systems management and associated information exchange – Data and communications security – Part 100-3: Conformance test cases for the IEC 62351-3, the secure communication extension for profiles including TCP/IP*
- IEC TS 62351-100-4: *Power systems management and associated information exchange – Data and communication security – Part 100-4: Conformance testing for IEC 62351-4*
- IEC/TS 62351-100-6: *Power systems management and associated information exchange – Data and communications security – Part 100-6: Conformance testing for IEC 62351-6*

ISA/IEC 62443

ISA/IEC 62443 was initially developed by the International Society for Automation (ISA) as ISA-99. It is the international standard for securing process automation systems, primarily those found in manufacturing and process industries.

NIST

The US National Institute for Standards and Technology (NIST) publishes cybersecurity recommendations for the US federal government. They are generally mandatory for US federal agencies and are often adopted by private industry. They include recommendations and guidelines for securing information technology and operations technology. The primary source of security guidance is contained in the NIST Risk Management Framework, specifically in NIST Special Publication (SP) 800-53 for information technology and SP800-82 for operational technology. The NIST guidelines specify high-level policy control statements and do not provide any specific technical controls for securing communications.

ISO 27000

The International Standards Organization (ISO) produces standards for information security in the ISO 27000 family of standards. The majority of those standards are focused on procedural controls for managing security in information systems. The ISO 27000 family of standards does not specify any technical controls itself and refers to the IEC 62351 family of standards for technical controls.

IETF

The Internet Engineering Task Force is responsible for managing the Request for Comments (RFC) process that develops the standards and recommendations for protocols used on the internet and in IP-

based networks. There are over 8600 RFCs available, although many of them have been superseded by later RFCs. RFCs define the Transport Layer Security (TLS) and Group Domain of Interpretation (GDOI) protocols used by telemetry and control protocols.

Mitigations for Telemetry and Control Protocols

In order to overcome some of the security vulnerabilities described above for the communication protocols commonly found in electric power systems, two kinds of approaches have been developed.

The first approach is to provide a secure wrapper around the traditional protocol to detect tampering and provide authentication, and optionally provide encryption of the payload to protect it from disclosure. This approach is the most common, since it does not require significant changes to the underlying protocol. The second method is to modify the protocol to add security services natively to the protocol.

Legacy mitigations

Since most legacy protocols are no longer being supported, the options for mitigation are severely limited. The most common approach is the use of a protocol wrapper. However, most protocol wrappers expect the data to be communicated using octets (8-bit bytes). In some cases, 16-bit data words can be readily split into two 8-bit chunks for processing, but this process may introduce unexpected jitter to the central station or outstation processing. Other protocols using communication words, not multiples of 8 bits (such as a 31-bit word), need to be buffered and padded to be processed using procedures that expect octet bounded communications. Additionally, the lack of external modems and access to the digital data stream makes intercepting the data after it leaves the central station or before it enters the outstation equipment nearly impossible without doing an analog-to-digital conversion before applying security, followed by a digital-to-analog conversion to send the data to the other end of the communication link, only to do the same processing upon receipt of the message.

For these reasons, mitigations for most legacy protocols are not performed. It is often less expensive to replace the equipment with protocols that support mitigation than it is to attempt to add mitigation on legacy protocols and engineer around all the latency, jitter, and additional equipment required. This replacement has the added benefit of replacing unsupported or unsupportable equipment with equipment that can be supported.

Protocol Wrappers

Protocol wrappers are software packages that take as input an unmodified communication stream, and “wrap” a security layer around the message. The receiving end of the communication can take the wrapped message, decode and verify it, and pass the unmodified data to the end station. This minimizes the impact on the sending and receiving equipment, especially if the protocol wrapping is done using “bump-in-the-wire” technology that does not require any modification of the central station or outstation equipment or processing. These techniques are most often the addition of a cryptographically secure hash that protects the integrity of the message by precluding the ability to modify the message during transmission and re-calculating the hash value. The hash can also provide authenticity of the message by digital signatures that can be embedded in the hash processing. Many of the wrapping technologies can provide encryption of the data in addition to integrity and authentication to prevent the data from being observed during transmission. All of these actions may have an impact on latency and jitter, which must be considered when designing a system that uses protocol wrappers.

