IEC 62351 Compliant Gateways

IEC 62351 Compliance for IEC 60870-5-104 Protocol

IEC 62351 Compliance

- IEC 62351 standards for IEC 608705-104 protocol
- Only authenticated access
- Prevention of eavesdropping
- Prevention of playback and spoofing
- Intrusion detection

Key Benefits

- SCADA protocol conversion
- IEC 101, IEC 104, IEC 61850, DNP3, Modbus
- Substation-hardened. IP-rated rugged device
- Last GASP power with power failure message
- High isolation options on the PSU and interfaces
- Vibration and mechanical to EN standards
- Resilient communication paths
- Scalable to tens of thousands of devices
- Outdoor enclosures for wired or wireless routers

Overview

IEC 62351 is an industry standard aimed at improving security in automation systems in the power system domain. Virtual Access is committed to integrating their devices into an IEC 62351 environment as security threats become more and more of an issue in the power and automation industry.

Virtual Access' cyber-security capabilities help power utilities to comply with the IEC 62351 standard for the IEC 60870-5-104 protocol. The security objectives include authentication of data transfer through digital signatures, ensuring only authenticated access, prevention of eavesdropping, prevention of playback and spoofing, and intrusion detection.
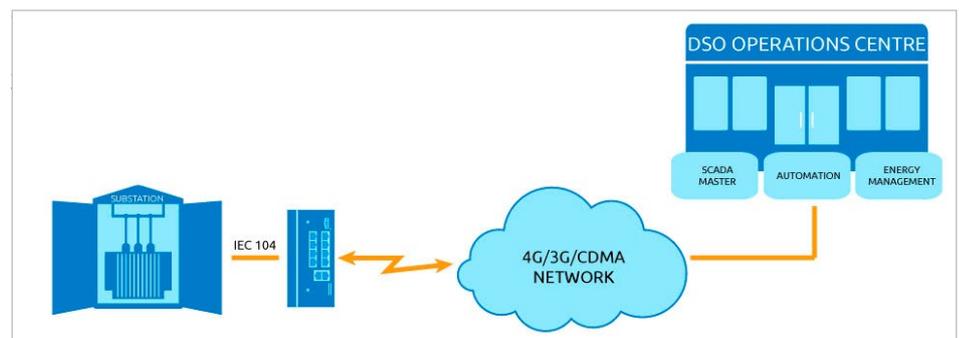
IEC 62351 contains provisions to ensure the integrity, authenticity and confidentiality for different protocols used in power systems. The different parts of IEC 62351 are described below.

IEC 62351 Part 3

Provides security for any profile that includes TCP/IP, including IEC 60870-6 TASE.2, IEC 61850 ACSI over TCP/IP, and IEC 60870-5-104. Specifically, IEC 62351-3 protects against eavesdropping through TLS encryption, man-in-the-middle security risk through message authentication, spoofing through Security Certificates IEC TC57 WG15 Security Standards ver 14 24 June, 2012 (Node Authentication), and replay, again through TLS encryption. However, TLS does not protect against denial of service. This security attack should be guarded against through implementation-specific measures.

IEC 62351 Part 4

Provides security for profiles that include the Manufacturing Message Specification (MMS) (ISO 9506), including TASE.2 (ICCP) and IEC 61850. It primarily works with TLS to configure and make use of its security measures, in particular, authentication: the two entities interacting with each other are who they say they are.

IEC 62351 Part 5

Provides different solutions for the serial version (primarily IEC 60870-5-101, as well as parts 102 and 103) and for the networked versions (IEC 60870-5-104 and DNP 3). Specifically, the networked versions that run over TCP/IP can utilize the security measures described in IEC 62351-3, which includes confidentiality and integrity provided by TLS encryption. Therefore, the only additional requirement is authentication.

IEC 62351 Part 6

IEC 61850 contains three protocols that are peer-to-peer multicast datagrams on a substation LAN and are not routable. The main protocol, GOOSE, is designed for protective relaying where the messages need to be transmitted within 4 milliseconds peer-to-peer between intelligent controllers. Given these stringent performance requirements, encryption or other security measures which may significantly affect transmission rates are not acceptable. Therefore, authentication is the only security measure included as a requirement, so IEC 62351-6 provides a mechanism that involves minimal compute requirements for these profiles to digitally sign the messages.

IEC 62351 Part 7

The scope of IEC 62351-7 focuses on Network and System Management (NSM) of the information infrastructure.

Power systems operations are increasingly reliant on information infrastructures, including communication networks, intelligent electronic devices (IEDs), and self-defining communication protocols. Therefore, management of the information infrastructure is crucial to providing the necessary high levels of security and reliability in power system operations.

The ISO CMIP and the IETF SNMP standards for Network Management can provide some of this management. In SNMP, Management Information Base (MIB) data is used to monitor the health of networks and systems, but each vendor must develop their own set of MIBs for their equipment. For power system operations, SNMP MIBs are only available for common networking devices, such as routers. No standard MIBs have been developed for IEDs, so vendors use "ad hoc" or proprietary methods for monitoring some types of equipment health. This standard thus provides MIB-like data objects (termed NSM data objects) for the power industry.

IEC 62351 Part 8

The scope of part 8 is the access control of users and automated agents to data object in power systems by means of role-based access control (RBAC).

IEC 62351 Part 9

Part 9 of the IEC 62351 series specifies how to generate, distribute, revoke and handle digital certificates, cryptographic keys to protect digital data and communication. Included in the scope is the handling of asymmetric keys (private keys and X.509 certificates), as well as symmetric keys (pre-shared keys and session keys).

IEC 62351 Part 10

Part 10 targets the description of security architecture guidelines for power systems based on essential security controls, i.e., on security-related components and functions and their interaction. Furthermore, the relation and mapping of these security controls to the general system architecture of power systems is provided as guideline to support system integrators to securely deploy power generation, transmission, and distribution systems applying available standards.

	CONFIDENTIALITY	INTEGRITY	AVAILABILITY	NON REPUDIATION	Requirements
	Unauthorised access to information	Unauthorised modification or theft or information	Denial of service or prevention of authorised access	Denial of action that took place or claim of action that did not take place	Threats
Passwords	✓	✓			
Certificates	✓	✓			
Audit Logging	✓	✓	✓	✓	
Public Key Infrastructure (PKI)	✓	✓			
Digital Signatures		✓		✓	
Virtual Private Network (VPN)	✓	✓			
Transport Level Security	✓	✓			
Role Based Access Control (RBAC)	✓	✓		✓	Key security services and technologies countermeasures
IEC62351 Security for DNP3	✓	✓		✓	
Access Control Lists (ACL)	✓	✓	✓		
Rate Limiting, Access Management			✓		
Network & System Management (NSM)				✓	