IEC 62351: Security for Grid Automation and Control Protocols

Maik G. Seewald, CISSP

maseewal@cisco.com

March 2025

IEC TC 57 in a nutshell
Power Systems Automation

TC 57 is Power systems management and associated information exchange

…to prepare international standards for power systems control equipment and systems including EMS (Energy Management Systems), SCADA (Supervisory Control And Data Acquisition), distribution automation, tele-protection, and associated information exchange for real-time and non-real-time information, used in the planning, operation and maintenance of power systems."

15+ Working groups and Sub Committees are defining IEC 61850, CIM, Tele-Control Protocols, Cyber Security, EMS, Distribution Automation, DER Integration

- WG 10: Power system IED communication and associated data models
- WG 15: Data and communication security
- WG 17: Communications Systems for Distributed Energy Resources (DER)
- WG 19: Interoperability within TC 57 in the long term
- WG 21: Interfaces and protocol profiles relevant to systems connected to the electrical grid

IEC TC 57 WG15 in a nutshell
Security for Power System Control Networks

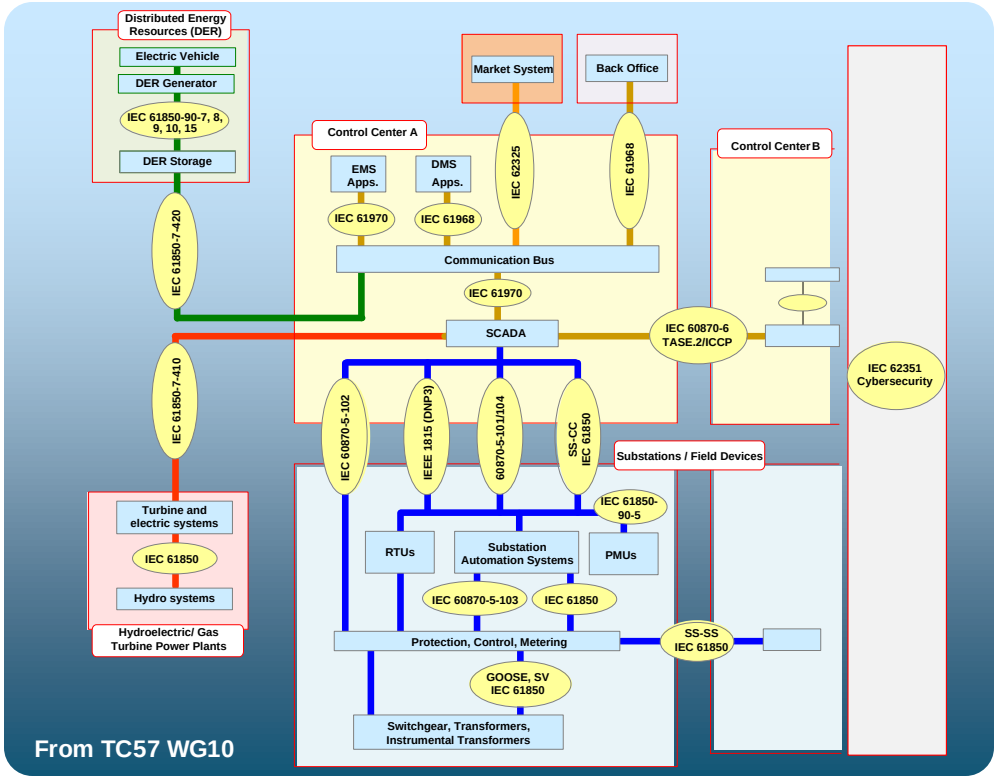
In IEC TC 57 (POWER SYSTEMS management and associated information exchange), WG 15 is responsible for IEC 62351, About 140+ members

Group charter:

- *"Undertake the development of standards for security of the communication protocols defined by the IEC TC 57, specifically the IEC 60870-5 series, the IEC 60870-6 series, the IEC 61850 series, the IEC 61970 series, and the IEC 61968 series."*
- *"Undertake the development of standards and/or technical reports on* ***end-to-end security*** *issues."*
- *"Review and advise on cyber security of TC57 standards."*

- Public Information: https://iec61850.dvl.iec.ch/what-is-61850/technical-principles/61850-cybersecurity/