Protocol wrappers can be implemented as either software-only, or as hardware additions. Software wrappers can be either integrated with existing communications applications or inserted as “shims” acting as device drivers. The advantage of using the shim approach is that the communications application does

not need to be modified and is not aware of the additional processing. This approach can be used if modifications to the communications software cannot be made but modifications to the operating system can be made.

If there is no provision for modifying the application or operating system environment, a hardware solution is required. These are called "bump-in-the-wire" (BITW) additions since they are implemented as additional hardware on the communications link. BITW solutions are generally purpose-built for a specific application and protocol and can be more efficient than attempting to retrofit the security function into existing hardware or software. If possible, the easiest way of inserting BITW hardware is to intercept the digital signal as it leaves the communications processor before it connects to a modem. The BITW hardware intercepts the digital bit stream, performs its processing, and then sends the modified digital bit stream to the modem for translation to an analog signal and transmitted on a voice-grade circuit. A similar process is performed at the other end of the line after the modem translates the analog signal to a digital bit stream.

Numerous approaches to implementing protocol wrappers are available, several of them are (or will be) defined by international standards.

SSCP (IEEE Standard 1711.2)

The Secure SCADA Communications Protocol (SSCP) is in the final stages of being approved as an IEEE standard and will be referred to as IEEE Std. 1711.2[4] when completed sometime in late 2019 or early 2020. SSCP was developed in the early 2000's by Pacific Northwest National Laboratory (PNNL) and commercialized by Schweitzer Engineering Laboratories (SEL) to secure serial SCADA communications links primarily used for telemetry and control, but can also be applied to securing configuration or maintenance access. SSCP is designed to secure serial (non-network) communications often found in legacy applications. SSCP can be implemented as a "bump-in-the-wire" solution for retrofit applications at either the central station or outstation or can be included as a software layer in equipment at either the head-end or remote location. SSCP provides the capability of cryptographically signing messages to protect their integrity during transmission, preventing undetected message modification, as well as encrypting the message to protect the contents of the message from being observed during transmission. SSCP is designed to be "lightweight" to minimize impact on communication channels as well as compute resources.

SSCP was designed to be underlying protocol agnostic, both for protocols and communication word sizes; however, only implementations supporting byte-oriented protocols, such as DNP3, have been produced.

Commercial versions of early (non-standard) versions of SSCP are available[5], but once finally approved and published by the IEEE, additional vendors are likely to produce compatible products.

SSPP (IEEE Standard P1711.1)

The Substation Serial Protection Protocol (SSPP) is under development as IEEE Std. P1711.1. SSPP was initially developed by the American Gas Association (AGA) and the Gas Technology Institute (GTI) as standard AGA-12. It is designed to provide integrity and optional confidentiality for 7-bit and 8-bit byte-oriented protocols such as Modbus and DNP3 transmitted over traditional serial communications channels. It supports point-to-point, point-to-multipoint, and broadcast communications links. SSPP can support a hybrid mode operation where some communication links are protected by the SSPP protocol,

[4] Until it is fully approved by the IEEE, it is referred to as P1711.2 – for proposed standard

[5] See for example, https://selinc.com/products/3025/

while others continue to operate in native (non-secured) mode, allowing a phased or incremental migration from unsecured communications to SSPP secured communication. Like SSCP, SSPP can be implemented natively in software or hardware, as well as by a "bump-in-the-wire" retrofit application at either the central station or outstation or both.

SSP-21

Secure SCADA Protocol for the 21st Century (SSP-21) is a cryptographic wrapper designed to secure point-to-multipoint serial protocols or to act as a security layer for new SCADA applications. It was developed by the Automatic consulting company with funding from a consortium of California utilities with support from the California Public Utilities Commission. It is intended to fill a gap where existing technologies like TLS are not applicable or require too much processing power or bandwidth. It can be used as a protocol-agnostic "bump-in-the-wire" at outstations or as a software bump-in-the-stack on the central station or the outstation. No provision is made for retrofitting central stations with a "bump-in-the-wire" as we assume that central station can be much more easily upgraded than outstations. SSP-21 is designed to be used for both serial and network (i.e., TCP/IP) communication channels.

