USE61400-25
IEC 61400-25 user group

27. Windenergietage

November 6 - 8, 2018
Linstow, Germany

IEC 61400-25
Wind Power Plant Communication under the aspects
of cyber risks and complience to security standards

Bertram Lange
Senior Application Manager, Bachmann electronic GmbH,
IEC 61400-25 user group Chairman

Agenda

- **1** Introduction of the standard IEC 61400-25

- **2** Cyber Risk Assesment and complience to security standards

- **3** Examples and challenges of Wind Power Plant communication in Europe

- **4** Introduction of the IEC 61400-25 user group
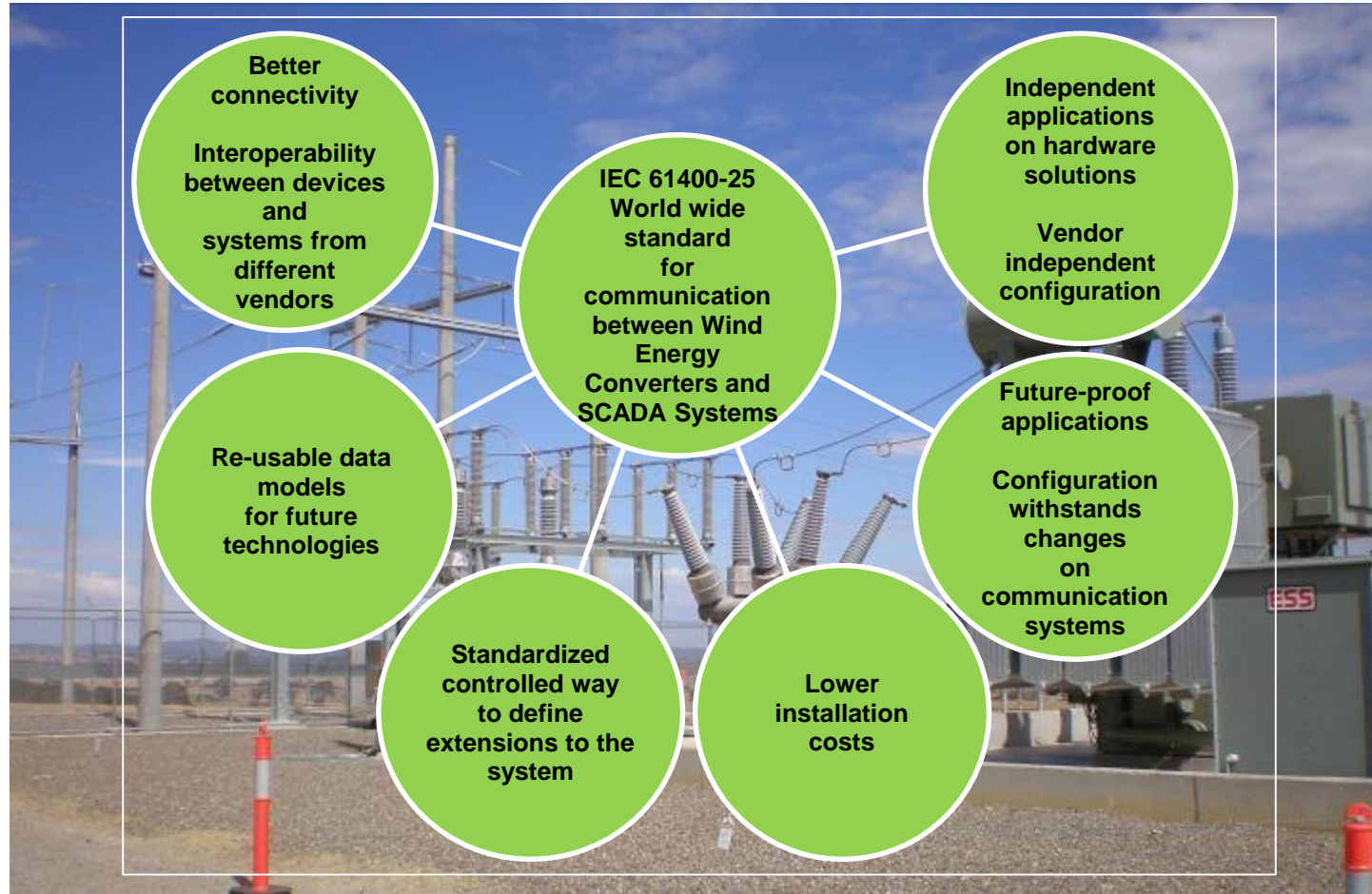
IEC 61400-25 builds on IEC 61850

IEC 61850

standard for the

design of

Electrical Substation Automation

**New title in Edition 2
Communication network and
Systems for power utility
automation**

IEC 61400-25

standard for

communications for monitoring and control

Wind Power Plants

Conceptual Model of the IEC 61400-25

The main focus is on communications between wind power plant components and SCADA systems

SCADA systems

Wind powerplant
Power unit
Meteorological

Communication model of the IEC 61400-25 series

Client

Information exchange model (get, set, report, log, control, publish / subscribe, etc.) defined in IEC 61400-25-3

Actor e.g. SCADA

Application

Wind power plant information model defined in IEC 61400-25-2

Outside scope

Messaging through mapping to communication profile (Read, write, ... message) defined in IEC 61400-25-4

Server

Information exchange model (get, set, report, log, control, publish / subscribe, etc.) defined in IEC 61400-25-3

Wind power plant component e.g. wind turbine

Application

Wind power plant information model (rotor speed, break status, total power production, etc.) defined in IEC 61400-25-2

