IEC 61850 Protocol

Communication standard for electrical substation automation

OT Security Learning Series

Document 206 | January 2026

Contributors: Matthias Niedermaier

Created with AI assistance

LEARNING RESOURCE

Contents

1 Introduction

Information

IEC 61850 is the international standard for communication in electrical substations. It enables interoperability between protective relays, circuit breakers, transformers, and control systems in power grid infrastructure.

Key characteristics:

- International standard for substation automation
- Object-oriented data modeling
- Multiple communication services (MMS, GOOSE, SV)
- Designed for power utility environments
- Critical infrastructure protocol

Critical

IEC 61850 controls protective relays and circuit breakers in the power grid. Attacks on this protocol can cause equipment damage, widespread outages, or safety hazards. The Industroyer/CrashOverride malware targeted IEC 61850.

2 Protocol Architecture

2.1 Data Model

IEC 61850 uses a hierarchical object model:

- **Physical Device** – The actual hardware
- **Logical Device** – Functional grouping within physical device
- **Logical Node** – Specific function (e.g., XCBR for circuit breaker)
- **Data Object** – Attributes of the logical node
- **Data Attribute** – Individual values

2.2 Logical Node Examples

3 Communication Services

Logical Node	Function
XCBR	Circuit breaker
XSWI	Disconnector/switch
PDIS	Distance protection
PTOC	Overcurrent protection
MMXU	Measurement unit
CSWI	Switch controller

Table 1: Common IEC 61850 Logical Nodes

3.1 Service Types

IEC 61850 Communication Services

- **MMS (Manufacturing Message Specification)** – Client/server for configuration, reporting
- **GOOSE (Generic Object Oriented Substation Event)** – Fast multicast for protection events
- **SV (Sampled Values)** – Real-time measurement streaming
- **Time Sync** – Precision time protocol (IEEE 1588 PTP)

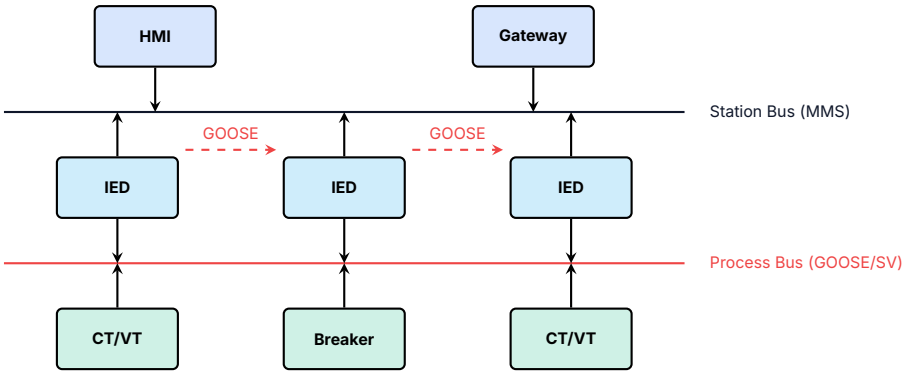

Figure 1: IEC 61850 Substation Architecture

3.2 Network Ports

Service	Port/Type	Purpose
MMS	TCP/102	Configuration, reporting
GOOSE	EtherType 0x88B8	Protection events (Layer 2)
SV	EtherType 0x88BA	Sampled measurements (Layer 2)
PTP	UDP/319, 320	Time synchronization

Table 2: IEC 61850 Network Services

4 GOOSE Protocol

4.1 GOOSE Characteristics

- Layer 2 multicast (no IP routing)
- Sub-4ms transmission for protection
- Publisher/subscriber model
- Carries binary status and commands
- Critical for protection coordination

4.2 GOOSE Message Structure

- **goID** – GOOSE identifier
- **gocbRef** – Control block reference
- **datSet** – Dataset reference
- **stNum** – State number (increments on change)
- **sqNum** – Sequence number
- **allData** – Actual data values

Warning

GOOSE operates at Layer 2 with no authentication. An attacker on the same network segment can inject GOOSE messages to trip breakers or block protection signals.