IPsec and TLS

If the protocol is transmitted using a standard Internet Protocol (IP) stack, then site-to-site VPNs using IP Security (IPsec) can be used to transmit the data across a wide area network (WAN). IPsec VPNs are commonly used in information technology (i.e., office network) environments to connect data centers and remote offices. IPsec VPNs are typically established between border routers at two locations and are therefore often referred to as "site-to-site VPN's," although an individual computer node could install IPsec VPN software and establish its own connection. Site-to-site VPNs using IPsec are therefore often used to connect two locations or zones that all have implicit trust of all the nodes within each location but must communicate over an untrusted network (such as the public Internet). IPsec can be implemented using pre-shared keys for encryption or can use X.509 digital certificates. If digital certificates are used, computers or routers at both ends of the IPsec VPN need to have access to a certificate authority (CA) or accept the trust level associated with using self-signed certificates (which offers the same level of trust as pre-shared keys and the increased overhead of managing the certificates).

The IEEE is developing a standard titled "Interoperability of IPsec Utilized within Utility Control Systems (P2030.102.1)," which should be of use when it is complete.

TLS is similar to IPsec but operates at the TCP layer (and therefore us unsuitable for UDP traffic). TLS is most often implemented on a per-node and per-application basis, therefore offering node-to-node (also referred to as "end-to-end") encryption of data, and authentication of an individual node, application, or user of an application. This allows nodes of varying security trust to coexist on a common network and establish connections with other nodes (within the same zone or different zones) with differing security levels.

TLS typically uses X.509 digital certificates to provide authentication as well as to manage encryption keys. Use of digital certificates is discussed in a separate section of this document.

Either IPsec or TLS are appropriate for securing wide-area communications, such as C37.118. If TLS is used, recommendations from IEC 62351-3 should be followed.

Since the wide-area connections are already using IP-based WAN technology, the additional latency and jitter introduced by the implementation of IPsec or TLS should be of little concern, and the high-speed

nature of most modern WAN infrastructure minimizes the impact of the increased bandwidth introduced by the IPsec or TLS protocols.

Digital Certificates

Digital certificates, and the corresponding use of public key infrastructure (PKI), can provide for authentication of users or computer nodes. Many users are familiar with PKI concepts when securely browsing websites on the Internet. In the general case, websites present a certificate to the web browser to establish that the user (browser) is connecting to the website they expect. In this case, there are no certificates required on the web browser end of the communication since the website doesn't need to know who is browsing it and can use alternate methods (such as username and password) to provide identification and authentication of the user accessing the website.

If both ends of a communication link need to verify the identity and authentication of the other ends of the communication link, both need to have a certificate that is presented to the other end to mutually verify identity and authentication before the link is used to exchange data. This happens automatically when establishing connections using TLS or an equivalent protocol without any user interaction, making it ideal for machine-to-machine communication.

To establish a secure and authenticated link between two nodes, each node must send its public key in certificate form to the other end to be verified using the corresponding private key. Once the keys are verified, and the identities are confirmed and validated, the connection is established, and data can flow. Connections using digital certificates can be established with either authentication only, or the connection can encrypt the data portion, providing confidentiality of the data. If the connection is established as authentication only, the data is available for inspection, for example to diagnose data communication problems. For most information technology or business commerce applications, confidentiality is important, so the links are commonly encrypted. For telemetry and control applications, integrity and the ability to diagnose problems is important, so connections are often not encrypted. Many telemetry and control applications support both cases, allowing a connection to be diagnosed during initial commissioning, and then encrypted once the application is commissioned.

