USE61400-25
IEC 61400-25 user group

User group of wind information model

MEMBERS

* 1) OPC UA foundation members

SERVICES PROVIDED TO MEMBERS

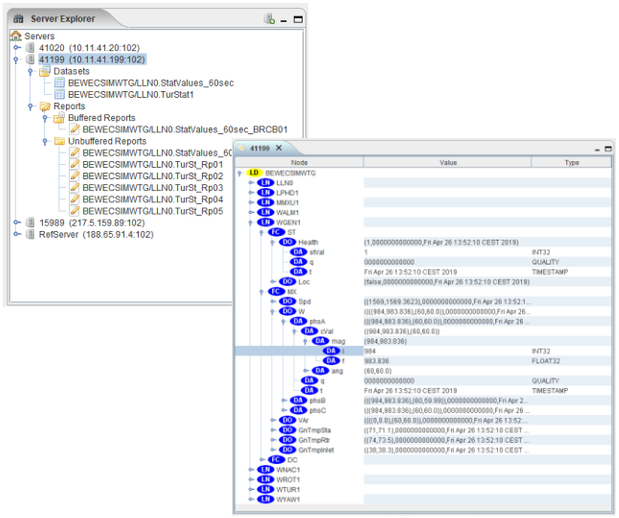
Access to workshops, implementation guideline and MMS Client

The main goal is to assist users with implementing the IEC 61400-25 standard.

The implementation guideline covers the following topics:

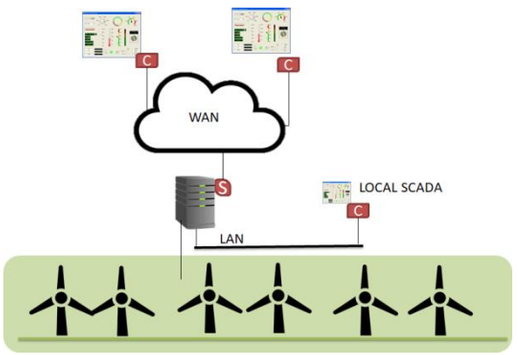
- Overview of the IEC 61400-25 standard series and the related standards
- Descriptions and examples how to read the standard
- Customization of the IEC 61400-25 models
- IEC 61400-25 as part of the wind power plant engineering process
- SCL guideline with examples

Open Source Client (MMS)
- Source code examples available



MMS-Client example

Use of the reference server implementation



It is a Wind Power Plant Server acting as a gateway that provides access to a simultated with farm using different communication mappings:

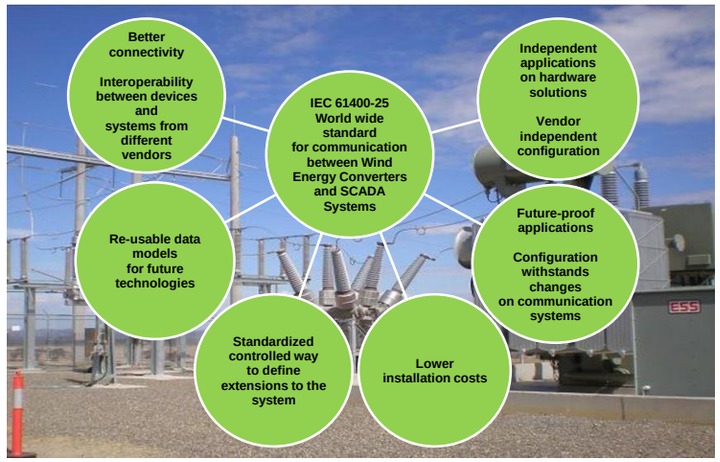
- mappings to IEC 61850 MMS, webservices, IEC 60870-5-104, DNP3 and OPC XML-DA (soon OPC UA).
- Connected to the information of existing Wind Turbine controllers.
- Simulate several wind turbines to provide a full wind power plant view.
- Accessed with any standard based client or with the specific software developed for the association members.

USE61400-25
IEC 61400-25 user group

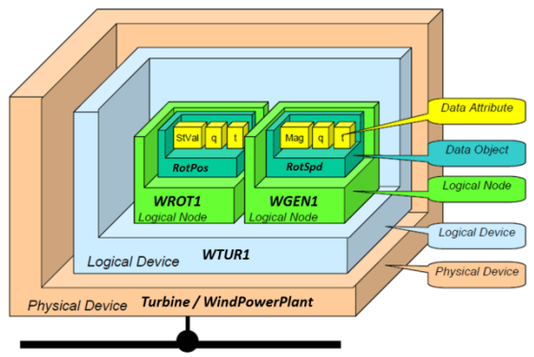
IEC 61400-25 is the wind information model for interoperable plant to supervision/operation/network control centers

