Trends for Smart Grid Automation and Industry 4.0 Integration

presented by Detlef Raddatz
Managing Director SystemCORP Embedded Technology
Agenda

• Introduction
• Short History of Utility Communication
• Utility Communication Today
• Transition to Smart Grid Technology
• Future Smart Grid Communication
• Cyber Security Requirements
• Q & A
In early days around 1890 electrical systems were isolated grids limited to small geographical areas.

- Local power generation
- Local limited transmission capabilities
- Local power distribution

Proof of Concept – AC generation proofs superior to DC systems - Tesla versus Edison

- Introduction of the single phase power grid system @133.33 Hz
- Transmission line totaled a length of 4000 feet -> 1220 meters
- Distribution system comprised of 1 transformer powering 7 offices, 2 hotels and 13 stores on main street.
Short History...

This is what happened!!

25 HP (18 kW) Power Generator

Transmission Line

Distribution System

500/100 Volt ac Substation

Protection ???
None – only by operator!!

Communication ???
Yes !!! 1 Bike/Minute

This is what happened!!
**Internationally Linked Utility Systems**

**National Utility Systems**

**Regional Utility Systems**

**Short History…**

- **Introduction of SCADA**
  - Electromechanical logic and analog telephone system
  - Introduction of analog data communication
  - Electromechanical logic and analog signaling

- **Supervisory Control and Data Acquisition**
  - Digital controllers and introduction of propriety communication protocols
  - Standardization of utility communication in the USA and Europe – the rest of the world followed

- **Geographical Distribution**
  - Local Utility Systems
  - Regional Utility Systems
  - Internationally Linked Utility Systems

- **1925**
  - Introduction of SCADA

- **1940**
  - Electromechanical logic and analog signaling

- **1950 … 1960**
  - Local controllers and introduction of analog data communication

- **1980**
  - Digital controllers and introduction of propriety communication protocols

- **1990 … 2010**
  - Standardization of utility communication in the USA and Europe – the rest of the world followed

- **2015 …**
  - Merging utility communication with IoT, Cloud Services and Industry 4.0
Utility Communication Today

Top to Bottom Hierarchy

Structure has historically grown in a regulated energy market with public utilities
Consumer does not participate in the electricity market
Does not allow the integration of decentralized energy resources (DER)
Favors electricity supplier monopoly
### Utility Communication Today...

#### Communication Protocols used in the electrical utility industry

<table>
<thead>
<tr>
<th>IEC/IEEE and other Standards</th>
<th>Client/Master Deployment</th>
<th>Server/Slave Deployment</th>
<th>Communication Medium</th>
<th>Distribution</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>IEC 60870-5-104</strong></td>
<td>Control centre and grid management system. Also used for local IED integration in substation</td>
<td>Substation and smart grid devices: Communication with control centre</td>
<td>Ethernet TCP/IP</td>
<td>Europe, Asia, Middle East, Africa</td>
</tr>
<tr>
<td><strong>IEC 60870-5-101</strong></td>
<td>Mainly in substation for legacy IED integration</td>
<td></td>
<td>Serial RS232</td>
<td>Mainly replaced by IEC 60870-5-104</td>
</tr>
<tr>
<td><strong>IEC 60870-5-103</strong></td>
<td>Substation for protection IED integration</td>
<td></td>
<td>Serial RS485</td>
<td>Mainly replaced by IEC 61850</td>
</tr>
<tr>
<td><strong>DNP3/IEEE 1815</strong></td>
<td>Substation and smart grid devices for local IED integration. Increasingly in smart grid management system for grid management</td>
<td>Substation and smart grid device: Communication with control centre or substation control system</td>
<td>Serial RS232/485 and Ethernet TCP/IP</td>
<td>USA, South America, Australia, United Kingdom</td>
</tr>
<tr>
<td><strong>IEC 61850</strong></td>
<td>Mainly in substation for legacy IED integration</td>
<td>Protection relays, remote terminal units, smart grid controllers, energy meters: Communication and management link to control centre or substation control system</td>
<td>Ethernet TCP/IP and Multicast Ethernet packets</td>
<td>Europe, Asia, Middle East, Africa, Canada and increasingly in Australia and South America</td>
</tr>
<tr>
<td><strong>Modbus</strong></td>
<td>Electrical meter integration</td>
<td></td>
<td>Serial RS232/485 and Ethernet TCP/IP</td>
<td>Worldwide</td>
</tr>
<tr>
<td><strong>M-Bus (based on IEC 60870-5)</strong></td>
<td></td>
<td></td>
<td>M-Bus serial and M-Bus wireless</td>
<td>Worldwide</td>
</tr>
</tbody>
</table>
Transition to Smart Grid Technology

Today’s electrical grids are currently transformed into smart grids integrating distributed energy resources (DER), components for the emerging E-Mobility (EM) infrastructure and in the near future also energy storage systems (ESS).