Using digital certificates allows the trust to be managed independently by revoking certificates associated with untrusted (or no longer trusted) accesses. Certificates can be self-signed, if that poses an acceptable level of trust, or can be issued by a third-party CA. Certificates can be revoked by the certificate authority using either a certificate revocation list (CRL), or, if supported, the online certificate status protocol (OCSP). Each application must determine the processing associated with handling expired or revoked certificates, and if using OCSP, what actions should take place if communication with the OCSP server cannot be established. Standard IEC 62351-9 provides guidance in these areas.

MODBUS/TCP Security

In October 2018, the Modbus Organization released a specification for the Modbus Security Protocol[6]. The specification applies to Modbus/TCP and uses Transport Layer Security (TLS) to secure the transmission of Modbus packets. According to the press release announcing the specification, "TLS will encapsulate Modbus packets to provide both authentication and message-integrity protection. The new protocol leverages X.509v3 digital certificates for authentication of the Server and Client."[7] This

[6] See http://modbus.org/docs/MB-TCP-Security-v21_2018-07-24.pdf
[7] See http://modbus.org/docs/Modbus-SecurityPR-10-2018.pdf

addresses the security vulnerabilities described in the previous section, including the ability to view the data in transit by encrypting it, the ability to modify the data in transit by providing cryptographically secure message integrity, and the ability to transmit rogue commands by authenticating the Modbus client and server.

The MODBUS/TCP Security protocol specifies a standard method of implementing TLS security and X.509 v3 certificates to secure the transmission of Modbus/TCP messages.

The use of TLS and X.509 v3 certificates by the Modbus Security Protocol is very similar to that specified in IEC 62351.

Since the Secure Modbus protocol is relatively new, its use will not be widespread until it is adopted and implemented by Modbus client and server software.

Secure ICCP

Security enhancements for ICCP were discussed and introduced in the early 2000's[8] and rely heavily on techniques that are now standardized in IEC 62351. However, the use of multiple digital certificates for securing the individual logical connections found between the primary and backup servers at primary and backup control centers has been found to be cumbersome and impractical[9]. Most control center links in North America are secured using site-to-site VPNs using IPSec, rather than the features of secure ICCP.

IEC 61858

GOOSE and SV

Very little can be done to secure GOOSE and SV traffic, due to the timing requirements and resource constraints placed on their use. IEC 62351-6 (approved in 2007) was intended to be used, specifying public and private keys for signatures and encryption of the messages. However, processing requirements to support this approach were insufficient and could not maintain the performance required for the application. A new version of IEC 62351-6 is in development.

Based on experiences from attempting to secure GOOSE and SV, a different approach was selected for securing the routable versions of the protocols: R-GOOSE and R-SV. Symmetric keys are used to protect the R-GOOSE and R-SV payloads and are managed and distributed by a key distribution center application based on the Group Domain of Interpretation (GDOI) as specified in RFC 6407 with the extensions in RFC 8052. IEC 62351-9 is used to provide a public/private key exchange to share the shared symmetric keys.

MMS

MMS traffic can be secured either with authentication or with encryption using procedures defined in IEC 62351-4 or IEC 62351-3.

---

[8] *Inter-Control Center Communications Protocol (ICCP, TASE.2): Threats to Data Security and Potential Solutions*, EPRI, Palo Alto, CA: 2001. 1001977.

[9] See https://www.pnnl.gov/main/publications/external/technical_reports/PNNL-26729.pdf

IEC 62351-3 and IEC 62351-6 provide for the use of TLS 1.2[10] to provide strong authentication and integrity of network traffic, while still allowing the traffic to be transmitted in plain text so that it can be inspected as it crosses security boundaries (e.g., NERC CIP ESPs). TLS 1.2 uses PKI and X.509 v3 format digital certificates to provide authentication and generate cryptographically secure hashes of the data to ensure that the messages were not modified in transmission. It includes a timestamp and sequence number as part of the processing to minimize the ability to retransmit (replay) existing commands.

IEC 62351-4 specifies the security protocols for the MMS protocol. It discusses security using two different profiles: the "T- profile" provides security for the "transport" layers of the OSI stack, specifically OSI layers 1-4, and the "A- profiles" provide security for the "application" layers of the OSI stack, specifically OSI layers 5-7.