AWEA WINDPOWER
Houston, TX | May 20-23, 2019

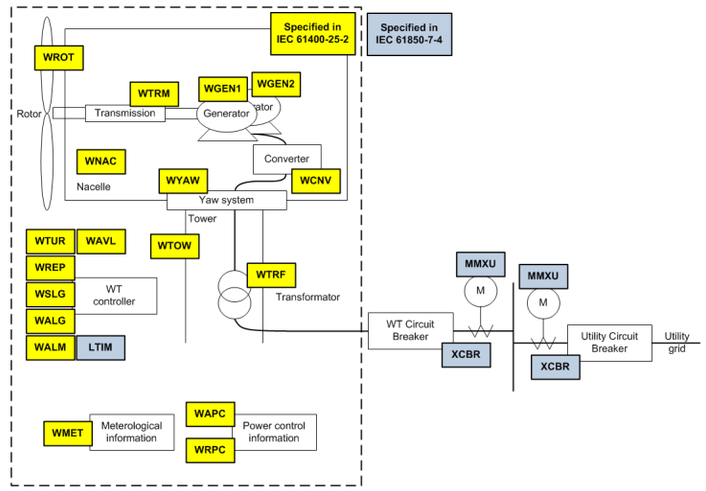
- IEC 61400-25 builds on IEC 61850 the worlds most used substation automation architecture
- enables connectivity between a heterogeneous combination of client and servers from different manufacturers and suppliers.
- only defines how to model the information, information exchange and mapping to specific communication protocols.
- excludes a definition of how and where to implement the communication interface, the application program interface and implementation recommendations.



Structure of wind power plant information model



Use of instances of logical nodes

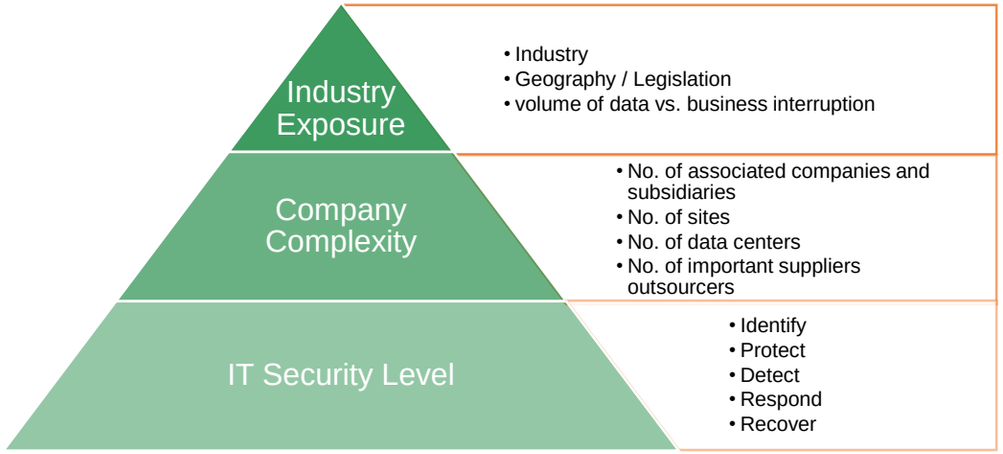


IEC 61400-25: Communications for monitoring and control of wind power plants

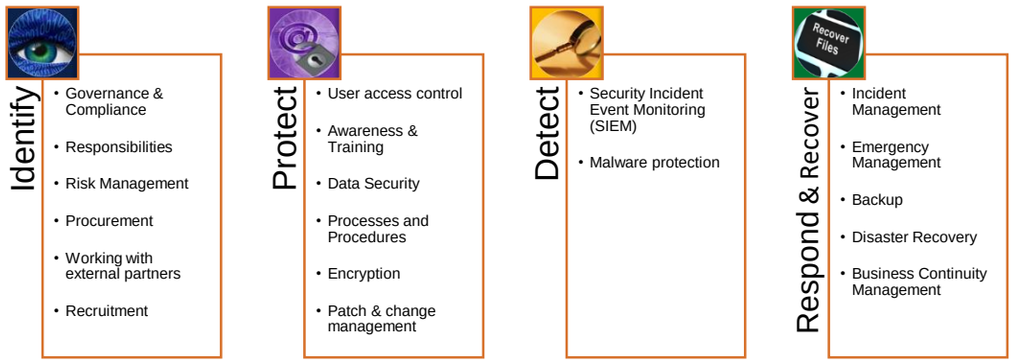
Standard series based on IEC 61850 (Communication networks and systems for power utility automation)

Standard	Description	State
61400-25-1	Overall description of principles and models	Edition 2, published 2017
61400-25-2	Information models	Edition 2, published 2015
61400-25-3	Information exchange models	Edition 2, published 2015
61400-25-4	Mapping to communication profile [web services, OPC XML-DA, MMS, IEC 60870-5-101/104, DNP3]	Edition 2, published 2016
61400-25-41	Mapping to communication profile based on IEC 62541 (OPC UA)	Edition 1, approved for CD 2019
61400-25-5	Compliance testing	Edition 2, published 2017
61400-25-6	Logical node classes and data classes for condition monitoring	Edition 2, published 2016
61400-25-71	Configuration Description Language	Edition 1, approved for publication 2019

