Substation Automation/IEC 61850

- 8:30 am Opening remarks and Introductions
  - Gerry Cauley, President and CEO, NERC
  - Tobias Whitney, Senior Manager of CIP Compliance, NERC
  - Tom Hofstetter, Senior CIP Compliance Specialist, NERC
- 9:00 am-10:00 am – Overview of IEC 61850
  - Deepak Maragal, Senior Protection & Control Engineer, New York Power Authority (NYPA)
  - Herb Falk, Senior Solutions Architect, Systems Integration Specialists Company (SISCO)
- 10:00 am-11:00 am – Building the business case for automation
  - Chan Wong, Sr. Engineer, Entergy
  - Jeff Gooding, IT Principal Manager, Enterprise Architecture & Strategy, Southern California Edison (SCE)
- 11:00 am-12:00 pm – Describing the Architecture of IEC 61850 and Generic Object Oriented Substation Event (GOOSE) Messaging
  - Craig Preuss, Engineering Manager, Black and Veatch
  - Eric Stranz, Business Development Manager, Siemens
- 12:00 pm – 1:00 pm – Lunch
- 1:00 pm – 2:00 pm – Security and CIP compliance considerations during deployment
  - Scott Mix, CIP Technical Manager, NERC
- 2:00 pm – 4:00 pm – Roundtable discussion, Industry and Vendor Experiences
- 4:00 pm – 4:30 pm – Closing and Next Steps
  - Tobias Whitney, Senior Manager of CIP Compliance, NERC
Questions and Answers

TransitionProgram@nerc.net
Overview of IEC 61850 technology

NERC Emerging Technology Workshop
Nov-15, 2016

Deepak Maragal, PhD, PE
Senior Protection & Control Engineer-I
New York Power Authority

Herbert Falk
Senior Solutions Architect
Systems Integration Specialists Company
Agenda

➤ What is IEC 61850?

➤ What applications do IEC 61850 cover?

➤ Pros-Cons of IEC 61850 based Substation Automation System

➤ Architectures

➤ Time synchronization

➤ Cyber Security
Perform functions necessary to aid in efficient generation, transmission, distribution of power
General Architecture of Substation Automation System

Substation Equipment

Network

Substation Equipment

Network
IEC 61850 based Substation Automation System

- **Digital Elements**
  - Logic
  - Logic Gates: N/AND, N/OR, NOT, XOR XNOR
  - Timers:
    - Time Delay Pick-up
    - Time Delay Drop-Out
  - Latches, Flip-flops

- **Standard Elements**
  - Circuit Breakers
  - MOD / Disconnect
  - Monitor
  - Equipment
  - Coil – V & I

- **LEDs / HMI**

- **Custom Analog Functions**
  - App. specific, Measurements

- **Substation Equipment / Relays**
  - Station Bus (Other IEDs)
    - GOOSE
    - MMS

- **Station Bus**
  - GOOSE
  - MMS

- **GOOSE**

- **MMS**
IEC-61850: What is Standardized?

**Functions**
- Definitions & Nomenclature
- Parameters & Attributes
- Hierarchical data structure

**Communication**
- Medium supporting Ethernet/IP
- Protocols: GOOSE, SV, MMS
- Security: IEC 62351

**Process and format**
- XML representation of all data
- Std. files & content: SCL files
- Std. interchanging process
Substation Automation System: IEC-61850

- Protection
- Protection Related
- Control
- Metering & Measurement
- Supervision & Monitoring
- Substation Equipment
- Device (IED)
- Instrument transformer (CT/PT)
- Cyber Security (IEC-62351)
IEC 61850 Modeling Framework

- Common data classes
  - Attributes: Data types
  - Behavior
    - Trigger on change
    - Operation states
  - Control states

Table 14 – Single point status common data class definition

<table>
<thead>
<tr>
<th>Attribute Name</th>
<th>Attribute Type</th>
<th>FC</th>
<th>TrgOp</th>
<th>Value/Value Range</th>
<th>M/I/O/C</th>
</tr>
</thead>
<tbody>
<tr>
<td>DataName</td>
<td>Inherited from Data Class (see IEC 61850-7-2)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DataAttribute</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>stVal</td>
<td>BOOLEAN</td>
<td>ST</td>
<td>chg</td>
<td>TRUE</td>
<td>FALSE</td>
</tr>
<tr>
<td>q</td>
<td>Quality</td>
<td>ST</td>
<td>chg</td>
<td></td>
<td>M</td>
</tr>
<tr>
<td>t</td>
<td>TimeStamp</td>
<td>ST</td>
<td></td>
<td></td>
<td>M</td>
</tr>
</tbody>
</table>

**status**

| subEna        | BOOLEAN        | SV |       |                  | PICS_SUBST |
| subVal        | BOOLEAN        | SV |       | TRUE | FALSE | PICS_SUBST |
| subQ          | Quality        | SV |       |                  | PICS_SUBST |
| subID         | VISIBLE STRING64 | SV |       |                  | PICS_SUBST |

**configuration, description and extension**

| d             | VISIBLE STRING255 | DC | Text |        | O     |
| dU            | UNICODE STRING255  | DC |      |        | O     |
| cdcNs         | VISIBLE STRING255  | EX |      |        | AC_DLND_M |
| cdcName       | VISIBLE STRING255  | EX |      |        | AC_DLND_M |
| dataNs        | VISIBLE STRING255  | EX |      |        | AC_DLNM |

**Services**

As defined in Table 13
IEC 61850 Communication Types

- Multicast (Publisher ↔ Subscriber)
  - Similar to Broadcast
  - GOOSE, SV
  - Applications:
    - Protection, Monitoring, Recording, Metering...

- Client – Server
  - Security possible through IEC-62351
    - Encryption, User Authentication, Access Control...
  - Applications
    - Control
IEC 61850 Communication Framework

Multicast
- Measurement Messaging
  - Sampled Values (SV)
- Protection Messaging
  - GOOSE
- UDP/IP
  - IGMP/DSCP (90-5)*

Client/Server
- Symmetric Key Access For 90-5
- Core ACSI Services
- GDOI (90-5)*
- MMS Protocol
- RFC 1006
- TLS
- TCP/IP

Time Sync
- IEEE 1588*
- IEEE NTP
- UDP/IP

ISO/IEC 8802-3 Ethertype - Ethernet

* - Added in Edition 2 Amendment
IEC 61850 Communication Types

- Multicast (Publisher ↔ Subscriber)
  - Similar to Broadcast
  - GOOSE, SV
  - Applications:
    - Protection, Monitoring, Recording, Metering...