Transport level security (the T- profile) specifies the use of TLS as described in standard IEC 62351-3, by specifying a specific set of options and parameters for the TLS configuration. IEC 62351-4 specifies TLS configuration parameters such as:

- TLS cipher suites supported
- CRL evaluation periods
- OCSP processing
- Validation of certificates

Application level security (the A- profiles) performs peer authentication using MMS features to pass authentication information comprised of an X.509 certificate, a time stamp, and a digitally signed time value in the Application Association Request (AARQ) and Application Association Response (AARE) messages of the MMS Association Control Service Element (ACSE). The X.509 certificate is used to verify the identity and check the authorization for each end of the communication link, while the time stamps and digital signatures are used to prevent replay attacks.

Both the A- and T- profiles use of X.509 certificates include using CRL and OCSP processing to handle revoked and expired certificates as specified in IEC 62351-9, with expired certificates generally allowing a connection with an optional warning issued, while revoked certificates generally cause existing connections to be terminated and new connections not to be established. These actions should be taken in coordination with an individual user's security policy.

Secure Protocols

While most protocols implement security through the use of wrapper technology, a truly secure protocol includes security as a set of built-in commands and structures. The advantage of using wrapper technology is that no modifications are required to the underlying protocol, making implementation more straightforward, and the same unmodified diagnostic tools can be used (once the wrapper has been stripped off the protocol). The disadvantage is that an additional software package or configuration is required.

It is anticipated that most future development of communication protocols will include security or secure options within the protocol itself. DNP3 Secure Authentication is an example of a protocol that inherently includes security.

[10] Note that TLS 1.3 has deprecated the use of all cipher suites that did not specify encrypting the payload.

DNP3 Secure Authentication

DNP3 Secure Authentication (DNP3 SA) is an example of a protocol modification to provide secure communication. DNP3 SA provides extensions to the traditional DNP3 payload, adding support for key management. It does not provide confidentiality of the data.

The primary goals of DNP3 SA are to ensure that an outstation can unambiguously determine if it is communicating with an authorized user at the central station, and the central station can unambiguously determine it is communicating with the correct outstation. The processing is consistent with that described in IEC 62351-5.

It is designed to address rogue devices masquerading as legitimate devices, modification of data packets, replay of commands and requests, and eavesdropping on the exchange of cryptographic keys. It provides authentication at the application layer, allowing its use over different transport technologies, including serial and network, and in architectures that bridge different network technologies, such as terminal servers and IP radios. It uses pre-shared keys and provides a mechanism to remotely change the pre-shared keys, protecting them with either symmetric or asymmetric (e.g., PKI) cryptography.

DNP3 SA requires that secure devices (i.e., those implementing DNP3 SA) must be able to interoperate with non-secure devices (i.e., those not implementing DNP3 SA), but recommends that secure devices not attempt to send security messages to non-secure devices.

Time Synchronization

As noted in previous sections, accurate and precise time is required by many telemetry and control protocols. Distribution of time over the same communication networks as the telemetry and control data requires that it should also be secured.

Time Synchronization Protocols

This section provides an overview of the common time synchronization protocols and methods commonly found in telemetry and control systems. The functions and features of each will be described, followed by a discussion of the security capabilities available for each protocol.

Time synchronization protocols are transmitted by devices called clocks. In order for the time in the protocol to be accurate, clocks must have access to an accurate and precise time source. The most common time source is a radio-based clock receiver (usually Global Navigation Satellite Systems [GNSS][11]), however, other radio-based time sources such as radio station WWVB, enhanced long range navigation [eLORAN], and cellular may be used) allowing for time signals at multiple locations to be synchronized through the radio-based time source. Since the radio signals can be interrupted, most clock receivers have internal oscillators that maintain time until the signal can be re-established (called "hold-over"). In cases where a radio-based time source cannot be used, a local atomic clock can be used as the time source.