This development is challenging for most utility companies because current systems are based on the traditional Electricity Generation – Transmission – Distribution model.

With the de-regulation of the electricity market and the introduction of DER, EM and ESS the traditional grid model is no longer suitable and the grid monitoring, control and management systems struggle to keep up with new requirements for a reliable and safe operation of the electrical grid.

A modern and state of the art grid requires distributed intelligence for data acquisition, monitoring and control covering all sections of the grid.

Information is now shared with external service providers and the consumer on a much larger scale.
Transition to Smart Grid Technology...

Integrated Structure

- Supports traditional Top-to-Bottom hierarchy
- Enables utilities to manage resources more economically and opens the market to competition

Energy and Service Providers

- Integrates distributed energy resources
- Manages local energy storage facilities and E-mobility

Adds more customer services

- Provides more information to the customer and allowing the customer to participate in the energy market

SystemCORP
Embedded Technology
# Future Smart Grid Communication

## IEC/IEEE Standards

<table>
<thead>
<tr>
<th>Standard</th>
<th>Client/Master Deployment</th>
<th>Server/Slave Deployment</th>
<th>Communication Medium</th>
<th>Distribution</th>
</tr>
</thead>
<tbody>
<tr>
<td>IEC 60870-5-104</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>YES</strong></td>
<td>Substation and smart grid devices: Communication with control centre</td>
<td>Ethernet TCP/IP</td>
<td>Europe, Asia, Middle East, Africa</td>
</tr>
<tr>
<td>IEC 60870-5-101</td>
<td>Limited</td>
<td>Mainly in substation for legacy IED integration</td>
<td>Serial RS232</td>
<td>Mainly replaced by IEC 60870-5-104</td>
</tr>
<tr>
<td>IEC 60870-5-103</td>
<td>No</td>
<td>Substation for protection IED integration</td>
<td>Serial RS485</td>
<td>Mainly replaced by IEC 61850</td>
</tr>
<tr>
<td>DNP3/IEEE 1815</td>
<td><strong>YES</strong></td>
<td>Substation and smart grid devices for local IED integration. Increasingly in smart grid management system for grid management</td>
<td>Ethernet TCP/IP</td>
<td>USA, South America, Australia, United Kingdom</td>
</tr>
<tr>
<td>IEC 61850</td>
<td><strong>YES</strong></td>
<td>Protection relays, remote terminal units, smart grid controllers, energy meters: Communication and management link to control centre or substation control system</td>
<td>Ethernet TCP/IP and Multicast Ethernet packets</td>
<td>Europe, Asia, Middle East, Africa and increasingly in Australia and South America</td>
</tr>
<tr>
<td>Modbus (based on IEC 60870-5)</td>
<td><strong>YES</strong></td>
<td>Mainly in substation for legacy IED integration</td>
<td>Serial RS232/485 and Ethernet TCP/IP</td>
<td>Worldwide</td>
</tr>
<tr>
<td>M-Bus</td>
<td><strong>YES</strong></td>
<td>Electrical meter integration</td>
<td>M-Bus serial and M-Bus wireless</td>
<td>Worldwide</td>
</tr>
<tr>
<td>IEC 61131</td>
<td><strong>YES</strong></td>
<td>Internal client server structure for exchange of input, commands and processed data from PLC to system database</td>
<td>Ethernet for programming and diagnostics</td>
<td>Worldwide</td>
</tr>
</tbody>
</table>

### The most popular communication media for future communication interfaces will be Ethernet TCP/IP and low level Ethernet communication protocols
Future Smart Grid Communication...

New Communication Protocols are emerging in the industry – and system integrity has to be maintained

IEC 61850 has the most comprehensive set of rules for interfacing with other communication applications
Future Smart Grid Communication...

New applications will be introduced to the power industry

E Mobility

**Electric Vehicle Charging Infrastructure**

**OCPP – Open Charge Point Protocol**

- Web based communication via secured communication
- Not related to any communication protocols or structures currently used in the industry
- Merges station monitoring, control and customer billing

Currently does not play an important role in utility communication in relation to grid management. Once the number of charging stations grows to a more significant number the importance of OCPP will also increase.
Future Smart Grid Communication...