- Client – Server
  - Security possible through IEC-62351
    - Encryption, User Authentication, Access Control ...
  - Applications
    - Control
Traditional P&C System

IEC-61850 based P&C System
Advantages of IEC 61850 based SAS

- Cable reduction
- Interoperability & standardization
- Extensive troubleshooting & performance data
- Self monitoring & improvement in reliability
- Distributed and Centralized implementation
Disadvantages of IEC 61850 based SAS

- New technology is Complex
  - Requires change
  - New skills & tools

- Additional burden on Network management

- Cyber security overheads: NERC CIP

- Complexity & overheads out way Benefits in many applications
IEC 61850 Beyond North America

IEC 61850 Adoption
- Trending towards adoption
- Committed to DNP
- Adapted IEC 61850

Created with mapchart.net ©
IEC 61850 Beyond the Substation (North America)

- Substation-to-Control Center (IEC/TR 61850-90-2) targeted for SCADA communication
  - AEP – in all substations
  - SCE – Centralized Remedial Action Scheme and all future substations
  - CONED and others have active deployments

- Substation-to-Substation (IEC/TR 61850-90-1) communication typically used for protection control
  - SCE’s, PG&E, SRP, Toronto Airport are examples

- Secure Synchrophasor for WAMPAC
  - PG&E has an active deployment for Wide Area Monitoring and Situational Awareness (no PAC)

- Windpower and DER (including aggregation) for SCADA
  - E.on and EDF Canada (Windpower)

- Largest IEC 61850 deployment coming in a SW Refinery
Transitioning to a Digital Substation

- SCADA
- RTU
- Relays
- Devices
- CTs/PTs

Process

- Station Bus

Merging Units
Station Bus – Performance and Resiliency Considerations

➢ Performance

➢ SCADA traffic
  ➢ “Low” speed
  ➢ Network Resiliency: RSTP

➢ Automation
  ➢ Combination of “Low” and “Medium” (<20 msec) speed
  ➢ Utilizes GOOSE
  ➢ Network Resiliency: HSR or PRP

➢ Protection (3-6 msec)
  ➢ Utilizes GOOSE
  ➢ Network Resiliency: HSR or PRP

➢ Time Sync Accuracy
  ➢ Resiliency probably needed
  ➢ Important for post mortem analysis
  ➢ Important for geographically disperse automation (e.g. out-of-step/synchrophasors)
Process Bus – Performance and Resiliency Considerations

- **Performance**
  - “High” Speed
  - Network Resiliency: HSR or PRP

- **Time Sync Accuracy**
  - Resiliency is needed
    - Important for post mortem analysis
    - Important for geographically disperse automation (e.g. out-of-step/synchrophasors)
Substation to Control Center (IEC 61850-90-2)

➢ Use Cases

➢ Telecontrol (SCADA)
➢ Synchrophasor
➢ Disturbance
➢ Counting
➢ Power Quality
➢ Asset/Condition Based Maintenance
➢ Configuration
Newton-Evans reports very low penetration of IEC 61850 in North America.
Synchrophasors

- Routable IEC 61850 Secure Sampled Values was developed for synchrophasors

- Time Sync accuracy and resiliency is typically needed
Substation-to-Substation

Use Cases:

- Distance line protection
- Transfer/Direct Trip
- Interlocking
- Multi-phase reclosing
- Current differential protection
- Phase Compensation protection

Typically uses GOOSE/Routable GOOSE and needs Time Sync Resiliency
Information courtesy of pacworld. Article can be found at: 
http://www.pacw.org/issue/june_2016_issue/secured_routable_goose_mechanism.html
Sampled Values for CT/PT sharing (Merging Units)

- 1 pps, IEC 61850-9-3, IEEE C37.238
Bump-less Network Resiliency: HSR & PRP

PRP – Packet ID in Ethernet padding
First packet received wins

HSR – Packet ID before Ethertype
If received packet previously discard packet
IEC 61850: Time and Time Synchronization

TimeStamp is UTC Time down to 60 nsec. Similar format to NTP except for Time Quality (last 8 bits of fractions of second)

Time Quality is embedded into timestamps of IEC 61850 (unique to 61850).

- Leap Seconds Known (TRUE)/ Leap second being processed (FALSE)
- Clock Not Synchronized
- Clock Failure (for internal clock failure)
- Time Accuracy (may change depending upon internal or source drift)

Logical Nodes of LTIM and LTMS expose information regarding time synchronization and allows for multiple time sync sources: NTP, 1 PPS, multiple 1588 masters and boundary clocks.
Network fault tolerance/resiliency provided by HSR or PRP

Ethernet switches must participate in 1588 adjustments in order to maintain maximum accuracy.
Mapping of TC57

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 61850-8-1 with MMS
- IEC 61850-8-2 XML 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 62351-10: Security architecture guidelines for TC 57 systems
- IEC 62351-12: Resilience and Security Recommendations for Power Systems with DER
- IEC 62351-9: Key Management

IEC 62351-90-1: RBAC Guidelines
- DC 06/2016

IEC 62351-90-2: Deep Packet Inspection
- DC 06/2016

IEC 62351-10: Security architecture guidelines for TC 57 systems
- TR Ed.1 – 2012

IEC 62351-12: Resilience and Security Recommendations for Power Systems with DER
- DTR - 01/2016, TR mid-2016

- DTR 01/2016, TR mid-2016

IEC 62351-90-3: Deep Packet Inspection
- NWIP Prepared

IEC 62351-100 Conformance Testing

IEC 62351-100-1: NWIP Prepared

IEC 62351-100-5-7 (Part 3/5)

IEC 60870-5-104 & DNP3

IEC 60870-6 TASE.2 (ICCP)

IEC 60870-6 TASE.2 (ICCP)

IEC 60870-5-104 & DNP3

IEC 60870-5-101 & Serial DNP3

IEC 61850 GOOSE and SV

IEC 61850-8-1 with MMS

IEC 61850-8-2 XML over XMPP
IEC 61850 Security: Client/Server

Security Plane

IEC 61850-90-19*
IEC 62351-90-2
IEC 62351-8 (RBAC)

IEC 62351-9 (Key Mgmt)

Data-Exchange

IEC 61850-8-1
IEC 61850-8-2

Security for Data-Exchange

IEC 62351-6 (61850 Security)

IEC 62351-4 (MMS Security)

IEC 62351-3 (TLS Security)

Session Security (Auth., Integ., Selected cipher suites)
Key Update (Resume & Renegotiate)

Use of TLS
Connection Security
End-to-End Security

GOOSE, SV Security
MMS by inheritance
RBAC infrastructure allows:

- New role definitions
- Area of responsibilities
- Changes based upon operational constraints

**Table 1 – List of pre-defined role-to-right assignment**

<table>
<thead>
<tr>
<th>Value</th>
<th>Role</th>
<th>Right</th>
<th>VIEW</th>
<th>READ</th>
<th>DATASET</th>
<th>REPORTING</th>
<th>FILEREAD</th>
<th>FILEWRITE</th>
<th>FILEMGT</th>
<th>CONTROL</th>
<th>CONFIG</th>
<th>SETTINGGROUP</th>
<th>SECURITY</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;0&gt;</td>
<td>VIEWER</td>
<td>X</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>&lt;1&gt;</td>
<td>OPERATOR</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>&lt;2&gt;</td>
<td>ENGINEER</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>&lt;3&gt;</td>
<td>INSTALLER</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>&lt;4&gt;</td>
<td>SECADM</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>&lt;5&gt;</td>
<td>SECAUD</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>&lt;6&gt;</td>
<td>RBACMNT</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>&lt;7...32767&gt;</td>
<td>Reserved</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>&lt;32768 .. -1&gt;</td>
<td>Private</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

For future use of IEC defined roles.

Defined by external agreement. Not guaranteed to be interoperable.
### IEC 61850 Security: GOOSE and SV

<table>
<thead>
<tr>
<th></th>
<th>GOOSE</th>
<th>SV for CT/PT</th>
<th>Synchrophasors</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>L2</td>
<td>UDP/IP</td>
<td>L2</td>
</tr>
<tr>
<td>Authentication</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Tamper Detection</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Confidentiality</td>
<td>x</td>
<td>x</td>
<td>Not Suggested</td>
</tr>
</tbody>
</table>

Policy and symmetric keys managed through extensions of GDOI – Key Distribution Center (KDC).