Inter-Range Instrumentation Group (IRIG)

The Inter-range instrumentation group (IRIG) time distribution format was developed by the U.S. military in the late 1950's and was published in 1960 as a method of distributing a common time signal over large geographic distances for the purpose of synchronizing and timestamping measurements. Its current format, IRIG-200[12], last updated in 2016, provides for six different message formats (A, B, D, E, F, G, H), with a number of different modulation methods. The U.S. utility industry typically uses the IRIG-B format, either as a digital or modulated analog format. IRIG-B signals are carried over a dedicated cable infrastructure, most commonly 50 ohm coax, but other media such as twisted pair can be used. IRIG-B cable lengths are generally limited to approximately 50m for digital signals, and 300m for modulated signals; however, cable, transmitter, and receiver characteristics may alter these distances. For these reasons, utility use of IRIG-B is typically within a single generation plant or substation, and is not transmitted long distances. Each individual site typically has its own radio clock receiver or has access to a network time source such as those described below. The precision of time distributed by IRIG-B is approximately 1 microsecond.

Redundancy requires either an IRIG generator to have multiple clock sources and an algorithm to select which clock source will be used, or multiple IRIG inputs to end devices (supporting multiple IRIG generators) with an algorithm in the end device to select which IRIG source is used. These are rarely seen.

[11] Note – GNSS is the generic name used to describe systems like the generic name for systems like the Global Positioning Satellite (GPS) system. Other GNSS systems include China's BEIDOU, Russia's GLONASS, Europe's GALILEO, and Japan's Quasi-Zenith Satellite System (QZSS).
[12] See https://apps.dtic.mil/dtic/tr/fulltext/u2/1013738.pdf

Since IRIG-B is not a network protocol, security of the signal is based on physical security of the cabling and equipment, as well as the security of the radio-based time source.

Network Time Protocol (NTP)

Network Time Protocol (NTP), is an Internet Engineering Task Force (IETF) standard first published in 1985, and is currently in its fourth version (NTPv4)[13] published in 2010. NTP uses a hierarchy of clocks, with each level of hierarchy referred to as a stratum. Stratum 1 clocks are directly tied to a time source (also referred to as a Stratum 0 clock), which could be a highly precise and accurate atomic clock, or a GNSS receiver, producing the most accurate time synchronization messages. Time synchronization messages are transmitted across a network using a client-server protocol, to other NTP servers and to NTP clients. NTP servers at different stratum levels synchronize with NTP servers at lower-numbered stratum levels and provide client services to servers and clients at higher numbered stratum levels. The higher the stratum level, the "further" it is from the primary time source, and the less accurate the time may be.

The time signals, in the form of network messages, are transmitted across wide-area and local-area networks from NTP servers to other NTP servers and NTP clients. NTP client processing includes a method to determine and correct the time errors that have been introduced by the networking infrastructure due to network propagation and processing delays. Time precision for NTP is approximately 1 millisecond, but may be affected if there is significant variability in the network architecture (e.g., path route reconfiguration, asymmetric communications paths, or non-deterministic propagation delays).

NTP clients synchronize their clocks by making small adjustments to the local time until it matches the time provided by the NTP server (however, if the time difference is too great, a manual adjustment may be necessary in order to get the client clock "close enough" to be synchronized). Once synchronized, the client periodically polls the server (generally about every 10 minutes) to maintain synchronization.

Redundancy in an NTP network allows for multiple NTP servers at each stratum level, with the protocol selected and NTP application coded to determine the "best" NTP server.

NTPv3 clients can be configured to use Message Digest Encryption 5(MD5) encrypted symmetric keys configured in the NTP server and NTP client to authenticate time stamps provided by a time server, providing authentication of the time server and integrity (tamper detection) of the time synchronization message. Time synchronization messages are not encrypted.

NTPv4 has been extended to use public key encryption (PKI) using the OpenSSL library with X.509 formatted certificates to manage the PKI functions. As with NTPv3, time synchronization messages are not encrypted.

Simple Network Time Protocol (SNTP)

Simple Network Time Protocol (SNTP) is also an IETF standard, last updated in 2006, and is in its fourth version (SNTPv4)[14]. It uses the same packet structure as NTP, but with simplified processing on the client. SNTP clients can synchronize with NTP servers.