Outside scope

IEC 2143/06

3 areas were defined:
- Information Model
- Information Exchange Model
- Mapping

Figure 1 – Conceptual communication model of the IEC 61400-25 series

Parts and release status of the standard

Standard	Description	Edition 1	Edition 2
61400-25-1	Overall description of principles and models	12.2006	10.2017
61400-25-2	Information models	12.2006	2015
61400-25-3	Information exchange models	12.2006	2015
61400-25-4	Mapping to communication profile	08.2008	04.2017
61400-25-5	Conformance testing	12.2006	09.2017
61400-25-6	Logical Node Classes and Data Classes for condition monitoring	11.2010	10.2017
61400-25-46	Mapping OPC-UA		03.2018 Excepted NWIP
61400-25-71	ICD-Files Proposal		10.2017 Technical draft

The stacks specified in this part of IEC 61400-25 comprise:

- SOAP-based web services,

- a mapping to OPC/XML-DA (to be replaced by OPC UA),

- a mapping to MMS (IEC 61850-8-1),

- a mapping to IEC 60870-5-104,

- a mapping to DNP3.

In order to be compliant with this part of IEC 61400-25, at least one mapping shall be selected.
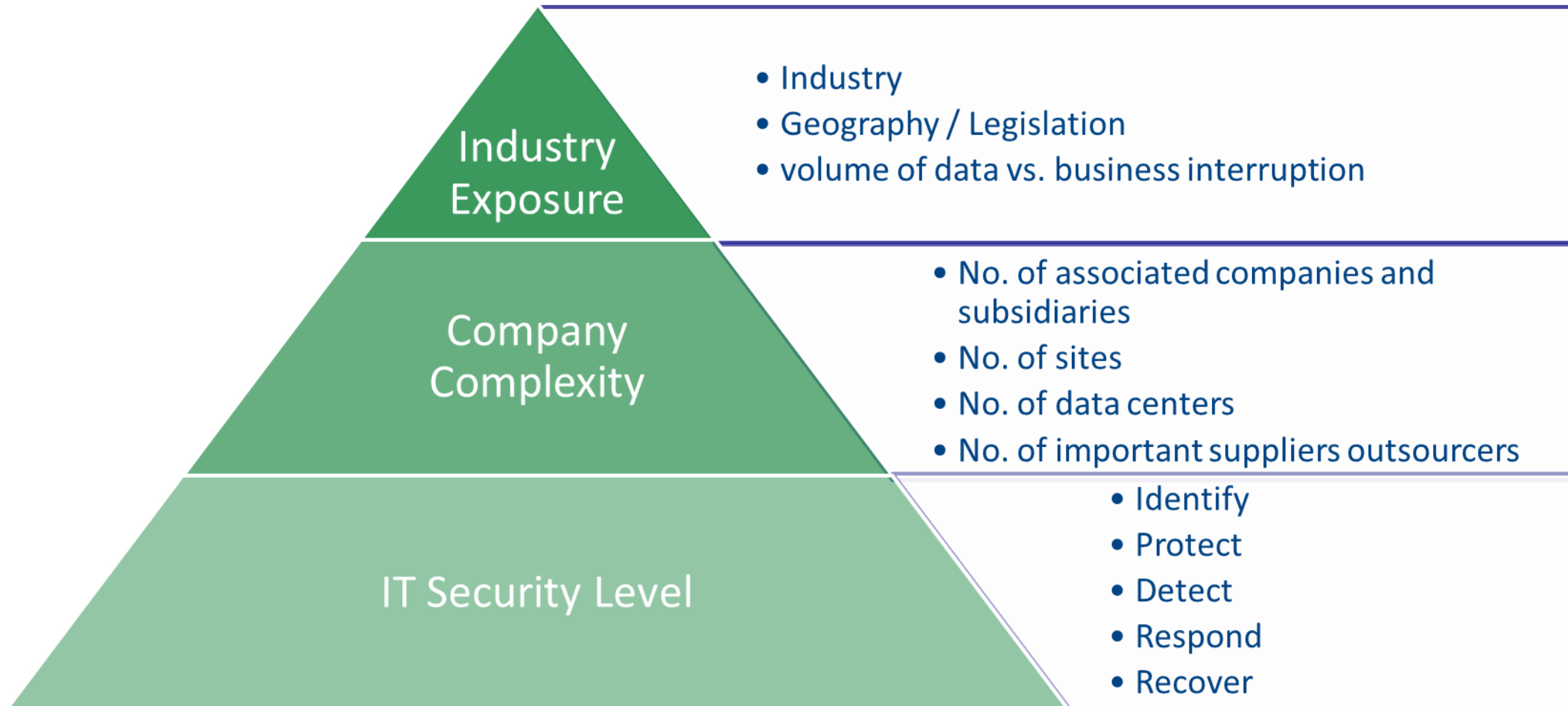
Table 1 – Mapping overview of IEC 61400-25-3 services

Mapping capability overview						
IEC 61400-25-3 Services	M/O	Web-services	OPC XML-DA	IEC 61850-8-1 (MMS)	IEC 60870-5-104	DNP3
Associate	M	Y	Y	Y	Y	Y
Release	O	Y	Y	Y	Y	N
Abort	O	Y	Y	Y	N	N
GetServerDirectory	O	Y	Y	Y	N	Y
GetLogicalDeviceDirectory	O	Y	Y	Y	N	Y
GetLogicalNodeDirectory	O	Y	Y	Y	N	N
GetDataValues	M	Y	Y	Y	Y	Y
SetDataValues	M	Y	Y	Y	Y	Y
GetDataDirectory	O	Y	Y	Y	N	N
GetDataDefinition	O	Y	Y	Y	N	N
GetDataSetValues	M	Y	P[a]	Y	N	Y
SetDataSetValues	O	Y	N	Y	N	Y
CreateDataSet	O	Y	N	Y	N	N
DeleteDataSet	O	Y	N	Y	N	N
GetDataSetDirectory	O	Y	N	Y	N	N
Report	O	Y	Y	Y	Y	N