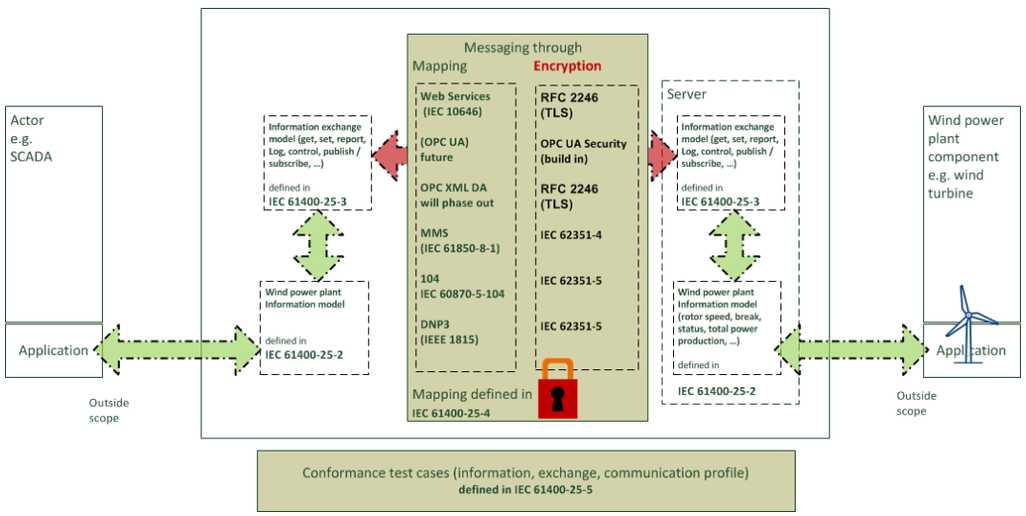
Comprehensive Approach to Cyber Risk Assessment



IT Security Level Evaluation



Build In Security By Using Security Standards



USE61400-25
IEC 61400-25 user group

Secure your wind communication with state-of-the-art IEC cyber security

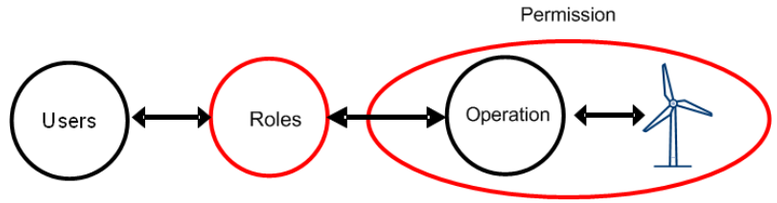
Security means defined for

- Authentication and authorization using Role Based Access Control (RBAC)
- Secure IP- based and serial communication
- Secure application level exchanges
- Security monitoring and event logging
- Test case definition
- Guidelines for applying specific security measures

by utilizing or profiling

- existing IEC standards and recommendations

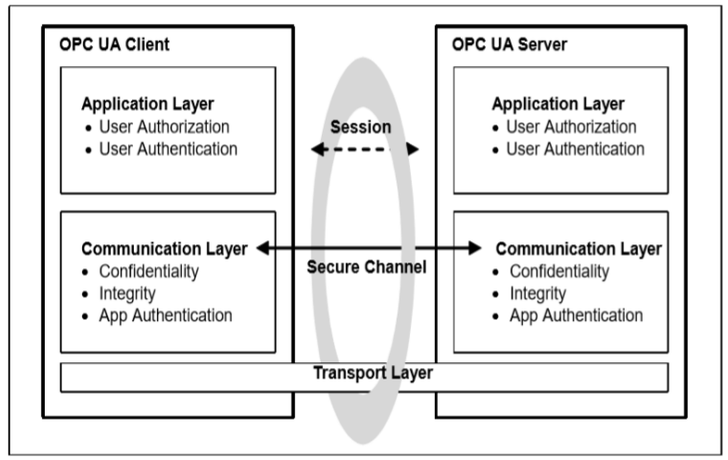
For example utilize IEC 62351-8:
RBAC supports verification of who has authorized and performed a dedicated action

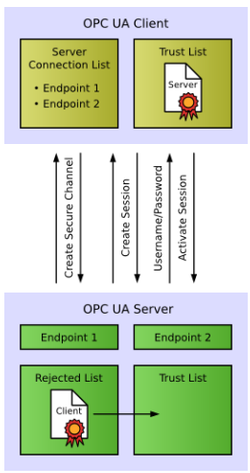


Combine IEC 61400-25 with OPC UA (IEC 62541)

Security features:

- User Authentication based on different user tokens
- User Authorization based on roles
- Secure communication channel with message signing and encryption based on Security Policies
- Application Authentication based on Application Instance Certificates
- Access control down to nodes and attributes
- Audit mechanisms for connection establishment, Write and Call services





Anonymous Identity Token
No user information is available.

Username Identity Token
A user identified by user name and password.

X.509 Identity Token
A user identified by an X509v3 Certificate.
Three types of X.509v3 certificates are used
OPC UA Application Instance Certificates
OPC UA Software Certificates
OPC UA User Certificates

Issued Identity Token
A user identified by a JSON Web Token (JWT).

Certificates are managed by PKI