[13] See https://tools.ietf.org/pdf/rfc5905.pdf
[14] See https://tools.ietf.org/pdf/rfc4330.pdf

SNTP clients only synchronize with a single NTP server, and client algorithms do not provide the same level of accuracy as NTP clients. With no provision to assess the quality or stability of the time message from the NTP server, a lower quality time synchronization solution is provided. However, due to their simplicity and low processing requirements, they are found in embedded devices like protective relays. Modern PCs no longer use SNTP (using full NTP instead) due to the increase in their computing capability. Because of the variability of implementation, and with no specific protocol support to assess precision, SNTP is "less precise" than NTP, but it is difficult to quantify exactly by how much.

There is no security available to secure SNTP clients due to the low computing resources typically found in an SNTP client. SNTP clients will accept any time synchronization message received, without the ability to assess the quality of the time source.

IEEE 1588 (Precision Time Protocol - PTP)

The IEEE Standard 1588, IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems, also known as Precision Time Protocol (PTP), was originally defined and standardized by the IEEE in 2002, with the most recent version released in 2008[15]. It is a network-based time synchronization protocol that uses the concept of a "grandmaster" clock as the root clock for the environment. Multiple masters are supported for redundancy, with an algorithm to select the "best" grandmaster. Once the best grandmaster clock is selected, other clocks in the infrastructure synchronize to it. If the grandmaster fails, the algorithm provides for re-selecting the best grandmaster clock from the remaining master clocks. Other kinds of clocks include "boundary clocks" and "ordinary clocks." Boundary clocks connect to multiple LAN segments and are used to accurately synchronize one LAN segment to another. Ordinary clocks connect to a single LAN, which is either the source or destination of the synchronization reference.

IEEE 1588 takes advantage of hardware assist capabilities built into Ethernet switches to minimize latency and jitter that can be introduced. Many modern Ethernet switches have this capability as a standard feature.

IEEE 1588 also uses a client-server architecture in which network packets are sent from the master clock (the server) to the slave clocks (the clients), generally using a multicast address, relying on the client to transmit packets periodically back to the server to calculate the round-trip delay. The protocol is designed to support sub-microsecond accuracy and precision. This level or precision dictates that the network transport is limited to LAN technologies and works best when the network infrastructure supports the hardware assist features.

There is an "experimental" security protocol extension to the 2008 version of the IEEE 1588 standards, but it is likely not implemented in commercial clocks. Due to the nature of the processing required on the switches, and their required ability to modify the 1588 packets to update latency, end-to-end encryption of the packets is not an option. These features are expected to be included in the upcoming version of the standard.

Time Synchronization Recommendation

Using IEC 61850 for telemetry and control requires that the data packets be identified with an accurate and precise timestamp. A precise clock with a GNSS time source is the most economical method of obtaining an accurate and precise time in a network (especially with geographically disperse locations),

[15] See https://standards.ieee.org/standard/1588-2008.html

but it requires a mechanism for transporting the time signal across a network. (IRIG may also be used but requires additional cabling to carry the IRIG signal.) IEEE-1588 provides a mechanism for accurately and precisely synchronizing clocks or time sources on a local network and at the required precision for use by IEC 61850. IEEE Standard C37.238 provides an IEEE 1588 profile created for the electric power industry that meets the needs of IEC 61850 and synchrophasor networks. The latest version of the IEEE C37.238 standard consists of two major components: a “base profile” contained in IEC/IEEE 61850-9-3:2016 and an “extended profile” contained in IEEE C37.238-2017. The extended profile contains support for dynamic time inaccuracy for better monitoring of delivered time quality and IRIG-B replacement and support for protocol converters.

In order for an Ethernet network containing switches to properly transmit the IEEE 1588 packets, they must be “IEEE 1588 aware”, i.e., they must have logic in them to detect IEEE 1588 data packets and adjust the time to account for the processing time required by the switch to process and transmit the IEEE 1588 data packets. Switches with this processing are known as “transparent clocks.”