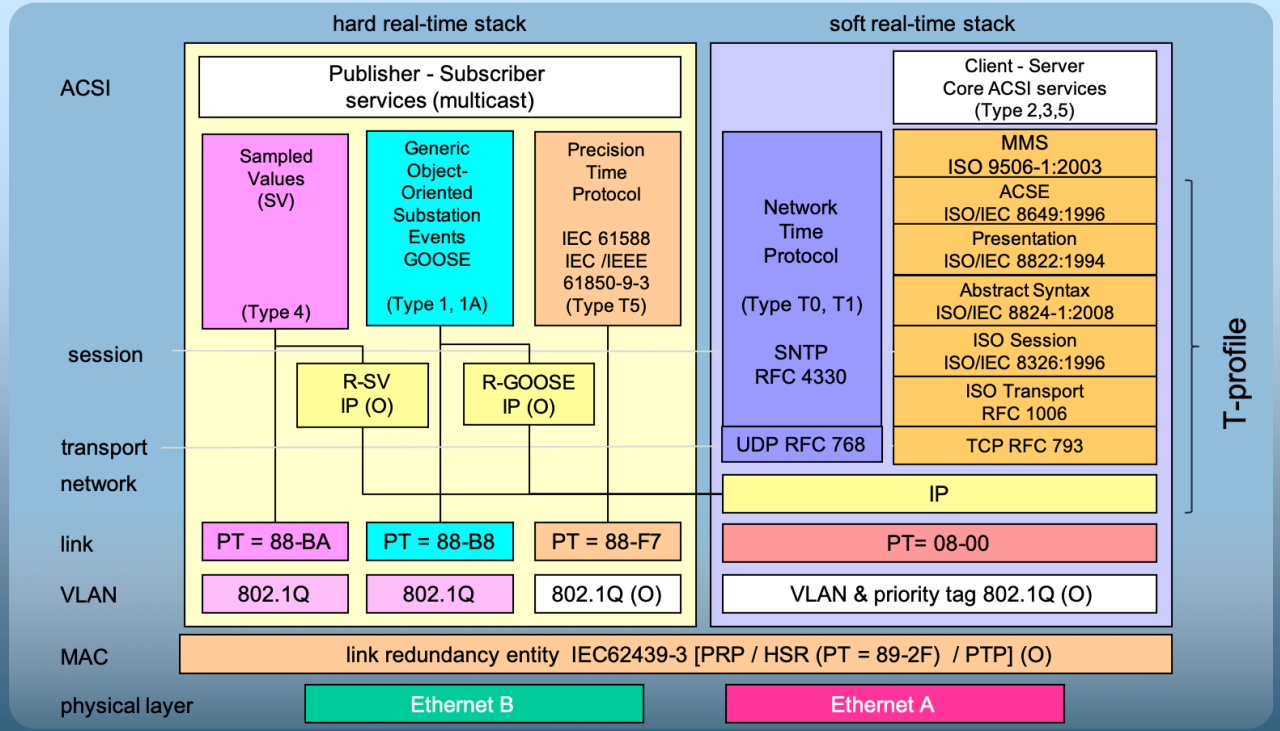
IEC 62351 – An Enabler for End-to-End Communication Security



Cyber Security Standards of IEC 62351 are an integral part of the IEC TC57 Reference Architecture, comprising:

- Protection of Ethernet, IP, and serial communication
- Authentication and authorization (including RBAC)
- Application layer security
- Security monitoring and event logging
- Test case definition
- Application Guidelines