IoT – Internet of Things

AT this stage no international standard for IoT communication has been accepted or recognized by the electrical utility industry. Industry alliances are working towards IEC or IEEE recognition.

The architecture of IoT protocols can be explained in layers instead of fitting them into the OSI model.

https://www.lora-alliance.org → Wireless local communication

http://zigbee.com → Wireless local and mesh networks

http://www.iotworldalliance.org → GSM Worldwide -Telstra
Future Smart Grid Communication...

IoT Protocol Integration

Instead of fitting the IoT protocols into the OSI model (Open System Interconnection Model) the structure has to be explained according to implementation methods

- Infrastructure – 6LowPAN, IPv4/IPv6, RPL
- Identification - - EPC, uCode, IPv6, URIs
- Comms/ Transport – Wifi, Bluetooth, LPWAN
- Discovery – Physical Web, mDNS, DNS-SD
- Data Protocols – MQTT, CoAP, AMQP, Websocket, Node
- Device Management – TR-069, OMA-DM
- Semantic – JSON-LD, Web Thing Model
- Multi-layer Frameworks – Alljoyn, IoTivity, Weave, Homekit

Most of the above listed features and standards are currently unknown in the electrical utility industry and will require expert knowledge from outside the industry!!
Future Smart Grid Communication...

IoT Protocol Integration...

- Temperature
- Vibration
- Humidity
- Weather
- Operation/Activities
- Metering
- ......

Substation Control System

Conventional Protection, Monitoring and Metering

Grid Monitoring and Control
- IEC 60870-5-104
- IEC 61850
- DNP3.0

Cloud Computing
- OPC-UA
- Amazon Cloud Services
- ......

Monitoring, Automation, Communication
Cyber Security

Cyber Security is defined in Cyber Security Frameworks worldwide

- NERC CIP
- NIST Cyber Security Framework
- bðew white paper

Compliant with Key-Standards
Describing ‘How’ should it be done

- ISO/IEC 62443 (System Security)
- ISO/IEC 62351 (Communication Security)
- ISO/IEC 27001/27019 (Security Mgmt)

Conform to regulatory requirements
Describing what ‘must’ be done

- IT Security Law
- Security Catalogue
- Protection Profile

- Follow industry standard, i.e. bdew
- Report on incidents
- Implementation and Certification of an Information Security Management System (ISMS)
- Cryptographic requirements for Smart Metering
- Assessment and certification of ICS systems
- Auditable compliance (NERC) is required for bulk power systems (since 2010)
Future Smart Grid Communication...

Cyber Security....

Managing Cyber Security Risks

<table>
<thead>
<tr>
<th>Secured Communication</th>
<th>• Secured with SSL/TLS/IPsec (IEC 62351-3)</th>
<th>• Client/server authentication (IEC 62351-4/6)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operational Security</td>
<td>• Signed software/firmware (IEC 62351-10)</td>
<td>• Malware protection</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• ProductCERT – Vulnerability handling</td>
</tr>
<tr>
<td>Access Control</td>
<td>• Centralized account management</td>
<td>• Centralized password management (IEC 62351-8)</td>
</tr>
<tr>
<td>Security Monitoring</td>
<td>• Centralized event logging (IEC 62351-14)</td>
<td>• Installed base monitoring (IEC 62351-7)</td>
</tr>
<tr>
<td>Future Readiness</td>
<td>• Ready for PKI (IEC 62351-9)</td>
<td>• Modularity for tomorrow</td>
</tr>
</tbody>
</table>

PKI = Public Key Infrastructure
Future Smart Grid Communication...

Cyber Security.... Examples of Cyber Attacks

- **Stuxnet**
  - Iran nuclear plant
  - 45,000 machines infected
  - PLC modified and destroyed

- **Duqu**
  - Iran, Sudan
  - Espionage malware targeted at Energy sector

- **Shamoon**
  - Saudi Aramco attack
  - 30,000 Windows-based machines infected

- **Unknown malware**
  - German steel mill
  - Uncontrolled shutdown of a blast furnace due to control component breakdowns

- **Sandworm, BlackEnergy**
  - Ukraine
  - 200,000 people left without electricity due to grid blackout


2017: Who’s next?

---

[Image with logos: Monitoring, Automation, Communication]

SystemCORP
Embedded Technology
Q&A

????

THANK YOU !!!