Layer 2 can also be non-secure and that is what is typically deployed for intra-substation communication.
Opportunities

Provides:
- Members with access to draft standards
- Supports user feedback and answering questions
- Sponsoring of the 4th IEC 61850 IOP
- Other benefits

IEC 61850 Boot Camp
Co-located with the 2017 IEC 61850 IOP. Scheduled October 12-13, 2017 in New Orleans.

2017 IEC 61850 Interoperability Testing
Set-up October 13, 2017 in New Orleans
Testing October 14-19, 2017
Coordination and test development starting 11/2016

IEEE PSRCC H30
Next meeting January 2017
New Orleans
Provides a forum for users and vendors to discuss issues in using IEC 61850 and forward issues that may impact the IEC standards to the appropriate standards body.
Deepak.Maragal@nypa.gov
Office: 914-287-3874
Cell: 914-364-1241

Herb@sisconet.com
Office: 586-254-0020 x105
61850 Business Drivers
Digital Re-Invention at Southern California Edison

Jeff Gooding
IT Principal Manager
Enterprise Architecture & Strategy

November, 2016
External factors drive transformative change...

**Policies**
- Ambitious environmental and renewable energy mandates
- Federal and state incentives for alternative energy
- Expectations about 3rd-party capabilities and technologies

**Technologies**
- Falling costs of distributed generation
- Advancement in demand-side technologies
- Possible emergence of effective energy storage
- Anticipated plug-in electric vehicle adoption rates

**Customers**
- Concerns about future costs and reliability
- Increasing self-generation
- Interest in getting off the grid

**Competition**
- Consumer product and Internet companies
- New energy service companies
- Large integrators and defense contractors
- Traditional energy technology vendors
...resulting in fundamental changes

CURRENT

Grid stability thru rotational inertia
Dispatchable generation
Passive/predictable loads
Human-in-the-loop grid management
Rigid and centralized system control

EMERGING

Drivers
- Policies
- Technologies
- Customers
- Competition

Reduced stability due to generation mix change
Stochastic generation
Transactive loads
Faster system dynamics by orders of magnitude
Flexible and resilient distributed systems
...that yield pressures to modernize the grid

- Network (end-to-end IP) and software-centric technologies that allow grid operations to adapt to the changing energy landscape are required
- Faster design and implementation of grid infrastructure is required
- Lower implementation and operational costs are required
- Increasing reliability and safety is required
- IEC-61850 is a comprehensive standard for design of substation automation and applications that supports these key business drivers
- The use of IEC-61850 may be extended beyond the substation to additional distribution automation and protection use cases
61850 Key Business Benefits

- **Capital Cost Reduction** – Less space for mechanical switches, copper wires, signaling devices and meters as well as decreased complexity in CT & PT wiring if process bus is used.

- **Interoperability** – Multi-vendor integration is faster and avoidance of vendor lock-in drives costs down. Integration costs are pushed to the vendors.

- **Increased speed to delivery** – Using the 61850 standard improves engineering efficiency, procurement and commissioning through standard configuration language, object-oriented software, XML and automated testing tools.

- **Operational Reliability** – Enhanced situational awareness allows for better and faster operational decisions with more timely data. Reduced equipment operations and maintenance costs by reducing time to find and fix issues (some fixed automatically).
Technical Imperatives in a Digital Utility

• Common “core” communications protocols across the grid with virtualized gateways and edge compute to translate non-61850 protocols
• End-to-end standard Internet Protocol (IP) communications to facilitate modern cybersecurity on the grid
• Common cybersecurity framework and a “defense-in-depth” design to protect the grid against attack
• Real-time, distributed control and event-driven architectures
• Software-centric solutions with remote upgradability and automated testing to accommodate requirements in the future
61850 enables information management

**Goals:**

- Make data visible
- Make data accessible
- Enable data to be understandable
- Enable data to be trusted
- Enable data interoperability

**Actions:**

- **Make Data Assets Available to the Enterprise:**
  - Use metadata to describe and advertise data assets
  - Create data asset catalogs and organize by community-defined structure
  - Post data assets to shared space for Enterprise users

- **Make System Data / Processes Available to the Enterprise:**
  - Define and register format and semantics of system data and processes
  - Provide reusable/easy-to-call access services to make system data and processes available to the Enterprise

To make the right decisions at the right time

Courtesy DOD office of CIO
1. Only one simplified substation shown. RASs are tightly integrated with one or more subs, generators, and transmission lines.

- Blue lines indicate high-speed diverse path communication links with switches and routers. A and B side monitoring and mitigating data goes to and from control centers. Per WECC requirements RASs have A and B sides and diverse paths for redundancy and reliability purposes. The small arrows represent high volume of messages.

- CRAS central controllers are servers in control centers that evaluate monitoring data and send mitigation signals.

- Mitigation relays trip generation or shed load as needed to protect the transmission grid (via circuit breakers not shown).
SA-3 IEC61850 System

• Security / access control
  – Access management
  – Active monitoring / notification

• Robust configuration management
  – Centralized management services for:
    • Configuration, remote access, and fault file retrieval
  – Auto-configuration
  – Elimination of vendor HMI build process & cost
  – Active monitoring / notification

• System operation
  – Integration to other systems (eDNA, DMS/SCADA, EMS, FAN, DVVC)
  – Real time data beyond SCADA (historian eDNA collect data for analysis)
  – Redundancy for higher reliability
  – Centralize substation data (Data Concentrator)
Transforming Substations into Intelligent Hubs

**Common Substation Platform:**
- Server-grade redundancy in the substation
- High availability, high capacity computing platform
- Centralized management of software/firmware
- Provides cyber-security / network segmentations
- Supports de-centralized control applications
- IT & OT device access and mgmt

**Next Generation Substation Automation:**
- Open, non-proprietary communications standard, 61850 protocols
- Process bus
- Remote management and diagnostics of equipment
- Data beyond SCADA: predictive maintenance
Questions?
IEC 61850
Next Gen Substation Automation

Chan Wong
cwong@entergy.com
While the project moving forward, we will be encourage more Entergy family members to join us for this venture.
Collaborators
Motivation

- Safety first
  - Energized conductors
  - Copper Theft
  - Easier and efficient blown fiber installation
  - Minimize windshield time (Employee driving to substation due to smarter condition monitoring)

- Customers first / satisfaction
  - Faster Disaster Recovery
    - Bundle of copper wires replaced by fiber optic cable
    - Commissioning time and settings configuration are reduced

- Cost saving
  - Material – Panels, wires, mechanical switches and etc
  - Engineering time
  - Construction time and blueprint
Katrina ? Sandy ? Mathew ...and...

