Substation Automation
Future Trends Substation Automation and IEC 61850
Future Trends in IEC 61850
List of Content

- IEC 61850 Edition 2

- IEC 61850-9-2 process bus
  Advantages and experiences

- Cyber Security
  for Substation Automation
IEC 61850
Edition 2
IEC 61850 Edition 2
Scope mapped to system architecture

Legend:
- Published (Ed1)
- Published (Ed2)
- Ongoing

New Title: Communication networks and systems for power utility automation

Maintenance Center
Control Center
Substation

Hydro Power Plant
- IEC 61850-7-410
Wind Power Plant
- IEC 61850
- IEC 61400-25
 DER, PV, ...
- IEC 61850-7-420
Battery storage
- IEC 61850-90-7
- IEC 61850-7-420
Electr. vehicles
- IEC 61850-90-9
Distribution Automation
- IEC 61850-90-6

Legend:
- Published (Ed1)
- Published (Ed2)
- Ongoing

Network Engineering Guideline
- IEC 61850-1...-10
- IEC 61850-90-4

Condition Monitoring
- IEC 61850-90-2
Mapping to IEC 101/104
- IEC 61850-90-5
Synchrophasors
- IEC 61850-90-1
Between substations
- IEC 61850-90-4

© ABB Group
Month DD, Year | Slide 4
# IEC 61850 Edition 2
## Overview of new main features

<table>
<thead>
<tr>
<th>Feature</th>
<th>Benefit</th>
<th>Impact</th>
<th>m/o</th>
</tr>
</thead>
<tbody>
<tr>
<td>Correction of errors and many small details</td>
<td>Ensure interoperability</td>
<td>Mainly on tools</td>
<td>M</td>
</tr>
<tr>
<td>Data model extension</td>
<td>Modeling for hydro, wind, DER and power quality</td>
<td>IEDs (servers and clients)</td>
<td>O</td>
</tr>
<tr>
<td>Longer LD names / prefixes</td>
<td>Object names extended from 64 to 128 characters</td>
<td>IEDs, Tools (IED and system)</td>
<td>M</td>
</tr>
<tr>
<td>SCL extension</td>
<td>Allow bottom-up system design and multiple projects</td>
<td>Tools (IED and system)</td>
<td>O</td>
</tr>
<tr>
<td>SCL implementation conformance statement SICS</td>
<td>Clarity on tool capability</td>
<td>Tools (IED and system)</td>
<td>M</td>
</tr>
<tr>
<td>Parameter and configuration Data revision and value change</td>
<td>Better version handling and reporting</td>
<td>IEDs (servers)</td>
<td>O</td>
</tr>
<tr>
<td>Defined named enumerations distinct from countable integers</td>
<td>Easier understandable, no interpretation needed</td>
<td>Clients, Tools (IED and system)</td>
<td>M</td>
</tr>
<tr>
<td>Link redundancy</td>
<td>Higher availability and interoperable solutions</td>
<td>IEDs (servers and clients)</td>
<td>O</td>
</tr>
<tr>
<td>Mechanisms for testing, simulation, maintenance</td>
<td>Support for efficient and automatic ‘in system’ testing</td>
<td>IEDs</td>
<td>O</td>
</tr>
</tbody>
</table>
IEC 61850 Edition 2 – New feature
Data model extension

- Logical nodes
  - Edition 1: Approx. 90
  - Edition 2: More than 150

- New LN groups
  - **F Group**: FCNT: Counter, FPID: PID regulator, FSPT: Set-point control function, …
  - **K Group**: KFAN: Fan, KFIL: Filter, KPMP: Pump, …
  - **Q Group**: QVVR: Voltage Variation, QFVR: Frequency Variation, QVTR Voltage Transient, …

