IEC 62351

In the RTU32 Series. Understand what it is

BRODERSEN

simplifying systems

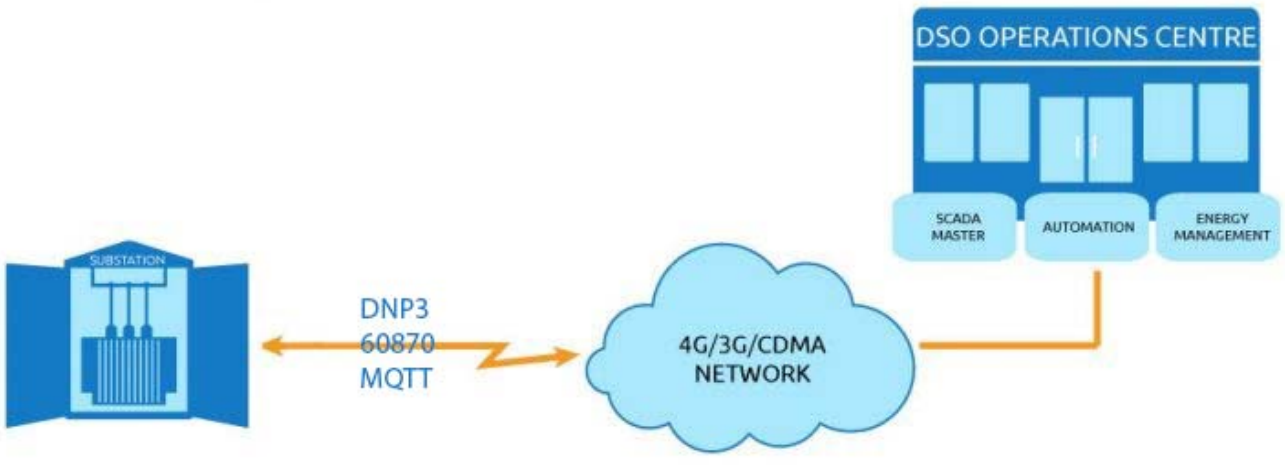
Overview

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.

Typical Network Scenario

An RTU using IEC 60870-5-104, DNP3, MQTT protocol is connected to top end over Ethernet. The connection can be IP radio, 4G or other wired or wireless connections that transports the data over a network to the top-end like DCS, SCADA, IOT platform or all in a mix.



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

Brodersen A/S, Islevdalvej 187, DK-2610 Roedovre, Denmark , Tel: +45 45 35 26 27, Fax: +45 45 35 26 29, Email: sales@brodersen.com

Security Certificates IEC TC57 WG15 Security Standards ver 14 24 June, 2012 (Node Authentication), and replay, again through TLS encryption.

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.

Brodersen A/S, Islevdalvej 187, DK-2610 Roedovre, Denmark , Tel: +45 45 35 26 27, Fax: +45 45 35 26 29, Email: sales@brodersen.com

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). In most larger utility companies the use of RBAC must be top managed through lightweight Directory Access Protocol (LDAP). In short, the possibility to control all users and their roles in the RTU from IT department.

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.

Brodersen A/S, Islevdalvej 187, DK-2610 Roedovre, Denmark , Tel: +45 45 35 26 27, Fax: +45 45 35 26 29, Email: sales@brodersen.com