- Faster Recovery Time (One of the motivations)
  - Replace with few pair of fiber and merging unit
  - Instead of re-pulling copper cable of a flooded substation
Current system with Copper wires
Fiber blowing and Microducts

- Collaborate with OptiCOM and Condux to test the Microducts MICRO-COM
- Save time, cost
- Improve safety
- 140 feet in 40 seconds
V-Model System: Integration

IEC 61850: V-Model

- Develop a integration process – V-Model
Developed a Multivendor lab

Develop a lab at Kenner with Multi vendor devices (2014-2015)
• As a sandbox to test the technology
• Develop integration process to the existing system

Mission statement of this lab includes:
• **Interoperability**
  • To create a system that is interoperable among multiple vendors
• **Sustainable**
  • To ensure knowledge, and skillset retention within the company, maintaining the project vision, momentum and direction
• **Transparent**
  • To create an open and transparent environment where goals and knowledge are shared and achieve together
Plugfest – Bring every one together

- Organized the Plugfest to have all the SME of each vendor to assist the integration process
Plugfest 1.0

- **Proof of concept** of IEC 61850
- Show the benefit of running fiber versus copper wire
- Show the different testing process
- Design, Settings, and Communication difference compare to existing process
- Vendors: Doble, Omicron, ABB, ALSTOM, SEL

**Outcome**

- Test station were suggested to test the IEDs in the real life environment
- Pilot system will run in parallel with the existing protection scheme
Entergy Transmission Engineering

Plugfest 2.0 -- March 2015

• Added more collaborators
  – SIEMENS
  – Opti-COM

• Joliet Substation
  – Overcurrent protection scheme based on existing Breaker Settings

• Requirements
  – Edition 2 IEDs were requested
  – PRP or HSR – redundancy features
  – IEEE 1588
  – Human Machine Interface (HMI)
  – Grandmaster clock (Optional)
  – DFR (Optional)
  – Wireless (Optional)
Plugfest 3.0 – June 2015

- New Collaborators
  - SUBNET
  - HIRSCHMANN
  - Condux International

- Resolve challenges found in Plugfest 2.0

- Try to integrate all vendors into one network

- Redundancy protocol
  - VLAN
  - Multicast (To be tested later)

- Settings matches Joliet Substation Breakers’ Overcurrent Settings

- WE ARE READY FOR JOLIET
Joliet Pilot Substation

Entergy IEC 61850 was started in Early 2014 where it was a effort to evaluate and learn about this substation automation standard.

- **First** multi vendor IEC 61850 Process bus pilot

- Crossed disciplinary internal groups efforts: Grid, Settings, Design, OT and etc

- Collaborating with vendors, research institutes and national labs

- Hosted multiple technology and system integrations with vendors to prove the technology and also demo to Entergy stakeholders

- Aug 2015 deployed the pilot test racks to Joliet substation
  - Parallel with the overcurrent protection scheme of Feeder 2012 only read and not allowed to operate the breaker
  - Multiple utilities, industry leaders and Entergy management visited the sub
  - Conference papers and T&D magazine highlight
Deployment day from Lab to Sub
Parallel Monitoring System

- The IEC 61850 system is configured
  - Based on the settings from the protection scheme settings in the substation
  - Parallel system to monitor the system
  - ONLY Read --- NOT ALLOWED to operate the breaker
  - Used for data validation after pilot duration (>3months)
Overcurrent scheme

• All relay settings are based on the existing setting in Joliet Sub’s pilot breaker
• Process bus -- Pass!!!!
  – Per testing via injecting current through the merging unit
  – Relay subscribe the data through the network
• PRP -- Pass !!!!!
  – Lost of communication alarm picks up
  – Relay still picks up with one network
Entergy Transmission Engineering

COO and VP visit the Pilot Sub

Interoperability Testing of Substation Equipment

Entergy’s future-substation team is proof-testing the interoperability of multi-vendor station equipment to ensure robustness and reliability.

In Chan Wong and Tammy Lapeyrouse, Entergy

How soon can I get my power back on? This is the most frequently asked question utility call centers get when the power is out. In emergency situations and after natural disasters, it is crucial the utility be able to restore all the affected customers quickly while maintaining the reliability and stability of the grid.

Historically, power outages and interruptions have hounded the region served by Entergy. August 2016 marked the 50th anniversary of Hurricane Katrina, one of the most significant natural disasters in the state. From New Orleans, Louisiana, U.S. It was a cataclysmic event for residents and companies in the city. Around 20,000 Entergy customers, and 1,200 feeders were damaged by Hurricane Katrina.

Read more about how Entergy has advanced grid reliability and automation to ensure a more secure and resilient power grid in this article. In recent years, the utility has made significant investments in modern infrastructure, including the deployment of new, smarter, and more adaptive technologies to enhance grid reliability and resilience.

Paradigm Shift

As Energy Transmission Engineering, a group of young and dedicated engineers, the team is revolutionizing the way substation equipment is designed with a focus on modular, scalable, and intelligent solutions.

In early 2014, Energy Transmission Engineering introduced its new design philosophy, the eHub concept, to achieve greater reliability and efficiency. These hubs integrate the various substation functions in a single, modular, and easily manageable unit, allowing for faster and easier installation and maintenance.

Compared to the traditional copper-based design, the new eHub-based approach offers several advantages: reduced footprint, better thermal performance, and improved operator visibility and accessibility. Furthermore, the modular design enables easier upgrades and maintenance, ensuring that the substation can adapt to future needs.

First Steps

A foundation of a substation engineering group consisting of process and control engineers, field/program engineers, and automation, and operations information technology (OIT) and commissioning managers were formed to perform research and design.
Projected Schedule and deliverables

2016-2017

- 12/25/2016: IEC61850 Lab complete
- 3/15/2017: Training for GRID,
- 7/7/2017: Quarterly review on Joliet Sub
- 9/15/2017: Plan for Greenfield
- 12/12/2017: 1st Year DOE Patterson Completed

- 10/1/2016: Today
- 1/1/2017: IEC61850 Medium Voltage Standard Completion
- 4/1/2017: Add more MU to Joliet
- 7/1/2017: 8/3/2017 IEC61850 Trans Diff Standard Completion
- 10/1/2017
- 12/25/2017

2018-2019

- 1/1/2018: Greenfield Construction (Preferable close to NOLA)
- 4/1/2018
- 5/23/2018: Training and refresh course for all
- 1/1/2019
- 4/1/2019
- 7/1/2019
- 10/1/2019
- 12/23/2019

- 1/11/2018: * Quarterly review the pilot sub performance
- 5/26/2018: Optical CT evaluation
- 1/6/2019: Pilot at each state (Medium voltage) * Quarterly review the pilot sub performance
- 6/25/2019: Performance review with each pilot crew
- 11/27/2019: Decision to standardized all medium voltage to 61850
- 12/17/2019: End of DOE Patterson project
ONE MORE THING !!!
UCA IOP New Orleans

- The IOP test will take place in New Orleans in October 2017. It will be hosted by Entergy.
- The Boot Camp training
- IOP testing
  - October 14 - 19.
- IEC TC57 WG10
  - Follow after IOP
- Marriott Arts District / Convention Center
Thanks

Chan Wong
cwong@entergy.com
A: Training and support

- Hosts multiple trainings with stakeholders
  - Train and educate the new standard
  - Provide hands-on training on the equipment
  - Create training videos

- Internal technical support
  - Dedicated engineers needed to be trained to provide internal support
  - Serves as career development for internal organizations
## A: Cost Saving Analysis