Source: http://iec61850-news.blogspot.com/2009/08/webservices-for-iec-61850-or-iec-61850.html

Agenda

- **1**   Introduction of the standard IEC 61400-25

- **2**   Cyber Risk Assesment and complience to security standards

- **3**   Examples and challenges of Wind Power Plant communication in Europe

- **4**   Introduction of the IEC 61400-25 user group

Cyber Risk Assesment Comprehensive Approch

Industry Exposure
- Industry
- Geography / Legislation
- volume of data vs. business interruption

Company Complexity
- No. of associated companies and subsidiaries
- No. of sites
- No. of data centers
- No. of important suppliers outsourcers

IT Security Level
- Identify
- Protect
- Detect
- Respond
- Recover

IT Security Level Evaluation

Identify
- Governance & Compliance
- Responsibilities
- Risk Management
- Procurement
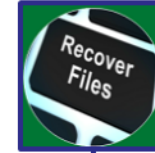- Working with external partners
- Recruitment

Protect
- User access control
- Awareness & Training
- Data Security
- Processes and Procedures
- Encryption
- Patch & change management

Detect
- Security Incident Event Monitoring (SIEM)
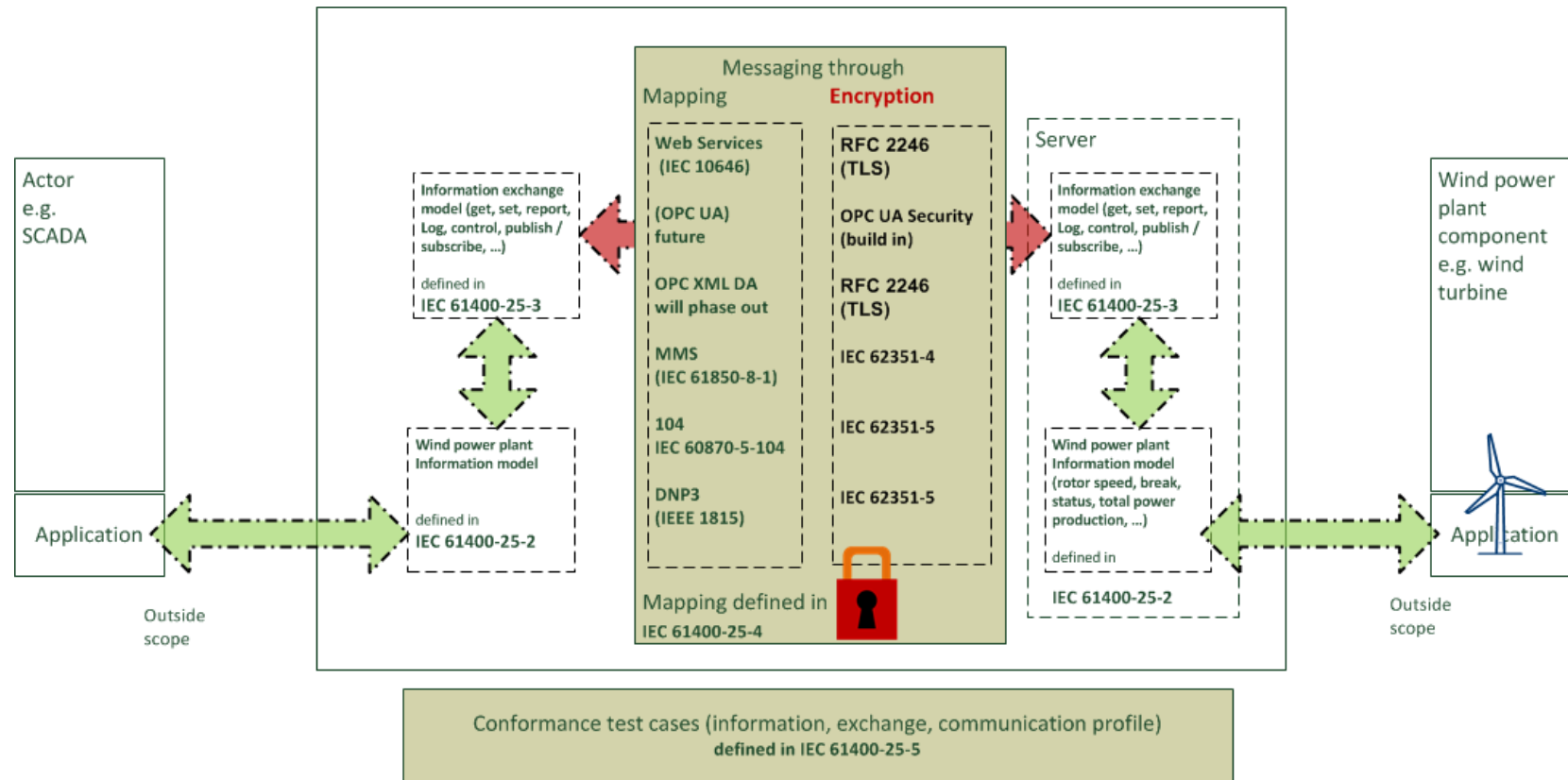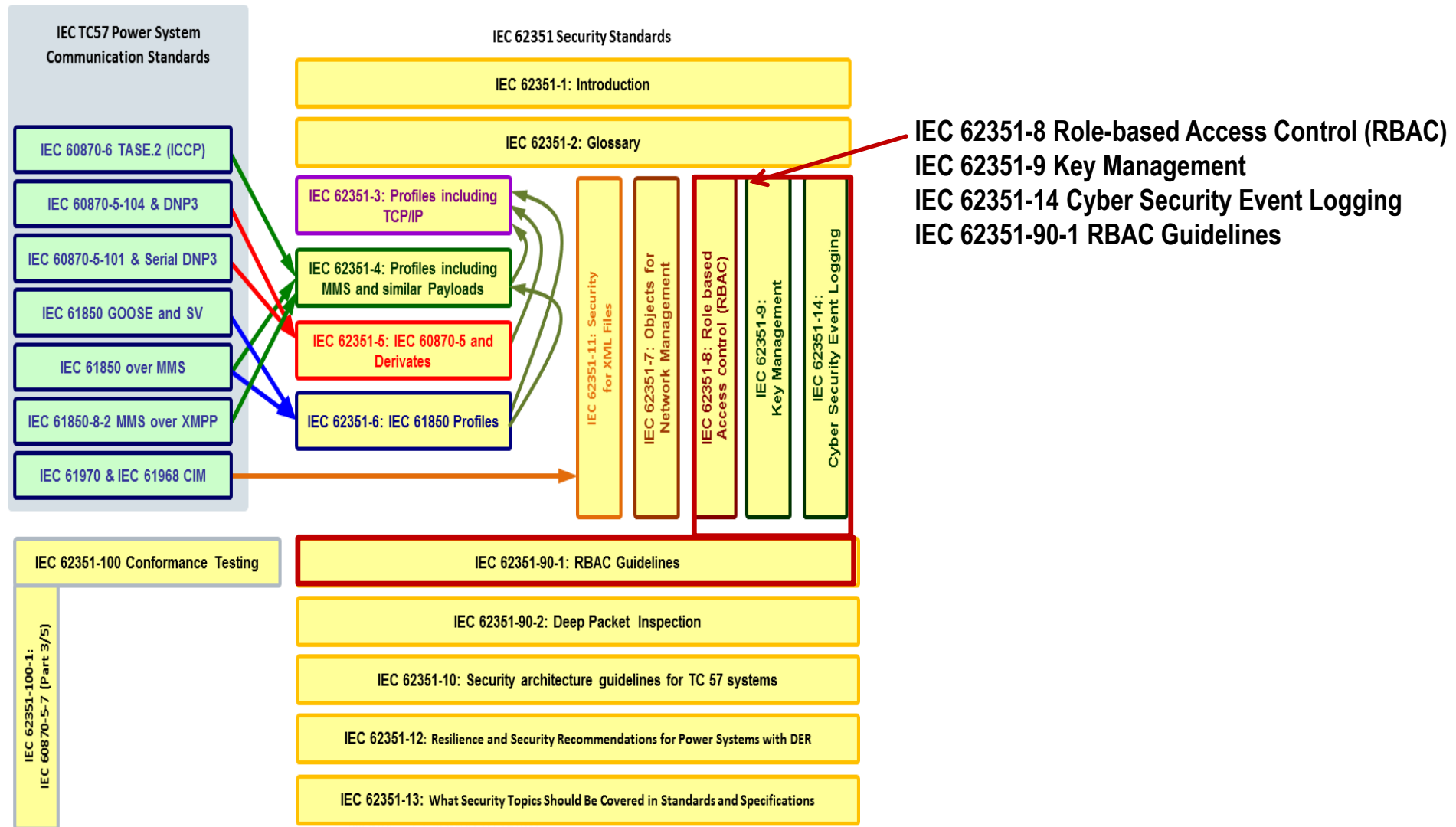- Malware protection