- Other new LN:
  - LTRK: Service tracking, …

<table>
<thead>
<tr>
<th>Group Indicator</th>
<th>Logical Nodes Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>Automatic control</td>
</tr>
<tr>
<td>C</td>
<td>Control</td>
</tr>
<tr>
<td>D</td>
<td>Distributed Energy Resources (DER)</td>
</tr>
<tr>
<td>F</td>
<td>Functional Blocks</td>
</tr>
<tr>
<td>G</td>
<td>Generic</td>
</tr>
<tr>
<td>H</td>
<td>Hydro</td>
</tr>
<tr>
<td>I</td>
<td>Interfacing and archiving</td>
</tr>
<tr>
<td>K</td>
<td>Mechanical and non-electrical primary equipment</td>
</tr>
<tr>
<td>L</td>
<td>System LN</td>
</tr>
<tr>
<td>M</td>
<td>Metering and measurement</td>
</tr>
<tr>
<td>P</td>
<td>Protection</td>
</tr>
<tr>
<td>Q</td>
<td>PQ events detection related</td>
</tr>
<tr>
<td>R</td>
<td>Protection related</td>
</tr>
<tr>
<td>S</td>
<td>Sensor and monitoring</td>
</tr>
<tr>
<td>T</td>
<td>Instrument transformers</td>
</tr>
<tr>
<td>X</td>
<td>Switchgear</td>
</tr>
<tr>
<td>Y</td>
<td>Power transformers</td>
</tr>
<tr>
<td>Z</td>
<td>Further power system equipment</td>
</tr>
</tbody>
</table>
IEC 61850 Edition 2 – New feature
SCL Extension

- SCL extensions
  - IID: Instantiated IED Description – Describes the instantiated data model of an IED
  - SED: System Exchange Description – Describes interface data exchange between different projects
- More flexible System engineering
  - Top Down (already supported in Ed1)
  - Bottom up
  - Use of IID file for modifications
  - Multiple projects
  - Substation to substation
IEC 61850 Edition 2 – New feature
SCL implementation conformance statement (SICS)

- SCL implementation conformance statement (SICS)
  - IED configurator conformance statements
  - System configurator conformance statements
  - Stating mandatory and optional features of IED tools and system tools

- Improved interoperability
  - Allows judging the degree of interoperability between different engineering tools, system tools as well as IED tools.

<table>
<thead>
<tr>
<th>PICS</th>
<th>Protocol Implementation Conformance Statement: Which Communication services are supported ...</th>
</tr>
</thead>
<tbody>
<tr>
<td>PIXIT</td>
<td>Protocol Implementation Conformance Extra Information for Testing: Restrictions and Limitations found in a device ...</td>
</tr>
<tr>
<td>MICS</td>
<td>Model Implementation Conformance Statement: Models supported ...</td>
</tr>
<tr>
<td>TICS</td>
<td>Tissue Implementation Conformance Statement: Which tissues have been implemented: <a href="http://www.tissue.iec61850.com">www.tissue.iec61850.com</a></td>
</tr>
<tr>
<td>SICS</td>
<td>SCL Implementation Conformance Statement: Which aspects of SCL have been implemented in a Tool</td>
</tr>
</tbody>
</table>
IEC 61850 Edition 2 – New feature
Link Redundancy

- Redundancy within the network
  - **RSTP**, IEEE 802.1D
  - (n-1) criteria
  - With recovery time upon failure

- Redundancy in the end nodes
  - **PRP**, IEC 62439-3
    Parallel Redundancy Protocol
  - **HSR**, IEC 62439-3
    High-available Seamless Redundancy
  - (n-1) criteria
  - Zero recovery time upon failure
**Operation principle**

- **DANP (Double Attached Node implementing PRP)** are attached to 2 independent LANs
- Source DANP sends same frame over both LANs
- Destination DANP receives frame from both LANs, consumes 1st frame, discards the duplicated
Link Redundancy – IEC 62439-3 HSR
High-availability Seamless Redundancy