### Itemized Costs

<table>
<thead>
<tr>
<th>Itemized Costs</th>
<th>Quantity</th>
<th>Cost / Unit</th>
<th>Totals</th>
<th>Benefits</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Copper System Costs</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Trenching</td>
<td>600</td>
<td>7.5 $/SF</td>
<td>$4,500</td>
<td></td>
</tr>
<tr>
<td>10 # 12 SIS wires, terminated</td>
<td>1800</td>
<td>28.0 $/SF</td>
<td>$50,400</td>
<td></td>
</tr>
<tr>
<td>20 # 14 SIS wires, terminated</td>
<td>1800</td>
<td>50.0 $/SF</td>
<td>$90,000</td>
<td></td>
</tr>
<tr>
<td>Schedule 80 &amp; boxes</td>
<td>1800</td>
<td>18.0 $/SF</td>
<td>$32,400</td>
<td></td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td></td>
<td></td>
<td>$177,300</td>
<td>Reference</td>
</tr>
<tr>
<td><strong>Fiber System Costs (PRP topology)</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Trenching</td>
<td>1600</td>
<td>1.0 $/SF</td>
<td>$1,600</td>
<td></td>
</tr>
<tr>
<td>Tubing</td>
<td>1600</td>
<td>2.5 $/SF</td>
<td>$4,000</td>
<td></td>
</tr>
<tr>
<td>Hardened Fiber</td>
<td>1600</td>
<td>2.5 $/SF</td>
<td>$4,000</td>
<td></td>
</tr>
<tr>
<td>GPS clock cabling</td>
<td>1600</td>
<td>2.5 $/SF</td>
<td>$4,000</td>
<td></td>
</tr>
<tr>
<td>Fiber Optic Terminations</td>
<td>128</td>
<td>$78</td>
<td>$9,984</td>
<td></td>
</tr>
<tr>
<td>GPS Clock</td>
<td>1</td>
<td>$2,500</td>
<td>$2,500</td>
<td></td>
</tr>
<tr>
<td>SIPROTEC 8MU80 Merging Units</td>
<td>16</td>
<td>4,000</td>
<td>$64,000</td>
<td></td>
</tr>
<tr>
<td>SIPROTEC PB201 Process Bus Modules</td>
<td>16</td>
<td>3,800</td>
<td>$60,800</td>
<td></td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td></td>
<td></td>
<td>$150,884</td>
<td>$26,416</td>
</tr>
<tr>
<td><strong>Fiber System Costs (HSR topology)</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Trenching</td>
<td>1600</td>
<td>1.0 $/SF</td>
<td>$1,600</td>
<td></td>
</tr>
<tr>
<td>Tubing</td>
<td>400</td>
<td>2.5 $/SF</td>
<td>$1,000</td>
<td></td>
</tr>
<tr>
<td>Hardened Fiber</td>
<td>533</td>
<td>2.5 $/SF</td>
<td>$1,333</td>
<td></td>
</tr>
<tr>
<td>GPS clock cabling</td>
<td>1600</td>
<td>2.5 $/SF</td>
<td>$4,000</td>
<td></td>
</tr>
<tr>
<td>Fiber Optic Terminations</td>
<td>34</td>
<td>$78</td>
<td>$2,652</td>
<td></td>
</tr>
<tr>
<td>GPS Clock</td>
<td>1</td>
<td>$2,500</td>
<td>$2,500</td>
<td></td>
</tr>
<tr>
<td>SIPROTEC 8MU80 Merging Units</td>
<td>16</td>
<td>4,000</td>
<td>$64,000</td>
<td></td>
</tr>
<tr>
<td>SIPROTEC PB201 Process Bus Modules</td>
<td>16</td>
<td>3,800</td>
<td>$60,800</td>
<td></td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td></td>
<td></td>
<td>$137,885</td>
<td>$39,415</td>
</tr>
</tbody>
</table>
• Entergy currently is the leader in process bus implementation but the station bus implementation had been performed by utility such as
  – AEP
  – BPA
  – SCE
  – NYPA
  – ConEd

• Experience sharing and learning about their deployment have been carried out to assist the process bus deployment of Entergy
IEC 61850 ARCHITECTURE AND GOOSE

CRAIG PREUSS
ENGINEERING MANAGER, TELECOM – PRIVATE NETWORKS
SECRETARY IEEE PES POWER SYSTEM COMMUNICATIONS AND CYBERSECURITY COMMITTEE
IEC 61850
ARCHITECTURE AND
GOOSE

Pieces, parts, and protocols
Architecture
The core parts easily demonstrate that any reference to a 61850 protocol is incorrect.
“OTHER STUFF” BESIDES PROTOCOLS

- System configuration language (61850-6)
- General requirements (61850-3)
  - Edition 1 primarily environmental
  - Edition 2 adds ratings, marking, documentation, packaging, dimensions, functional performance, safety, burden, mechanical, enclosure, documentation, etc.
- Testing (61850-10)
- Project management (61850-4)
- Object models
- Technical reports

61850 is so much more than just a protocol
WHO COMMUNICATES WITH WHOM?

IEC 61850-1:2013 INTERFACES (IFx)

- IF1: protection-data exchange between bay and station level
- IF2: protection-data exchange between bay level and remote protection (not in scope)
- IF3: data exchange within bay level
- IF4: CT and VT instantaneous data exchange (especially samples) between process and bay level
- IF5: control-data exchange between process and bay level
- IF6: control-data exchange between bay and station level
- IF7: data exchange between substation (level) and a remote engineer’s workplace
- IF8: direct data exchange between the bays especially for fast functions like interlocking
- IF9: data exchange within station level
- IF10: exchange between substation (devices) and a remote control center (in scope with 90-2-2016)
- IF11: the control-data exchange between different substations.

90-5-2012 introduces IF12 (between control centers) and IF13 (WAMS), then adds condition monitoring and diagnosis to IF7.
<table>
<thead>
<tr>
<th>PIECES, PARTS, AND PROTOCOLS</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>MMS</strong>&lt;br&gt;61850-5:2003</td>
</tr>
<tr>
<td><strong>Sampled Values</strong>&lt;br&gt;61850-9-2:2003</td>
</tr>
<tr>
<td><strong>GOOSE</strong>&lt;br&gt;High speed communication of analogs and digitals (61850-8-1:2004)</td>
</tr>
<tr>
<td><strong>Synchrophasors</strong>&lt;br&gt;61850-90-5&lt;br&gt; R-SV (routable sampled values)&lt;br&gt; R-GOOSE (routable GOOSE)</td>
</tr>
<tr>
<td><strong>Time synchronization</strong>&lt;br&gt;SNTP (61850-8-1:2003)&lt;br&gt; 1588v2 PTP&lt;br&gt; 61850-9-3</td>
</tr>
<tr>
<td><strong>File transfer</strong>&lt;br&gt;MMS file transfer&lt;br&gt;FTP/sFTP is “local issue”&lt;br&gt;61850-8-1:2011</td>
</tr>
<tr>
<td><strong>Rapid Spanning Tree Protocol</strong>&lt;br&gt;(RSTP)&lt;br&gt;61850-8-1:2011</td>
</tr>
<tr>
<td><strong>PRP (Parallel Redundancy Protocol) and HSR</strong>&lt;br&gt;(High availability Seamless Ring)&lt;br&gt;(61850-8-1:2011)</td>
</tr>
<tr>
<td><strong>ARP</strong>&lt;br&gt;Address Resolution Protocol&lt;br&gt;61850-8-1:2004&lt;br&gt;mandatory</td>
</tr>
<tr>
<td><strong>ICMP</strong>&lt;br&gt;Internet Control Message Protocol&lt;br&gt;61850-8-1:2011&lt;br&gt;Mandatory</td>
</tr>
<tr>
<td><strong>OTHER PROTOCOLS</strong>&lt;br&gt;61850-90-4&lt;br&gt;SNMP, Syslog, FTP, SSH&lt;br&gt;And others</td>
</tr>
</tbody>
</table>
Abuse of GOOSE – using it for Type 2 or 3 functions when MMS should be used