Respond & Recover
- Incident Management
- Emergency Management
- Backup
- Disaster Recovery
- Business Continuity Management

Combine IEC 61400-25 With IEC 62351

IEC TC57 Power System Communication Standards

- IEC 60870-6 TASE.2 (ICCP)
- IEC 60870-5-104 & DNP3
- IEC 60870-5-101 & Serial DNP3
- IEC 61850 GOOSE and SV
- IEC 61850 over MMS
- IEC 61850-8-2 MMS over XMPP
- IEC 61970 & IEC 61968 CIM

IEC 62351 Security Standards

- IEC 62351-1: Introduction
- IEC 62351-2: Glossary
- IEC 62351-3: Profiles including TCP/IP
- IEC 62351-4: Profiles including MMS and similar Payloads
- IEC 62351-5: IEC 60870-5 and Derivates
- IEC 62351-6: IEC 61850 Profiles
- IEC 62351-11: Security for XML Files
- IEC 62351-7: Objects for Network Management
- IEC 62351-8: Role based Access control (RBAC)
- IEC 62351-9: Key Management
- IEC 62351-14: Cyber Security Event Logging

IEC 62351-8 Role-based Access Control (RBAC)
IEC 62351-9 Key Management
IEC 62351-14 Cyber Security Event Logging
IEC 62351-90-1 RBAC Guidelines

- IEC 62351-100 Conformance Testing
- IEC 62351-100-1: IEC 60870-5-7 (Part 3/5)

- IEC 62351-90-1: RBAC Guidelines
- IEC 62351-90-2: Deep Packet Inspection
- IEC 62351-10: Security architecture guidelines for TC 57 systems
- IEC 62351-12: Resilience and Security Recommendations for Power Systems with DER
- IEC 62351-13: What Security Topics Should Be Covered in Standards and Specifications