- **Operation principle**
  - DANH (Double Attached Node implementing HSR) has 2 ports operated in parallel
  - Source DANH sends a frame over each port (“A”-frame and “B”-frame)
  - Destination DANH receives frame from each port, consumes 1st frame, discards the duplicated
  - DANH support bridge functionality and forward frames from one port to the other (not frames that it injected)
Link Redundancy
System configuration with PRP according IEC 61850

- ABB is committed to **interoperable** solutions based on IEC 62439

- Station level
  - MicroSCADA Pro SYS600
  - MicroSCADA Pro SYS600C

- Bay level IEDs
  - Relion 670 series
  - REB500

- 670 series
- REB500
- Single Port devices
- SNTP Time Master
IEC 61850 Edition 2 – New feature
Communication between substations

- Data model and SCL extensions for communication between substations
- Technical Guideline for two possible solutions
  - Direct tunneling of Ethernet
    - IEDs on both side need to support IEC 61850
  - Proxy gateways
    - Low-bandwidth
    - Allows mixed operation of command types
NSD570 Rel. 3.3 / GOOSE LAN Interface G3LS
Proxy gateway solution – mixed operation

- Max. 4 commands via analog channels, max 8 commands via all others
- Commands arranged in pairs of two, e.g. 2x contact I/O and 6x GOOSE
- PLC
- Power Line
- MUX
- Radio Link
- Optical Fibre
- Copper Wires
- Ethernet
- IP based network
- Stationbus according IEC 61850-8-1
- Protection Commands of Contact I/O Type
- Protection Commands in GOOSE messages
- Proxy gateway solution – mixed operation
IEC 61850 Edition 2 – New feature
Mechanisms for testing, simulation, maintenance

- New data objects and concepts for testing
  - Testing of function parts in the running system
  - Allows a standardized application of the test and test-blocked mode

- Enables more efficient testing and maintenance
IEC 61850-9-2 process bus
Advantages and experiences
IEC 61850-9-2 process bus
List of Content

- Advantages of NCITs and IEC 61850 process bus
- Loganlea secondary system upgrade, ABB’s first IEC 61850-9-2 process bus installation
  - Customer and customer requirements
  - ABB’s solution
  - Site pictures
- Conclusion
Introduction to process bus IEC 61850-9-2

Process bus system for sampled values

- The station bus connects IEDs and substation automation system
- It transmits information between the station level and the bay level as well as between IEDs (GOOSE)
- The process bus connects the process to the bay level
- Sampled analog values are transferred via Ethernet according IEC 61850-9-2
- The optical communication network reduces cabling and isolates the P&C system from the process

Station level

IEC 61850 station bus

Bay level

IEC 61850-9-2 process bus

Process level

MU = merging unit
NCIT = non-conventional instrument transformer
Advantages over conventional technology
Non-conventional instrument transformers

Increased operational safety
- Total absence of oil, NCITs can not explode
- No iron core, therefore no ferroresonance

Lower environmental impact
- No oil and reduced volume of SF$_6$
- Lower power consumption

Reduced life-cycle costs
- Permanent and comprehensive system supervision supports efficient maintenance
- Software-configurable nominal values

High accuracy for protection and metering
- A single device for protection and metering applications

Simplified project execution
- No CT calculations
- Simplified switchgear design because of standardized device dimensions
- VT does not need to be disconnected during HV testing

Less space required
- Reducing switchgear footprint
Advantages over conventional technology

Process bus

Increased operational safety

- Handling of CT and VT circuits is obsolete
- Galvanic Isolation from process

Reduced life cycle costs

- Permanent real-time system supervision increases system availability by increasing maintenance cycles and reducing outage times
- Computer based tools enable simple measurement, e.g., without the need to short circuit and disconnect CT terminals

Reduced copper cabling

- By replacing parallel copper wires with optical process bus

Simpler system design

- Signal distribution is virtually independent of cable length
- CT burden is independent from connected devices

Future-proof interoperable design

- By applying the established IEC 61850 standard
Introduction to customer and project
Loganlea secondary system upgrade