FUNCTION PERFORMANCE REQUIREMENTS AND 61850 PROTOCOLS

Table 37 – IEC 61850-5 interface traffic

<table>
<thead>
<tr>
<th>Function Type/Message</th>
<th>Interface (Table 1)</th>
<th>Protocol</th>
<th>Max. delay ms</th>
<th>Bandwidth</th>
<th>Priority</th>
<th>Application</th>
</tr>
</thead>
<tbody>
<tr>
<td>1A. Trip</td>
<td>GOOSE</td>
<td>L2 Multicast</td>
<td>3</td>
<td>Low</td>
<td>High</td>
<td>Protection</td>
</tr>
<tr>
<td>1B. Other</td>
<td>GOOSE</td>
<td>L2 Multicast</td>
<td>10 to100</td>
<td>Low</td>
<td>Medium High</td>
<td>Protection</td>
</tr>
<tr>
<td>2. Medium Speed</td>
<td>MMS</td>
<td>IP/TCP</td>
<td>&lt;100</td>
<td>Low</td>
<td>Medium Low</td>
<td>Control</td>
</tr>
<tr>
<td>3. Low Speed</td>
<td>MMS</td>
<td>IP/TCP</td>
<td>&lt;500</td>
<td>Low</td>
<td>Medium Low</td>
<td>Control</td>
</tr>
<tr>
<td>4. Raw Data</td>
<td>SV</td>
<td>L2 Multicast</td>
<td>4</td>
<td>High</td>
<td>High</td>
<td>process bus</td>
</tr>
<tr>
<td>5. File Transfer</td>
<td>MMS</td>
<td>IP/TCP/FTP</td>
<td>&gt;1 000</td>
<td>Medium</td>
<td>Low</td>
<td>Management</td>
</tr>
<tr>
<td>6. Time Sync</td>
<td>Time Sync</td>
<td>IP (SNTP) L2 (PTP)</td>
<td>&lt;1000</td>
<td>Low</td>
<td>Medium High</td>
<td>General Phasors, SVs</td>
</tr>
<tr>
<td>7. Command</td>
<td>MMS</td>
<td>IP</td>
<td>Low</td>
<td>Medium Low</td>
<td>Control</td>
<td></td>
</tr>
</tbody>
</table>

Taken from 61850-90-4-2013
WHERE ARE THESE PROTOCOLS EXPECTED TO BE SEEN ON A LAN?

<table>
<thead>
<tr>
<th>IF1</th>
<th>IF2</th>
<th>IF3</th>
<th>IF4</th>
<th>IF5</th>
<th>IF6</th>
<th>IF7</th>
<th>IF8</th>
<th>IF9</th>
<th>IF10</th>
<th>IF11</th>
<th>IF12</th>
<th>IF13</th>
<th>Protocol from IEC 61850-8-1-2011 Figure 1 IEC 61850-90-4 Table 37</th>
</tr>
</thead>
<tbody>
<tr>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td>MMS</td>
</tr>
<tr>
<td></td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>GOOSE</td>
</tr>
<tr>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>SV</td>
</tr>
<tr>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>MMS</td>
</tr>
<tr>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>SNTP/PTP</td>
</tr>
</tbody>
</table>

Red is “station bus” and green is “process bus”
VIEWING GOOSE FROM THE OSI STACK

Figure 6 – IEC 61850 protocol stack
GOOSE and SV are similar as defined in Annex C of 8-1-2011.

**GOOSE PACKET**

- **APPID** is from the GOOSE control block and is a system wide unique identifier of the application for the message.

- **gocbRef** describes the GOOSE control block that controls the message.

- **datSet** describes the objects sent in the message.

- **confRev** is the configuration revision.

- **allData** contains the objects sent in the message.

- **TAL** informs the subscribers how long to wait for the next message.

- **goID** is a user-assigned identification for the message.

- **stNum** a counter that increments each time a message is sent and value change detected.

- **sqNum** a counter that increments each time a message is sent.

- **goID** is a user-assigned identification for the message.

- **allData** contains the objects sent in the message.
GOOSE EVENT TIME LINE

- Publisher – subscriber
- Publisher sends control, status point, or analog values
- Not just one message, but a sequence calculated by the vendor that continuously sends data from publisher to subscriber
- Each IED that needs GOOSE messages from another must subscribe to those messages
- Even if the receiving IED is just powered up, it will be able to get updated status it needs
- Very fast and faster than wired

GOOSE messages can be constantly monitored, wires can not!
# Required Performance and Transfer Time for Functions Supported by GOOSE

| Message Performance Class | Transfer Time Class | IF1 | IF2 | IF3 | IF4 | IF5 | IF6 | IF7 | IF8 | IF9 | IF10 | IF11 | IF12 | IF13 | Protocol from IEC 61850-8-1-2011 Figure 1 IEC 61850-90-4 Table 37 |
|---------------------------|--------------------|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|------|------|------|--------------------------|---------------------------------|
| P6                        | TT1                | X   |     |     | X   | X   | X   | X   | X   | X   | X    | X    | X    | X    | MMS                      |
| P5                        | TT2                | X   | X   | X   | X   | X   | X   | X   | X   | X    | X    | X    | X    | MMS                      |
| P4                        | TT3                |     |     | X   |     | X   |     | X   |     | X   | X    | X    | X    | X    | MMS                      |
| P3                        | TT4 (20)           | X   | X   |     |     |     | X   | X   |     | X   | X    | X    | X    | X    | GOOSE                    |
| P2                        | TT5 (10)           |     |     | X   | X   |     |     |     | X   | X    | X    | X    | X    | X    | GOOSE                    |
| P1                        | TT6 (3)            |     |     |     |     | X   | X   |     |     | X   |     |     |     |     | GOOSE                    |
| P7                        | TT6                |     |     |     |     |     |     |     |     |     |     |     |     |     | SV                       |
| P8                        | TT5                |     |     |     |     |     |     |     |     |     |     |     |     |     | SV                       |
| P9                        | TT0                |     |     |     |     |     |     | X   |     |     |     |     |     |     | MMS                      |
| P10                       | TT2                |     |     |     |     |     |     |     |     |     |     |     |     |     | SNTP/PTP                 |
| P11                       | TT1                |     |     |     |     |     |     |     |     |     |     |     |     |     | SNTP/PTP                 |
| P12                       | TT0                |     |     |     |     |     |     |     |     |     |     |     |     |     | SNTP/PTP                 |
A ping pong (echo) test is actually used to measure transfer time, but it virtually eliminates the network and assumes symmetry on $t_a$ and $t_c$. 

PERFORMANCE IN IEC 61850-5:2013

- Transfer time
  - Impossible to directly measure
  - Not what is important to utilities – an end to end test
GOOSE CYBERSECURITY

• GOOSE message structure has an optional framework to support cybersecurity
  • Based on IEC 62351-6
  • Uses Reserved1 and Reserved2 fields from the message
  • Uses an extension to the message that contains the message authentication code

• Research indicates
  • The authentication using 1024-bit keys takes 8.3 ms
  • Using 2048-bit keys today will take longer
GOOSE ATTACKS

• Typical Layer 2 attacks
  • ARP attacks, MAC flooding attacks, spanning-tree attacks, multicast brute force attacks, VLAN trunking protocol attacks, private VLAN attacks, identity theft, VLAN hopping attacks, MAC spoofing and double-encapsulated 802.1Q/Nested VLAN attacks

• GOOSE attacks
  • GOOSE spoof (and variants)
  • GOOSE storm
  • High Status Number Attack (or GOOSE poison) (send stNum value of $2^{32}-1$
  • High rate flooding attack
  • Semantic attack
GOOSE SPOOF ATTACK

• GOOSE Spoof attack (one variant)
  • Publishing false layer 2 packets and subscribing IEDs mistakenly believe the messages are valid

