IEC 61850 in Digital Substation and Cyber security

72nd Annual Georgia Tech Protective Relaying Conference

Steven Kunsman, May 4, 2018
The digital systems

Communication services

Client-Server
- Reliable point to point sessions for central monitoring and control
- Commands, reporting, logs, file transfer,…

GOOSE
- Real-time data broadcast for station wide applications e.g. interlocking
- Binary data, indications, commands

Sampled Values (SV)
- Real-time data broadcast for collecting measurements from process
- Sampled analog values
IEC 61850: introduction to process bus
What is a sampled measured value?

- Communication interface according to IEC 61850-9-2
  - Merging and timely correlation current and voltage values from the three phases
  - Sampling or re-sampling of current and voltage values
  - Technology specific interface between NCIT/CIT and MU

**Time synchronization**

- Synchronize IEDs or other MUs when acting as time master, if required
- Receive time synchronization when acting as time slave, if required
Standardization and interoperability

Allocation of logical nodes

Station Bus

Protection IED

PTOC PDIS PBR

PTRC

TVTR TCTR XCBR

Protection IED

PTOC PDIS

PTRC

TVTR TCTR XCBR

Breaker IED

PTOC PDIS

PTRC

TVTR TCTR XCBR

with Process Bus

Merging Unit IED

hardwired
Why Digitalize Substations?
Replacing 1000’s copper wires with a few communications fiber

Digitalization Benefits
— Improved safety
— Improved reliability
— Improved resiliency
— Reduced CAPEX
— Reduced OPEX
— Reduced footprint
— Information availability
— System self-supervised

Ethernet in the switchyard
Risk or benefit?
Digitalization Enables Asset Performance Management
Real time information flow for continuous risk-based optimization

- Expert models
- Statistical models

Continuous optimization and improvement

Enterprise asset and work management

Advanced operational business intelligence

Data analysis

Fleet Management

Connect / collect
Analyze / predict
Inform
Track
Act
Business Challenge: The Ultimate Goal
Balancing Reliability and Cybersecurity

- Safe & Secure delivery of Reliable Power
- Air gap is not a solution
- Information flow critical for today / tomorrow’s successful grid management

Let’s not forget: The “R” in NERC stands for Reliability!
Growing Cybersecurity Threats

Unauthorized access and attacks

Attacks on utilities

Ukraine I – Dec 2015 (Sandworm)
— Spear phishing, BlackEnergy, KillDisk
Ukraine II – Dec 2016 (Electrum)
— Industroyer/CrashOverride

Challenge: Information Sharing
Incident response / forensics
— Collaboration between agencies, utilities and manufacturers essential

E-ISAC-SANS Report on Ukraine I
E-ISAC-SANS Report on Ukraine II
Cybersecurity Subcommittee (S0) Scope – Newly formed in 2017

Studying and reviewing engineering (including information technology and operation technology), operational, and testing aspects of cybersecurity related to the Electric Power System.

– Scope includes IEEE cyber security for the entire electric power system

Developing and maintaining related standards, recommended practices and guides for such aspects

Coordinating with other technical committees, groups, societies and associations as required

Preparing and arranging for publication technical reports related to the Subcommittee’s scope

Subcommittee Officers

Chair: Steven Kunsman
Vice-chair: James Bougie
Secretary: Farel Becker

For additional information contact: steven.a.kunsman@us.abb.com
Webpage: http://sites.ieee.org/pes-pscc/cybersecurity-subcommittee-s0/
| **WG S1**: IEEE 1686 Standard for Intelligent Electronic Devices Cybersecurity Capabilities |
| **WG S2**: IEEE P1711.1 Serial SCADA Protection Protocol (SSPP) |
| **WG S3**: IEEE P2030.102.1 Standard for Interoperability of IPSEC Utilized within Utility Control Systems |
| **WG S4**: IEEE P1711.2 Trial-Use Standard for Secure SCADA Communications Protocol (SSCP) |
| **WG S5**: IEEE C37.240 Cybersecurity Requirements for Power System Automation, Protection and Control Systems |
| **TF S6**: IoT for connected home - communication and cybersecurity requirements |
| **TF S7**: Electrical Power System Cyber Device Function Numbers, Acronyms, and Designations |
| **TF S8**: Testing Power System Cybersecurity Controls |
### IEEE PSCC CYBERSECURITY SUBCOMMITTEE

S0 Study Group Activity for May 2018 Meeting

<table>
<thead>
<tr>
<th><strong>SG S9</strong>: Utility IT-OT Cybersecurity challenges in roles and terminology</th>
</tr>
</thead>
<tbody>
<tr>
<td>A core theme from the IEEE Cybersecurity workshop was the utility need for IT and OT collaboration to address cybersecurity differences (culture, application, perspective and terminology). Assess the IT-OT challenge in Utility Cybersecurity roles and create a report to assist in building organizational understanding and collaboration.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>SG S10</strong>: Utility &amp; municipality challenges on understanding cybersecurity standards</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assess the challenge in utilities &amp; municipalities with limited resources on the applicability and relevance of the cybersecurity standards and create a report to assist summarizing the relevant cybersecurity standards.</td>
</tr>
</tbody>
</table>
Applicability of cybersecurity standards and regulations

Building Cybersecurity Defense-in-Depth

- IEEE C37.240
- IEC 62443
- IEEE 1711.2
- IEC 62351
- IEEE 1686
- NERC CIP
Cybersecurity
Process bus and NERC CIP

Security architecture

NERC CIP v5

- Electronic Security Perimeter is no longer bound by 6 walls
- Routable protocol allowed inside the chain link fence
- BES Substations are Medium or Low classification
- Single factor authentication
- IEEE C37.240 to address:
  - Technical standard for cyber security requirements for communications outside the control house but inside the substation fence