Agenda

- **1**   Introduction of the standard IEC 61400-25

- **2**   Cyber Risk Assesment and complience to security standards

- **3**   Examples and challenges of Wind Power Plant communication in Europe

- **4**   Introduction of the IEC 61400-25 user group

31 x IEC 61400-25 (30 WEC + 1 Power Management Unit)

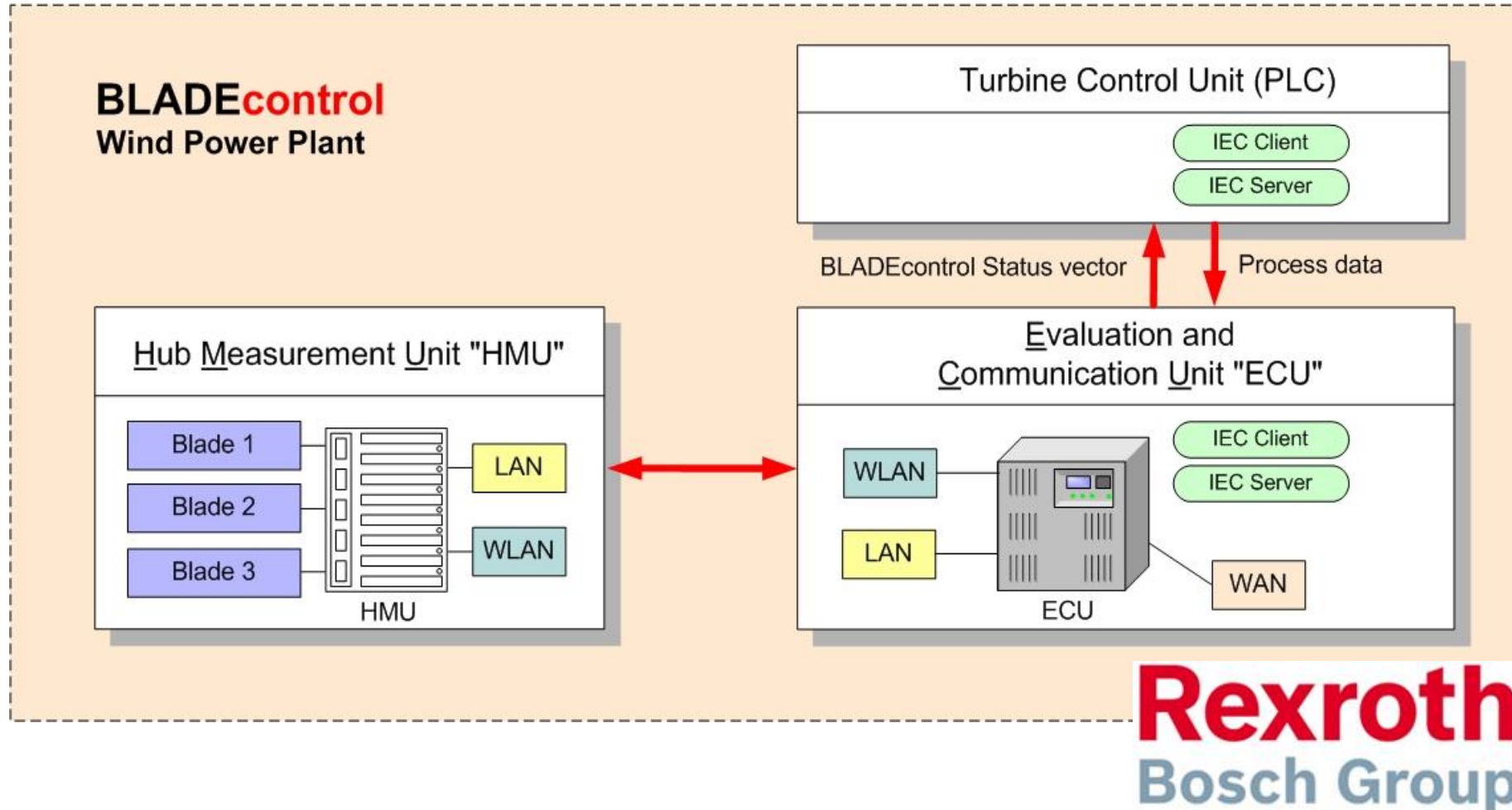|	
Customer :	Ormonde Energy Limited (subsidiary of Vattenfall)
Wind farm:	Ormonde offshore wind farm
Location:	Irish Sea, 35 kilometers off the northwest coast of England
Vendor:	Senvion SE
Total Capacity:	150 MW (30 turbines)
Turbine type:	Senvion 5M