GOOSE SPOOF MITIGATION

• Existing mitigations (typical to layer 2)
  • A dedicated VLAN ID for all trunk ports
  • Disable all unused ports and place in unused VLAN
  • Do not use the default VLAN (1)
  • Set all ports to non-trunking
  • Physical security to detect and delay unauthorized Layer 2 access

• GOOSE Spoof specific mitigations
  • GOOSE anomaly detection in switches and routers to reject GOOSE messages not consistent with 61850 configuration

• Other GOOSE mitigations
  • GOOSE anomaly detection in IEDs
IEC 61850 ARCHITECTURE AND GOOSE

Pieces, parts, and protocols

Example LAN Architectures
Figure 24 – Station bus as single bridge
Figure 25 – Station bus as hierarchical star
Figure 26 – Station bus as dual star with PRP
Figure 27 – Station bus as ring of RSTP bridges
61850-90-4-2013 EXAMPLE LAN ARCHITECTURES

Figure 28 – Station bus as separated Main 1 (Bus 1) and Main 2 (Bus 2) LANs
Figure 29 – Station bus as ring of HSR bridging nodes
Figure 30 – Station bus as ring and subrings with RSTP
Figure 31 – Station bus as parallel rings with bridging nodes
61850-90-4-2013 EXAMPLE LAN ARCHITECTURES

Figure 32 – Station bus as parallel HSR rings
Figure 33 – Station bus as hierarchical rings with RSTP bridging nodes
Figure 34 – Station bus as hierarchical rings with HSR bridging nodes
Figure 35 – Station bus as ring and subrings with HSR
Figure 48 – Process bus as star to merging units and station bus as RSTP ring
Figure 49 – Station bus and process bus as rings connected by a router
61850-90-4-2013 EXAMPLE LAN ARCHITECTURES

Figure 50 – Station bus ring and process bus ring with HSR
Figure 51 – Station bus as dual PRP ring and process bus as HSR ring
CONCLUSIONS

- IEC 61850 specifies an architecture for utility automation systems
- IEC 61850 includes many different protocols
- IEC 61850 supports applications that have performance requirements that can be met by some protocols and not others
- IEC 61850 has numerous possible architectures featuring “station bus” and “process bus”
- IEC 61850 GOOSE protocol is fast enough to support any time critical applications, plus those that are not
- IEC 61850 GOOSE protocol presents some cybersecurity challenges
Now is the time for any questions and discussion
Authors:
Eric Stranz, Business Development Manager, Siemens
Motivation
NERC Roundtable Forum

NERC CIP – Cyber security for TSO and Generation

- **Customer**
  - Consumer behavior tracking, e.g., through smart meters
  - Fraud through smart meter manipulation

- **Generation / DER**
  - Misuse of local administrative rights

- **Distribution and Transmission**
  - Substation Configuration is manipulated via local network, wireless or remote access

- **Market**
  - Fraud based on falsified offers and contracts (Customer, Utilities, DNOs, …)

- **Operation**
  - Unauthorized remote service access

11/21/2016 Energy Automation
**Cyber Threat Potential**

**Possible Attackers:**
- Countries
- Criminal organizations
- Script kiddies
- Insider
- Spoofing
- Malware
- Viruses
- …..
NERC Roundtable Forum

IEC-61850

Control Center

Substation Data Collector & Controller

Station Bus

MMS (data collection & controls)

GOOSE (virtual wires)

Process Bus

GPS Clock

3rd party device

Sampled Values (currents / voltages)

GOOSE (virtual wires)

IEEE 1588v2 time synch
Network Segmentation – Process and Station Bus Networks
IEC 61850 is an Ethernet-based standard for the design of electrical substation automation and the abstract data models can be mapped to a number of protocols, including MMS (Manufacturing Message Specification, the underlying communication architecture for ICCP), GOOSE, and Web Services. IEC 61850 is not a data link or network layer protocol, thus declaring IEC 61850 to be a routable or non-routable protocol is not appropriate. Time-critical messages, such as GOOSE messages for direct inter-bay communication, typically run on a flat Layer 2 network without the need for Layer 3 IP addresses. Other non-time-critical messages, including MMS and web services, typically run on a Layer 3 network, such as TCP/IP, with addressing and routing. The registered entity should carefully evaluate the communication environment supporting the IEC 61850 data protocol to determine if routable communication exists. If the IEC 61850 data is being communicated over a TCP/IP network, then that network connectivity is considered routable and should be protected per the CIP Standards accordingly.
IEC 61850 is an architecture for utility automation systems, including substations, that includes several protocols. Thus declaring IEC 61850 to be a routable or non-routable protocol is not appropriate. One protocol in the IEC 61850 standard is GOOSE, which can be used for time-critical applications, is a Layer 2 multicast protocol. GOOSE may be used on what 61850 calls station bus and/or process bus. Other protocols used in 61850, such as MMS and web services, typically run on a Layer 3 network, such as TCP/IP, with addressing and routing. Any utility automation system using 61850 protocols are likely using other protocols in addition to those included in 61850. The registered entity should carefully evaluate the communication environment supporting the IEC 61850 communication protocols to determine what Routable communication exists. Any TCP/IP network supporting communication protocols above layer 2 is considered Routable as newly defined in the NERC Glossary of Terms. Once Routable communication is determined, the registered entity should carefully evaluate ESPs, ERC, EAPs, LERCs, and LEAPs and any potential negative impacts on the performance on the protocols being protected.
A well designed Substation system can determine the health of the network by monitoring sequence or state alarms and indications for fast network diagnosis.
Why do people want to move to IEC-61850

• Up to 40% cost savings with Sampled Values Technology within a substation compared to a traditional copper installation (Based on a 12 Feeder Install)

• IEC-61850 GOOSE reduces copper interconnectivity between devices which results in significant savings in some installations

• Templates, reusable engineering make IEC-61850 an attractive option

• Physical Security is already required and Communications Security is already required if Ethernet is deployed in the substation

Is NERC CIP Compliance too difficult to even consider these technologies?
1.) Assess stations designations based on the CIP -014-01 (4.1.1.2)
2.) Define the (BES) Cyber System (formerly Critical Cyber Assets)
3.) Define Physical Security Perimeter (PSP)
4.) Define Electronic Security Perimeter(s) (ESP)
5.) Provide a Cyber Security Framework to Cyber Assets per CIP Standards
6.) Define Electronic Access Points into ESP(s)

In Version 5 NERC now allows for multiple ESP’s and does not restrict the ESP’s to the 6 wall approach.
Physical & Cyber security

• The physical security requirements
  • Need of authentication before entrance of station
  • Recognize and Alarm in case of unauthorized access
  • Protection against unauthorized access
• Cyber security
  • Mitigate misuse of access rights
  • Authentication of access
  • Prevents from outside threads and attacks on infrastructure
Normal NERC CIP Applicable Substations Should Already Include Physical Security Measures

The FERC Order No. 706, Paragraph 572, directive discussed utilizing two or more different and complementary physical access controls to provide defense in depth.

Two Factor Authentication
(Something you know, Something you are, Something you have)

Card Scanners, Cameras, Authentication Systems typically are already in place for a NERC CIP Station
**ESP at the Control House**

- 2 Factor Authentication
- Card Scan to Retrieve Key for Breakers
- Door switch triggers alarm where camera monitors activity
Network Design
2 Factor Authentication

Card Scan to Retrieve Key for Breakers

Door switch triggers alarm where camera monitors activity
Conclusions

- Further clarity on the IED straddling Station and Process bus

- V5 helps for utilities to adopt 61850 but decisions on PSP, ESP and ERC’s require additional effort by utilities

- Moving forward NERC needs to provide further clarification of existing Q&A and other materials referencing 61850. Engage Industry Experts to help clarify existing statements on 61850.