- Powerlink performed a cost-benefit analysis comparing a solution deploying the new IEC 61850-9-2 solution and their standard conventional solution
- The first substation, Loganlea, is located between Brisbane and the Gold Coast
- With the Loganlea secondary system upgrade, ABB undertook its first commercial IEC 61850-9-2 process bus installation with NCITs and protection and control IEDs
- The upgrade was completed in December 2011
Customer requirements

- Replacement of the existing SA system with proprietary communication on process and station level with a new **fully IEC 61850 compliant system**
  - IEC 61850 station bus
  - IEC 61850-9-2LE process bus system
- Two **fully redundant** and independent protection systems
- Application of **standard products** that are part of the active product portfolio
- **Step-wise substation retrofit** with only minimal service interruption
ABB’s solution overview

- ABB’s SAS600 series substation automation system featuring MicroSCADA Pro as station HMI, and two RTU560 as gateways to the network control center.
- Protection and control IEDs from ABB’s Relion family 670 series, as well as the REB500 busbar protection system:
  - Supporting IEC 61850-9-2LE
  - Fully IEC 61850 compliant
- Upgrade of the NCITs with new secondary converters (sensor electronics) to interface with ABB’s conformance-certified IEC 61850-9-2LE merging unit CP-MUP.
ABB’s solution
IEC 61850 compliant SA system
ABB’s solution
670 series protection and control IEDs

- 670 series high-end protection and control IEDs with IEC 61850-9-2LE:
  - Bay control IED  REC670
  - Line distance protection  REL670
  - Line differential  RED670
  - Transformer protection  RET670

- All IEDs can have a 1PPS input for synchronized sampling

- All devices support mixed mode with conventional CT and VT interfaces eg, transformer low-voltage side for transformer differential protection

- Line differential protection runs with conventional and 9-2 remote-end substations

© ABB Group
ABB’s solution
REB500 busbar and breaker failure protection

- REB500 decentralized busbar protection system is fully compliant with IEC 61850-9-2LE
  - Busbar protection
  - Breaker failure protection
  - End-fault protection

- Seamless combination of bay units with IEC 61850-9-2LE and conventional bay units in one system
  - This allows flexible extension of conventional substations
ABB’s solution
Process bus overview

- simplified view of one of the two fully redundant protection systems
ABB’s solution
Highly available process bus, without Ethernet switches

- Highest availability of the process bus system was achieved by:
  - Building two fully independent process bus and protection systems from NCIT to protection IEDs
  - Minimizing number of components without using Ethernet switches
  - Refraining from common devices across feeders and the redundant protection system

Extract of the applied concept:

Control and redundant line and busbar/breaker failure protection
ABB’s solution
Complete system supervision

- Permanent system supervision of all intelligent electronic devices. From Communication gateways to NCIT electronics
- Supervision diagrams for fast overview of the substation health
  - System overview with all substation automation, protection and control equipment as well as merging units
  - Process bus overview with more detailed information about merging units and NCITs
Site pictures
IEC 61850-9-2 process bus

Conclusion

- ABB’s IEC 68150 compliant process bus systems for analog values are now available
- ABB’s installed base of pilot and real systems is continuously increasing
- ABB is committed to standard conform implementation and actively supports the developments and evolution of international standards
- Development to integrate more non-conventional instrument transformers as well as binary signals are on-going

➢ A promising technology is taking off
Cyber Security for Substation Automation
Cyber Security for Substation Automation
Why is Cyber Security an issue?

Cyber security has become an issue by introducing Ethernet (TCP/IP) based communication protocols to industrial automation and control systems. e.g. IEC60870-5-104, DNP 3.0 via TCP/IP or IEC61850

Connections to and from external networks (e.g. office intranet) to industrial automation and control systems have opened systems and can be misused for cyber attacks.

Cyber attacks on industrial automation and control systems are real and increasing, leading to large financial losses.