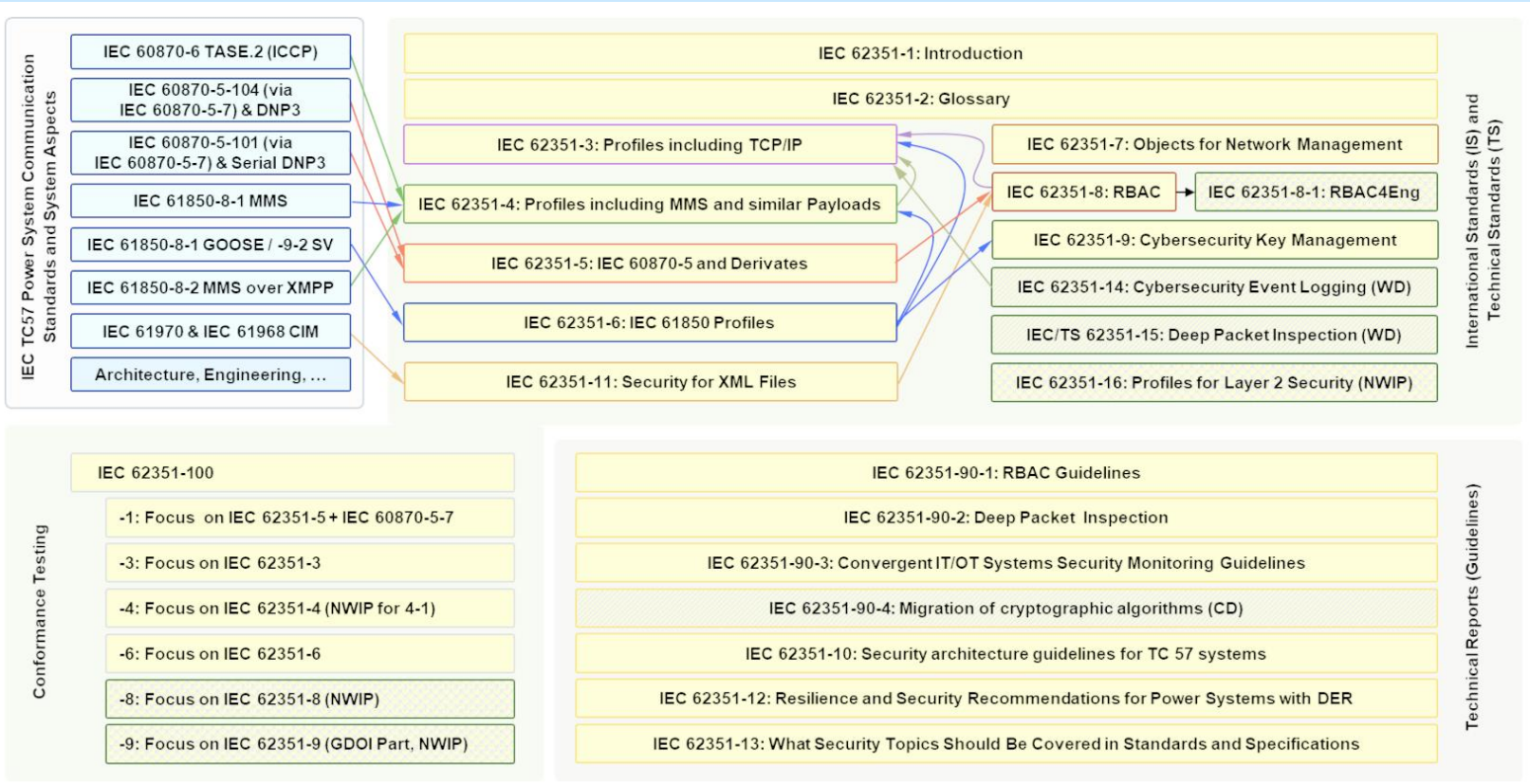
IEC 61850 Communication networks and systems for Power Utility Automation: Protocol Stack



The entire protocol requires protection based on adequate security controls

From TC57 WG10

IEC 62351 – An Enabler for
End-to-End Communication Security



Source: TC57 WG15

IEC 62351 Standard Series
NWIP: Part 16: Profiles for Ethernet security, MACsec I

Scope: *The IEC 62351 series defines standards and technical reports for the security of communication protocols defined by IEC TC 57, specifically the IEC 60870-5 series, the IEC 60870-6 series, the IEC 61850 series, the IEC 61970 series, and the IEC 61968 series. This document is Part 16 of the IEC 62351 series and describes MACsec profiles for Ethernet security.*

Purpose: *This standard specifies Media Access Control Security (MACsec) as a method for the security of OSI Layer 2 IEC 61850 protocols. This document is self-contained and meant to complement existing methods found in IEC 62351-6. Part 16 identifies how to implement MACsec with a focus on interoperability between devices both inside and outside substations in such a way as to provide low-latency encryption optimized for embedded devices to enable confidentiality for Layer 2 GOOSE and Sampled Values.*

IEC 62351 Standard Series
NWIP: Part 16: Profiles for Ethernet security, MACsec II

Details and Assumptions

- Interoperability
- 2+ Profiles
- MKA and GDOI for Key Management
- Interplay with PTP and IEC 62439-3 (PRP/HSR)
- Use of Ascon cipher suite?