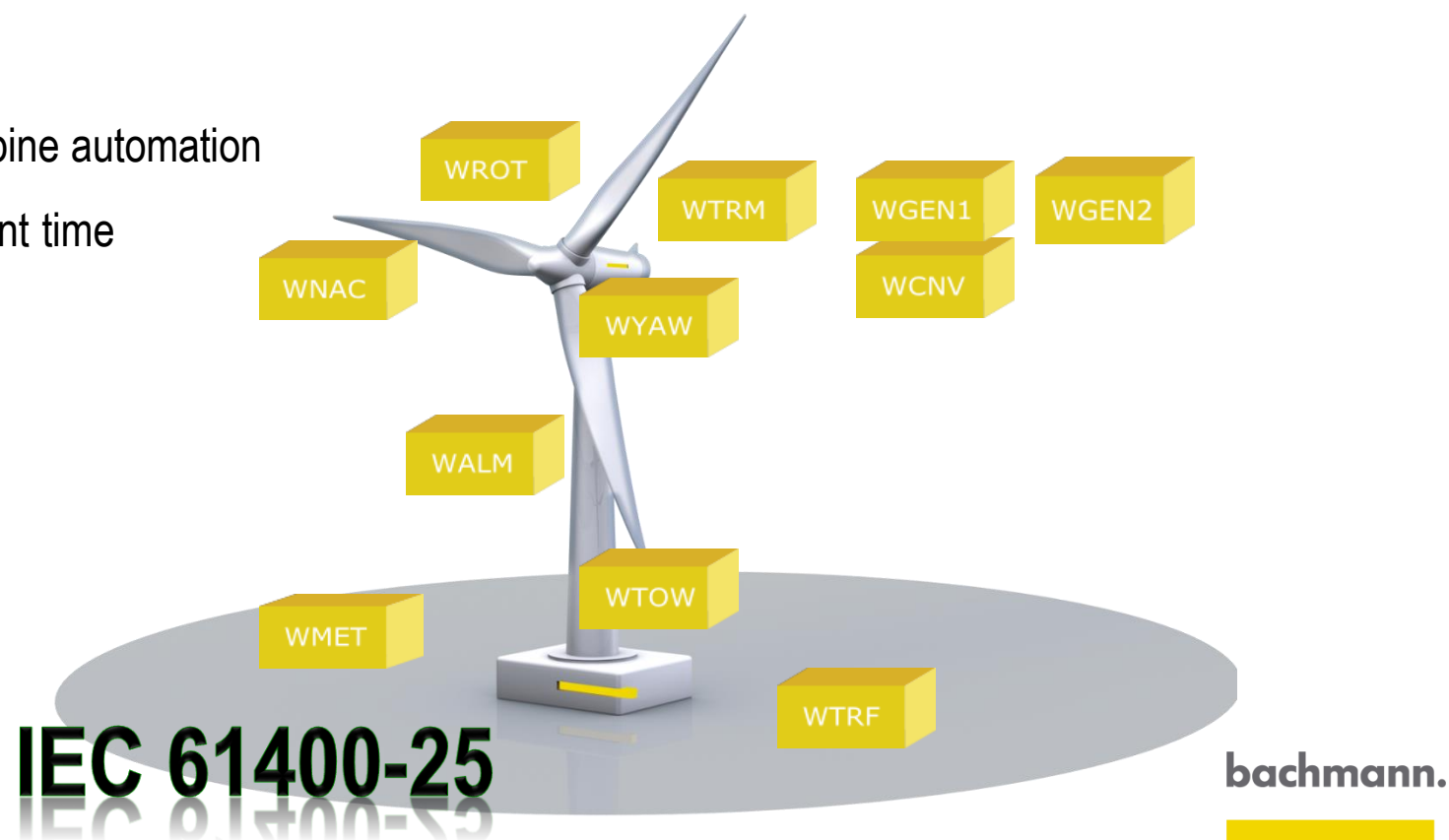USE61400-25 IEC 61400-25 user group   SENVION wind energy solutions   VATTENFALL   OSIsoft.   bachmann.
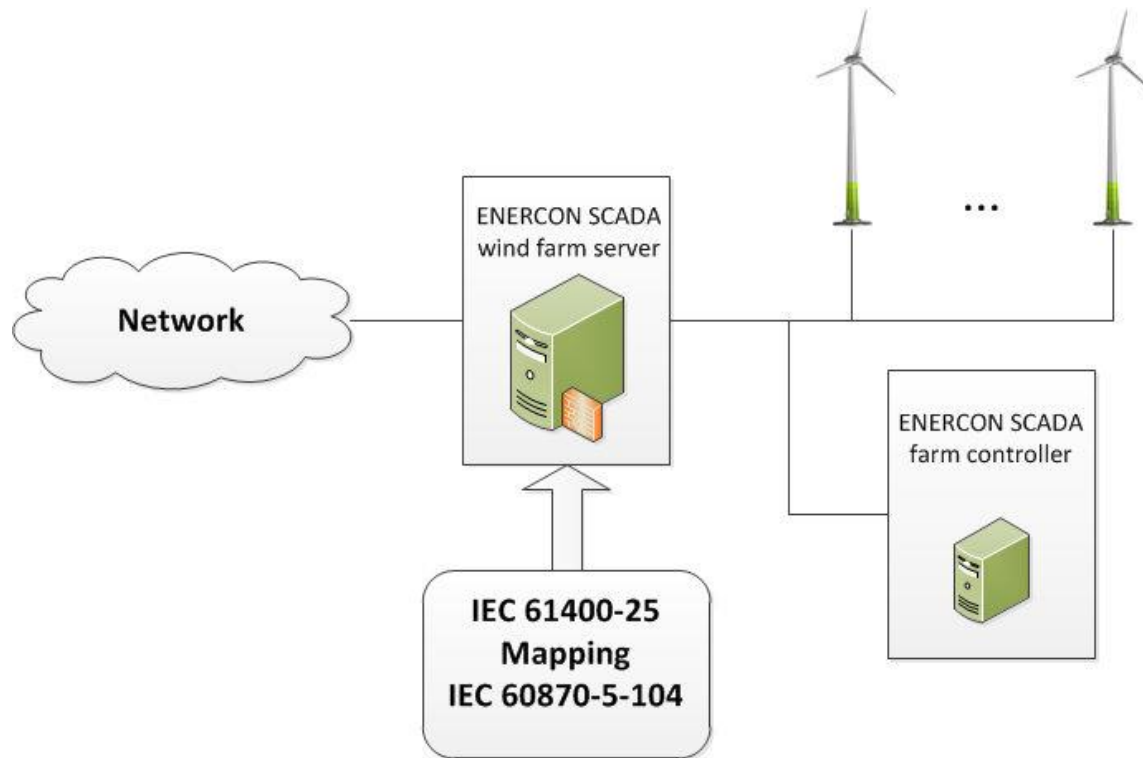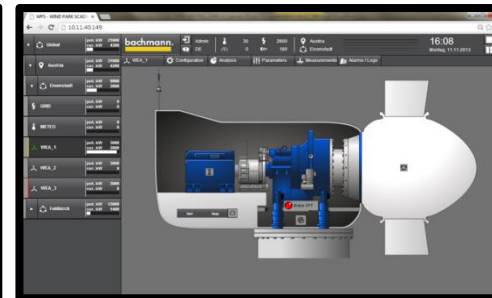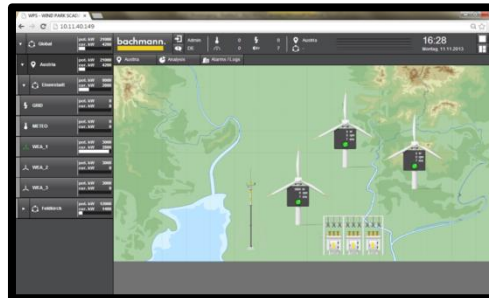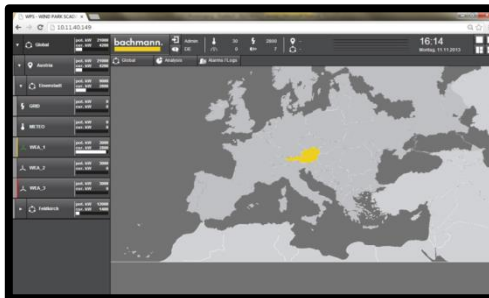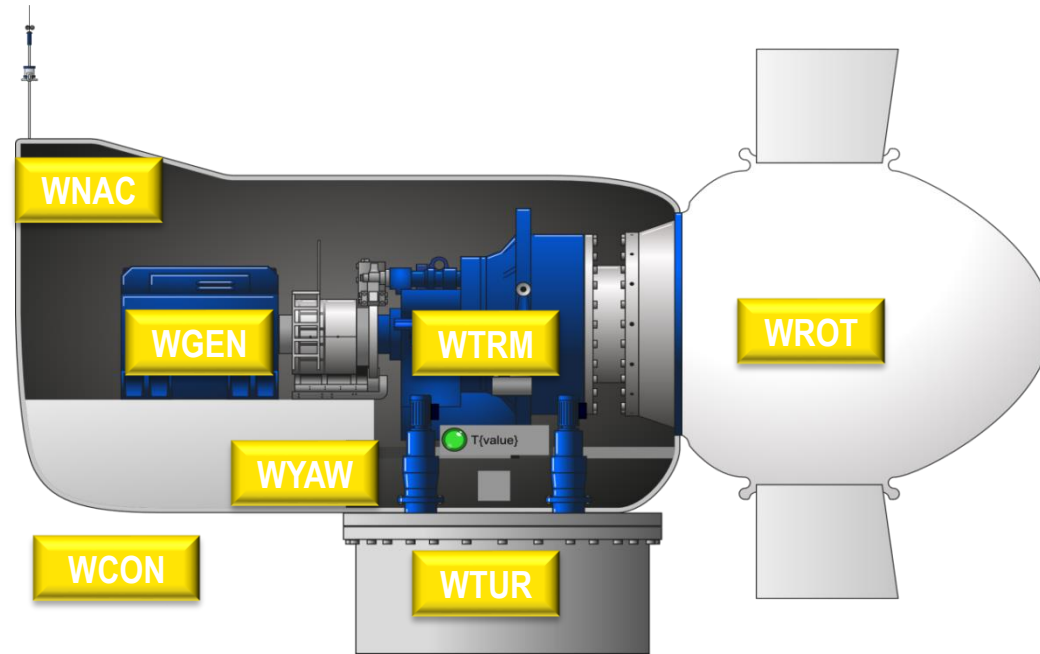
- Covers most standard use cases in wind turbine automation