- Tunneling Goose between stations, Routable Goose, Routable Sampled Values are topics that have not been addressed or discussed and will require more review and discussion.

- End to End application to application encryption and authentication is years away for IEC-61850 MMS and GOOSE. NERC needs to continue to provide a framework that give utilities flexibility until it is complete. V5 has helped.

- Vendors may need to do more for GOOSE and SV monitoring
Thank you for your attention!
NERC CI P Implications of IEC 61850 in Transmission Stations

Scott R Mix, CISSP, CI P Technical Manager, NERC
Agenda

- Application of NERC Standards
- NERC Definitions
- What Does it Mean? (Compliance Implications)
- Effective Dates (Implementation Timeframes)
• NERC Standards apply to the Bulk Electric System (BES)
  ▪ Generally, 100kV and above, but with some exceptions, primarily for radial lines
  ▪ 20MVA and above generating units, 75MVA and above generating plants, with some exceptions for wholly behind-the-meter generation

• NERC Standards *do not* apply to distribution (i.e., non-BES)
  ▪ With several exceptions, primarily UFLS, UVLS, Blackstart Resources (generation), Cranking Paths
NERC CIP standards (CIP-002 through CIP-011) in their current version require a high / medium / low categorization, with corresponding requirement for the levels

- High only applies to Control Centers
- Medium and low applies to field assets (and Control Centers)

For medium impact assets, external connectivity also informs the requirements

- External Routable Connectivity includes more requirements

This presentation is not about the requirements; rather it is about scoping of assets subject to the requirements
• **Cyber Asset**: Programmable electronic devices, including the hardware, software, and data in those devices.
• **BES Cyber Asset (BCA):** A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, misoperation, or non-operation, adversely impact one or more Facilities, systems, or equipment, which, if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the reliable operation of the Bulk Electric System. Redundancy of affected Facilities, systems, and equipment shall not be considered when determining adverse impact. Each BES Cyber Asset is included in one or more BES Cyber Systems.
• **BES Cyber System (BCS)**: One or more BES Cyber Assets logically grouped by a responsible entity to perform one or more reliability tasks for a functional entity.

  (not part of the formal definition) Components of the BCS also include “glue” infrastructure components (e.g., networking infrastructure) necessary for the system to perform its reliability tasks, like merging units and network switches

  Tremendous flexibility is built into the definition – BCS could be the entire substation, all relays/equipment at a voltage level, relays/equipment at feeder/bay level, etc
• **Electronic Security Perimeter (ESP):** The logical border surrounding a network to which BES Cyber Systems are connected using a routable protocol.
• **Protected Cyber Asset (PCA):** One or more Cyber Assets connected using a routable protocol within or on an Electronic Security Perimeter that is not part of the highest impact BES Cyber System within the same Electronic Security Perimeter. The impact rating of Protected Cyber Assets is equal to the highest rated BES Cyber System in the same ESP.

  - A stand-alone substation HMI, if not needed for control processing, would be a PCA; however, if it was needed for control processing, it would be a BES Cyber Asset
  
  - Note that there are no requirements or restrictions on communications between Cyber Assets located within an ESP – the only requirements are for communications that pass through an EAP
• *Electronic Access Control or Monitoring Systems (EACMS)*: Cyber Assets that perform electronic access control or electronic access monitoring of the Electronic Security Perimeter(s) or BES Cyber Systems. This includes intermediate Systems.
  - Typically this includes Cyber Assets that perform firewall / filtering services, intrusion detection or monitoring services, logging services, authentication services, proxy services, etc
**Low Impact:**

- Current proposed requirements for Low Impact BES Cyber Systems (posted for comment and ballot until December 5, 2016) have eliminated definitions for both “LERC” and “LEAP”
- However, the concepts of external routable connectivity and requirements for controlling external routable access remain in the requirement language
CIP-003-7, Attachment 1, Section 3:

**Section 3. Electronic Access Controls:** For each asset containing low impact BES Cyber System(s) identified pursuant to CIP-002, the Responsible Entity shall implement electronic access controls to:

**3.1 Permit only necessary inbound and outbound electronic access as determined by the Responsible Entity for any communications that are:**

- **i.** between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s);
- **ii.** using a routable protocol when entering or leaving the asset containing the low impact BES Cyber System(s); and,
- **iii.** not used for time-sensitive protection or control functions between intelligent electronic devices (e.g. communications using protocol IEC TR-61850-90-5 R-GOOSE).

**3.2 Authenticate all Dial-up Connectivity, if any, that provides access to low impact BES Cyber System(s), per Cyber Asset capability.**
• **4.2.3.2** Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

- Language as written assumes ESPs at both ends of the communication link
- Guidance has been issued to allow entities to define a “demarcation point” in the instance where there is no ESP at one or both ends of the communication link, that is used to define which systems are “in scope” and which are allowed to be excluded
Compliance Implications

• What does it all mean?
  ▪ 61850 relays meet the definition of BES Cyber Asset
  ▪ 61850 devices constitute components in a BES Cyber System
  ▪ Merging Units and other ethernet switches are necessary communication components connecting the individual 61850 relays together – they are therefore part of the BES Cyber System
Compliance Implications

• What does it all mean?

  ▪ 61850 instrumentation components (e.g., CTs, PTs, sensors, actuators) are necessary for the relays to perform their functions – they are therefore part of the BES Cyber System

  ▪ 61850 relays use routable protocols for communication (e.g., TCP/IP)
    ○ Expect extensive scrutiny if asserting this is not true
    ○ Communication includes management as well as control capabilities
Compliance Implications

• What does this mean for medium impact implementations?
  ▪ Networks of 61850 devices (as BES Cyber Systems) need to be enclosed in an ESP
  ▪ An EAP would be required to manage all routable traffic to external systems
    ○ The GOOSE message exclusion does not (currently) exist for medium impact
  ▪ The CIP Standards apply to all the 61850 devices, as well as any other network-attached PCAs
  ▪ Even if there is no external routable connectivity, there are CIP Standards requirements that apply
What does this mean for low impact implementations?

- There are no ESP requirements at low impact locations
  - However, there are requirements for controlling external routable access to low impact BES Cyber Systems
- 61850 devices which communicate externally (i.e., to devices outside the station) via a routable protocol need to be analyzed for external access
  - GOOSE messaging is specifically excluded, but other communication is included
- Routable external access must be managed and controlled
- In any case, policy, security awareness, physical security, and incident response are required – even if there is no routable external access
Implementation Considerations:

- Start with a non-BES implementation, e.g., a distribution installation
  - Distribution is not NERC jurisdictional, so there are no NERC compliance implications with any actions performed
  - Work out 61850 technical implementation issues

- Treat the distribution installation as if it were (initially) a low impact installation, and apply the low impact controls
  - Develop and document necessary procedures and controls
Implementation Considerations (cont’d):

- Once comfortable, treat the distribution installation as if it were a medium impact without External Routable Connectivity requirements
  - Develop and document necessary procedures and controls
- Then, treat the distribution installation as if it were a medium impact with External Routable Connectivity
  - Develop and document necessary procedures and controls
- Finally, roll out 61850 at a BES station (low or medium)
Questions and Answers

Scott Mix, CISSP
scott.mix@nerc.net
215-853-8204