For equipment not supporting IEEE-1588, support for NTP or SNTP is often included in clock receivers that support IEEE-1588. IRIG-B capability may also be available.

Most cryptographic protocols include provision for including a timestamp as part of the hash or encryption process to preclude the re-use of validly formed and processed data in a “replay attack.” This means that time at both ends of the secured communications channel must be synchronized. This can be accomplished by the use of a universally accessible time source, such as GNSS, with clock receivers at all geographic locations, or if applicable, the use of a network-based time distribution accessible at all points in the network requiring accurate and precise time. Either IEEE 1588 or NTP can be used as the basis for the time distribution. NTP is often less expensive, but not as precise, while IEEE 1588 is much more precise but at an additional cost.

Communication Protocols

The following table is a partial list of telemetry and control communication protocols commonly found in energy delivery systems. This table is included for informational purposes only.

Vendor or Standard	Variant
IEC 60870-5	101
	103
	104
DNP3	Serial
	WAN/LAN
IEC 61850	MMS
	GOOSE
	SV
IEC 60870-6 (ICCP or TASE.2)	
IEEE C37.118	
Modbus	ASCII
	RTU
	TCP/UDP
ABB	Spa Bus
	RP-570
	RP-571
	Triguard Peer
	Indactic 33/1
	Indactic 33/41
	Indactic 33/41 Ext.
ACS	3100
AEP	Synchronous
	Asynchronous
Alstom	Courier RS485/RS232

Altus	Modbus (custom)
Amtrak	SDLC
ASEA	ADLP 80
	ADLP 180
ASW	LS RTU1
Avista	Independence 1000
BACnet	IP
Bailey	MPC
Boeing	SDLC
CAE	Micro RTU1
	HDLC
CDC	Type 1
	Type 1-12 bit address
	Type 1 ASCII
	Type 2
	Type 2 synchronous
	Type 2 extended
CDT	Type 1
	Type 2
	Type 3
	Type 4
	Type 5
Cegelec	HN Z 66 S 11/15
CMC Master	CMC Master
Compumech	CD-4150
Conitel	300
	2000
	2020
	2025

	2100B
	2100H
	2100M
	3000
DLMS	Serial / HDLC
	TCP Profile
DYNAC	DYNET
Excom	Modbus Custom
Ferranti	Van Comm
Fuji	
Getac/Betac	7020/4-BCH
	7020-LP
	SDLC
GE	Modbus Custom
Harris	5000/6000
	Micro 2
	Micro 3
HNZ	Gas Analyzer
Honeywell	7000
Landis & Gyr	See Telegyr
Moore	9000
Newfoundland	
NMEA	NMEA 0183
OPC-COM	DA
	AE
OPC-XML	DA
Paybus	
Pert	26/31
PG&E	2179

QEI/Quindar	QPLH1
	QuicsII
	Quics IV1
Quantum	DNP 1/QDIF
RainWise	Serial
RDSO	SPORT
Recon	1.1
Redac	70D
	70H
Redsad	
Rockwell	5010
	5011 (standard)
	5011 (PSI)
	5012
	5020
RTK/ Cooper	RTK ASCII
Scadapac	1
	5
SCA	2500
SCI	RDACS1
SEL	300G
	311
	421
	451
SEPAM	Modbus Custom
SES 92	
SES 92 (GRE)	
SES 92 IP (GRE)	
Siemens	Sinaut 8-FW/DPDM

	Profinet
	Profibus
Southern Services	
Southwestern Pub. Svc Co.	SPS
Systems Control SC1801	5
	5.2
	5.4.1
	5.5
	6
Systems Northwest	11
	111
	Distribution
Toshiba	
Telegyr	BOA
	BOA Byte
	MPS9000 Async
	Telegyr 8065 or MPS9000 Sync
	Telegyr 800
	Telegyr 8979
TLC 11M	
TRW	850
	9550
	System 9
Valmet (Tejas)	Series 3
	Series 5
	Series 5 extended
Westinghouse	Wisp+
	Wisp+ Extended
Weston	Recon 1

http://gridmodernization.labworks.org/