- Time-to-market reduction by less development time

- Uses wind standard IEC 61400-25

- Interface to visualization / SCADA

WROT
WTRM   WGEN1   WGEN2
WNAC   WCNV
WYAW
WALM
WTOW
WMET
WTRF

IEC 61400-25

bachmann.

WTT – Integration – Wind Power SCADA (WPS)

USE61400-25
IEC 61400-25 user group

… just add your **WTT-prepared M1** …

… via **OPC-UA** …

… and your **SCADA**-System is ready !

WNAC
WGEN
WTRM
WROT
WYAW
WCON
WTUR

bachmann.

WTT – Software components and workflow

1. Configuration and mapping of M1 values with Solution Center WTT configurator (Plugin)
2. Code generation: automatically creates PLC Developer project with configured structures/variables
3. Configuration files for SCADA are also generated
4. Configure access control via SCADA or with Solution Center integrated plugin

Configuration	IEC Mapping/ IO Mapping		Operations	Access control / user management
• Events • Alarming • Brake level • Statistics	• **WTT_IO** – Averages – Counter (state/energy) – Availability – Parameter (range checked) – Data logging according to IEC61400-25: ✓ WGEN ✓ WCNV ✓ WROT ✓ etc. **Component libraries:** – Converter – Anemometer – Pitch	▪ Code generation ▪ Configuration file generation e.g. for SCADA	• **WTT_MAIN** – Turbine state machine: ✓ WGEN ✓ WCNV ✓ WROT ✓ etc. – Library functionality with API for own implementations – Template implementation / own source code, algorithms and know-how	• **WTT_ACC/ENC** - Extension of system user management - Adapted login checker module with changeable encryption checker - Encrypted login data - Active state handling - IP-based priority handling of locations

bachmann.