Utilities need to avoid liability due to non-compliance with regulatory directives or industry best practices;
Cyber Security for Substation Automation
Customer concerns and ABB solutions

- Protect
  Is my system protected against an attack?

- Manage
  Can I sustain the security of my system?

- Security Organisation

- Product and System Hardening

- Monitor
  Do I know what happens on my system?
ABB’s cyber security initiatives
Security organization & involvement

- **Customer Needs**
  - Same high level of security for all products & solutions
  - Fast response and reliable partner in case of a cyber security issue

- **ABB’s Solution**
  - Since many years ABB has a global, cross-functional cyber security organization
  - Security is well established in all process areas
    - Security assessment and robustness testing
    - Patch management process
    - Actively working in security standard committees
ABB’s cyber security initiatives
Product and System Hardening

- Customer Needs
  - Robust and reliable products and solutions

- ABB’s Solution
  - Centralized security testing center guarantees a common and best practice robustness testing of all products
  - Regular regression tests on ABB products and systems ensure a high level of robustness against cyber security attacks
Monitor

Do I know what happens on my system?

- **Customer Needs**
  - Alert about critical security alarms in real-time to enable fast corrective actions

- **ABB’s Solution**
  - Logging & Alarming: All security related events are recorded, sever events are sent as an alarm to the remote center
  - Reporting & Auditing: Produce necessary data, reports and documentation for an audit
Monitor
Security events logging / Audit trail

- RTU560 Features
  - Event logs are stored secured
  - Security event logs can be displayed via the device tools
  - Send security events to external security log clients using syslog
  - Security events can be sent via host protocol to remote control centers

**Archive Information - Security Events**

<table>
<thead>
<tr>
<th>Seq. No.</th>
<th>Date</th>
<th>Time</th>
<th>Event Type</th>
<th>Event Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>912</td>
<td>04.03.30</td>
<td>14:35:56</td>
<td>Event Security</td>
<td>Download configuration files succ</td>
</tr>
<tr>
<td>913</td>
<td>04.03.30</td>
<td>14:35:24</td>
<td>Event Security</td>
<td>User logged out</td>
</tr>
<tr>
<td>914</td>
<td>04.03.30</td>
<td>14:36:36</td>
<td>Event Security</td>
<td>User log in successful</td>
</tr>
<tr>
<td>915</td>
<td>04.03.30</td>
<td>14:36:43</td>
<td>Event Security</td>
<td>Test mode started (control allow)</td>
</tr>
<tr>
<td>916</td>
<td>04.03.30</td>
<td>14:36:51</td>
<td>Event Security</td>
<td>User logged out</td>
</tr>
<tr>
<td>917</td>
<td>04.03.30</td>
<td>14:36:55</td>
<td>Event Security</td>
<td>User logged out</td>
</tr>
<tr>
<td>918</td>
<td>04.03.30</td>
<td>14:37:01</td>
<td>Event Security</td>
<td>User logged out</td>
</tr>
<tr>
<td>919</td>
<td>04.03.30</td>
<td>14:37:01</td>
<td>Event Security</td>
<td>User logged out</td>
</tr>
<tr>
<td>920</td>
<td>04.03.30</td>
<td>14:37:11</td>
<td>Event Security</td>
<td>User logged out</td>
</tr>
<tr>
<td>921</td>
<td>04.03.30</td>
<td>14:37:30</td>
<td>Event Security</td>
<td>User logged out</td>
</tr>
<tr>
<td>922</td>
<td>04.03.30</td>
<td>14:38:11</td>
<td>Event Security</td>
<td>User logged out</td>
</tr>
<tr>
<td>923</td>
<td>04.03.30</td>
<td>14:38:15</td>
<td>Event Security</td>
<td>User logged out</td>
</tr>
<tr>
<td>924</td>
<td>04.03.30</td>
<td>14:39:54</td>
<td>Event Security</td>
<td>User logged out</td>
</tr>
<tr>
<td>925</td>
<td>04.03.30</td>
<td>14:39:57</td>
<td>Event Security</td>
<td>User logged out</td>
</tr>
<tr>
<td>926</td>
<td>04.03.30</td>
<td>14:39:59</td>
<td>Event Security</td>
<td>User logged out</td>
</tr>
<tr>
<td>927</td>
<td>04.03.30</td>
<td>14:40:01</td>
<td>Event Security</td>
<td>User logged out</td>
</tr>
<tr>
<td>928</td>
<td>04.03.30</td>
<td>14:40:03</td>
<td>Event Security</td>
<td>User logged out</td>
</tr>
<tr>
<td>929</td>
<td>04.03.30</td>
<td>14:40:04</td>
<td>Event Security</td>
<td>User logged out</td>
</tr>
<tr>
<td>930</td>
<td>04.03.30</td>
<td>14:40:05</td>
<td>Event Security</td>
<td>User logged out</td>
</tr>
<tr>
<td>931</td>
<td>04.03.30</td>
<td>14:40:07</td>
<td>Event Security</td>
<td>User logged out</td>
</tr>
<tr>
<td>932</td>
<td>04.03.30</td>
<td>14:40:21</td>
<td>Event Security</td>
<td>User logged out</td>
</tr>
</tbody>
</table>