5 Security Vulnerabilities

Critical

The base IEC 61850 standard (Edition 1 and 2) includes no security mechanisms. GOOSE and SV are particularly vulnerable as they operate at Layer 2 and must be processed within milliseconds.

5.1 Protocol Weaknesses

- **No authentication** – Messages accepted from any source
- **No encryption** – All traffic in cleartext
- **Layer 2 protocols** – GOOSE/SV bypass IP firewalls
- **Time-critical** – Security checks may impact performance
- **Multicast** – Easy to sniff and replay

5.2 Attack Vectors

- **GOOSE injection** – Send fake trip commands to breakers
- **GOOSE blocking** – Prevent legitimate protection signals
- **SV manipulation** – Inject false measurements
- **MMS exploitation** – Unauthorized configuration changes
- **Time sync attacks** – Disrupt PTP to desynchronize protection
- **Replay attacks** – Capture and replay GOOSE messages

5.3 Industroyer/CrashOverride

The 2016 Ukraine power grid attack used IEC 61850:

- Targeted IEC 61850 and other substation protocols
- Opened circuit breakers causing outages
- Demonstrated real-world IEC 61850 attack capability

6 IEC 62351 Security Standard

Key Point

IEC 62351 provides security extensions for IEC 61850 and other power system protocols. It addresses authentication, integrity, and confidentiality requirements.

6.1 IEC 62351 Components

- **Part 3** – TLS for TCP-based protocols (MMS)
- **Part 4** – Security for MMS specifically
- **Part 6** – Security for GOOSE and SV (digital signatures)
- **Part 8** – Role-based access control
- **Part 9** – Key management

6.2 GOOSE Security (IEC 62351-6)

- Digital signatures for message authentication
- Requires hardware acceleration for timing
- Adds 20 bytes overhead per message
- Limited vendor implementation

> **Warning**
>
> IEC 62351 adoption is slow. Most installed IEC 61850 devices lack security features, requiring network-based protection.

7 Security Mitigations

7.1 Network Architecture

- **Physical isolation** – Separate process bus from station bus
- **VLAN segmentation** – Isolate GOOSE/SV traffic
- **Managed switches** – Port security, disable unused ports
- **No remote access** – Or strictly controlled VPN only

7.2 Layer 2 Security

Since GOOSE/SV are Layer 2:

- MAC address filtering
- 802.1X port authentication
- Private VLANs
- Physical access control to network equipment

7.3 Monitoring

- Monitor for unauthorized GOOSE publishers
- Alert on stNum/sqNum anomalies
- Detect unexpected MMS connections
- Log all configuration changes
- Watch for time synchronization issues

8 Substation Architecture

8.1 Network Zones

- **Process Bus** – GOOSE/SV between bays (most critical)
- **Station Bus** – MMS to station controller
- **Remote Access** – Connection to control center

8.2 Defense in Depth

- Physical perimeter security
- Network segmentation between buses
- Firewall between substation and control center
- Intrusion detection for IEC 61850 protocols
- Secure engineering access procedures

9 Summary

Key Takeaways

- **Substation standard** – Controls breakers, relays in power grid
- **Multiple services** – MMS (TCP), GOOSE/SV (Layer 2)
- **Time-critical** – GOOSE requires sub-4ms response
- **No native security** – Base standard lacks authentication
- **Industroyer target** – Real attacks have occurred
- **IEC 62351** – Security extensions, limited adoption
- **Layer 2 isolation** – Critical for GOOSE/SV protection

10 Further Reading

Standards

- **IEC 61850** – Communication networks in substations
  https://webstore.iec.ch/publication/6028
- **IEC 62351** – Power systems security
  https://webstore.iec.ch/publication/6912

Resources

- **NERC CIP Standards**
  https://www.nerc.com/standards/reliability-standards/cip
- **CISA – Energy Sector Security**
  https://www.cisa.gov/topics/industrial-control-systems

Part of the OT Security Learning Series