WTT – Software components

WTT_Sim

WTT_CTRL

WTE

WTT

WTE configuration

WTT_WTE

WTE-Libraries
(API)
Configurator
Events
Trends
Logging
Alarming
Security
Statistics
Averages

I/O control

C
C++

WTT_IO

I/O handling:
(according IEC61400-25)

Logical Nodes:
WGEN
WCNV
WROT
...
Component Libs:
-Converter
-Annemometer
-Pitch

Operation control

CoDeSys

WTT_Main

Turbine state machine:
(according IEC61400-25)

Logical Nodes:
WGEN
WCNV
WROT
...
- User library with pre-defined function handling
- Use template implementation or own

bachmann.

Agenda

- **1**   Introduction of the standard IEC 61400-25

- **2**   Cyber Risk Assesment and complience to security standards

- **3**   Examples and challenges of Wind Power Plant communication in Europe

- **4**   Introduction of the IEC 61400-25 user group

IEC 61400-25 user group members

Mission

The USE 61400-25 user group has the main aim to

- ease the use of IEC 61400-25 – Communications for monitoring and control of wind power plants

- support users implementing the standard within the wind power industry

- support the use of the IEC 61400-25 standard series

Vision

- Add value for the users of IEC 61400-25

- Share information of relevance for use of IEC 61400-25

- Share documents of relevance for use of IEC 61400-25

- Discussion forum for resolution of technical issues / data base

- Feedback to IEC 61400-25 standardization group

- Coordinate activities with related user groups and organizations

- Validate member devices spending the least effort, money and time

"This means efficient and with expected interoperability".

Objectives

- Presentation how to use the standard within workshops with specific companies and organizations

- Conference exhibitions

- Established Task Force to develop reference server for edition 2

- Open Source Client (MMS)
  (only for user group members)

- Implementation guideline for 61400-25

Implementation Guideline

- The USE61400-25 has developed a guideline

- The main goal of the implementation guideline is to assist users with implementing the 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

USE61400-25
IEC 61400-25 user group

- Reference server implementation

  - Development of a WPPS reference server
  - Validation of the WPPS with existing implementations
  - Deployment and publication of results
  - Maintenance and update
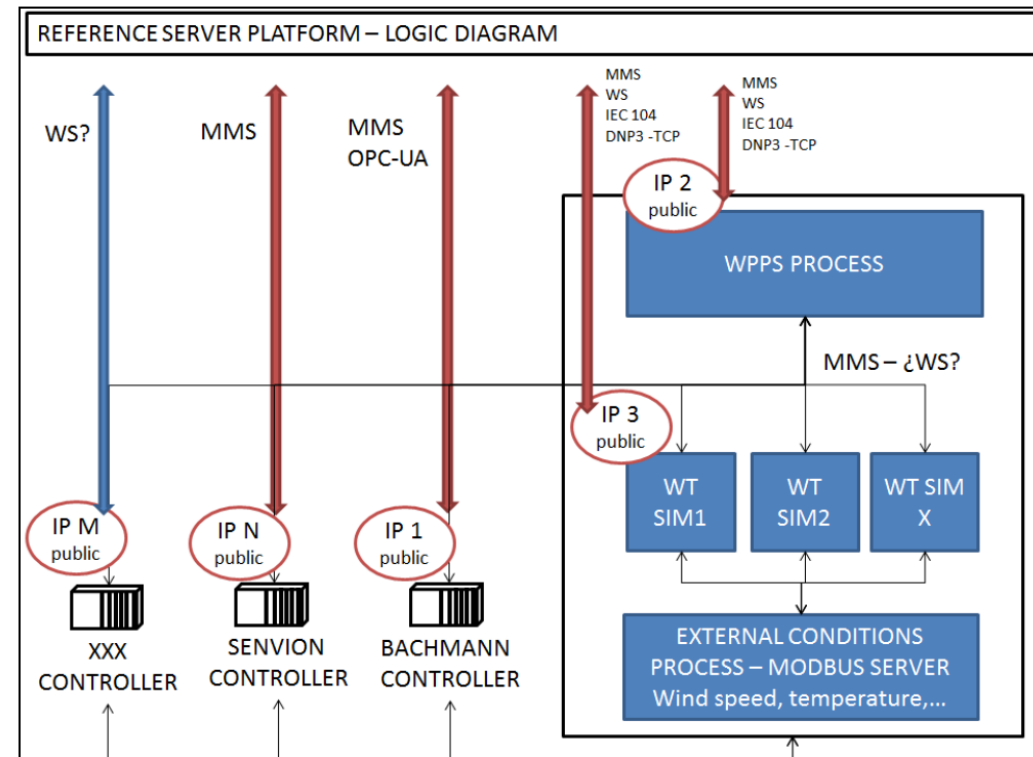
Thank you for your attention !

USE61400-25
IEC 61400-25 user group

Management Team

Bertram Lange (Chairman)
Hennig Harden (Technical Team Chairman)
Knud Johansen (Treasurer)
Maurizio Scavazzon (Validation, Interoperability, Cyber Security)
Michael Rueter (Standardization)

Please visit

www.new.use61400-25.com