© ABB Group
5 October 2012 | Slide 38
Protect
Is my system protected against attacks?

- Customer Needs
  - Ensure reliable system operation (availability and performance)

- ABB’s Solution
  - Malware Protection: Prevent, detect, and remove malware, e.g. viruses, worm, …
  - Perimeter Protection: Restrict access by blocking / filtering inbound and outbound connections
  - Secure Communication: Encryption to prevent unauthorized users from reading and manipulating data
Protect
Secure communication via VPN

- **AFF650 VPN Features**
  - Secure tunneling of private communication through an insecure network (e.g. the Internet).
  - Function of VPNs:
    - Authentication
    - Encryption
  - Applications: Connecting geographically distributed participants
    - Connection of RTU in substation to control center (through public or private network)
    - Connection of remote offices to headoffice.
Manage
I can sustainably ensure the security of my system?

- Customer Needs
  - Keep the security of the system up to date
- ABB’s Solution
  - Patch Management: Reduce risk of vulnerability for windows based system components
  - Backup & Restoration: Ensures complete data security and enables fast restoration in case of data loss /manipulation
  - Accounts & Authentication: Restrict access to indented users only, protected by high password complexity
Manage
User management, strong passwords

- Features
  - Enforced password complexity (min. password length, upper/lower case, number, non-alphanumerical)
  - Encrypted password storage
  - Administration of user accounts (Add new users with initial password, change passwords, delete users, assign and change user roles and permission for each role)
  - Applies to all ABB station level devices
SAS 600 Series
Standard Security Architecture
SAS 600 Series
Enhanced Security Architecture

Legend:
- Disabled ports / services
- Removable media access
- Individual User Accounts
- Malware protection
- Firewall
- Router
- Encrypted communication

Maintenance Center (Security Zone 4)

Workstation
Antivirus

Security Zone 2
MicroSCADA Pro SYS600
Antivirus

Remote Control Center
(Security Zone 3)

Firewall / Router / VPN

Station LAN

Encrypted communication

Control and Protection IED

Security Zone 1

IEC61850 Station Bus

Parimeter Protection

© ABB Group
5 October 2012 | Slide 44
SAS 600 Series
Advanced Security Architecture

Legend:
- Disabled ports / services
- Removable media access
- Individual User Accounts
- Malware protection
- Firewall
- Router
- Encrypted communication
- Industrial Defender Agent
ABB’s cyber security activities
Summary

- Cyber security from ABB
  - is embedded in substation automation products and solutions
  - is an integral part of product development and quality assurance
  - comprises the latest technology and high competence
  - enables customers to protect, monitor and manage their systems
  - safeguards substations in a changing world