NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Emerging Technology Roundtable – Substation Automation / IEC 61850

November 15-16, 2016

RELIABILITY | ACCOUNTABILITY




Agenda - Emerging Technology Roundtable

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

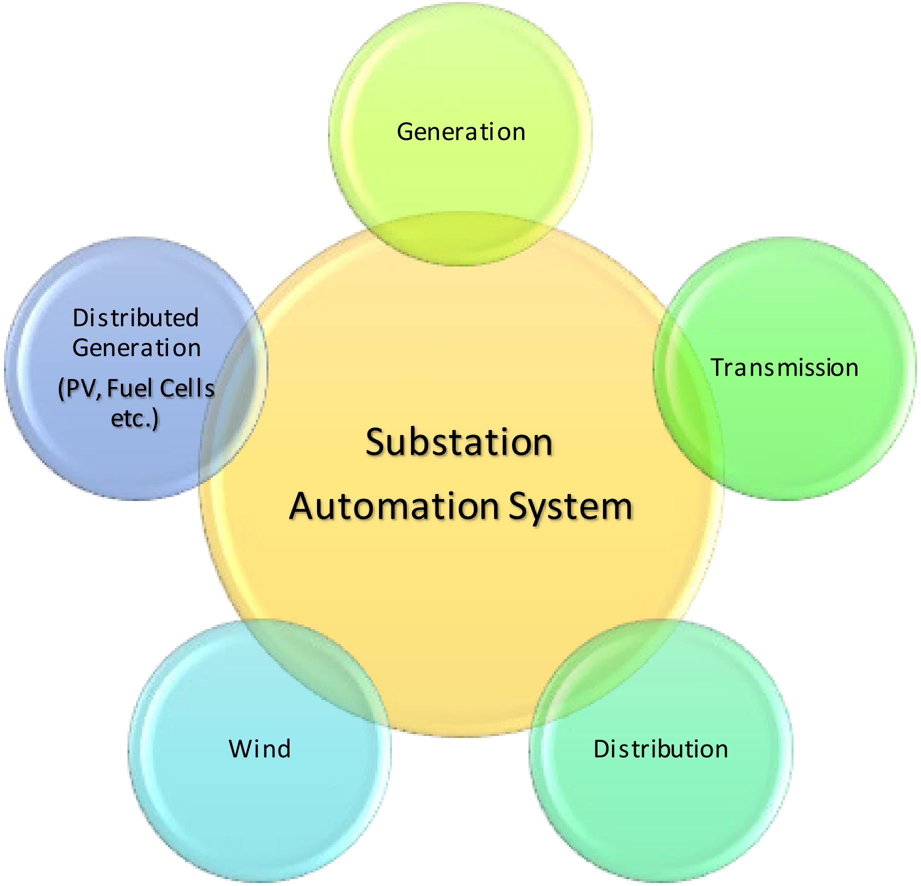
Herbert Falk

Senior Solutions Architect

Systems Integration Specialists Company

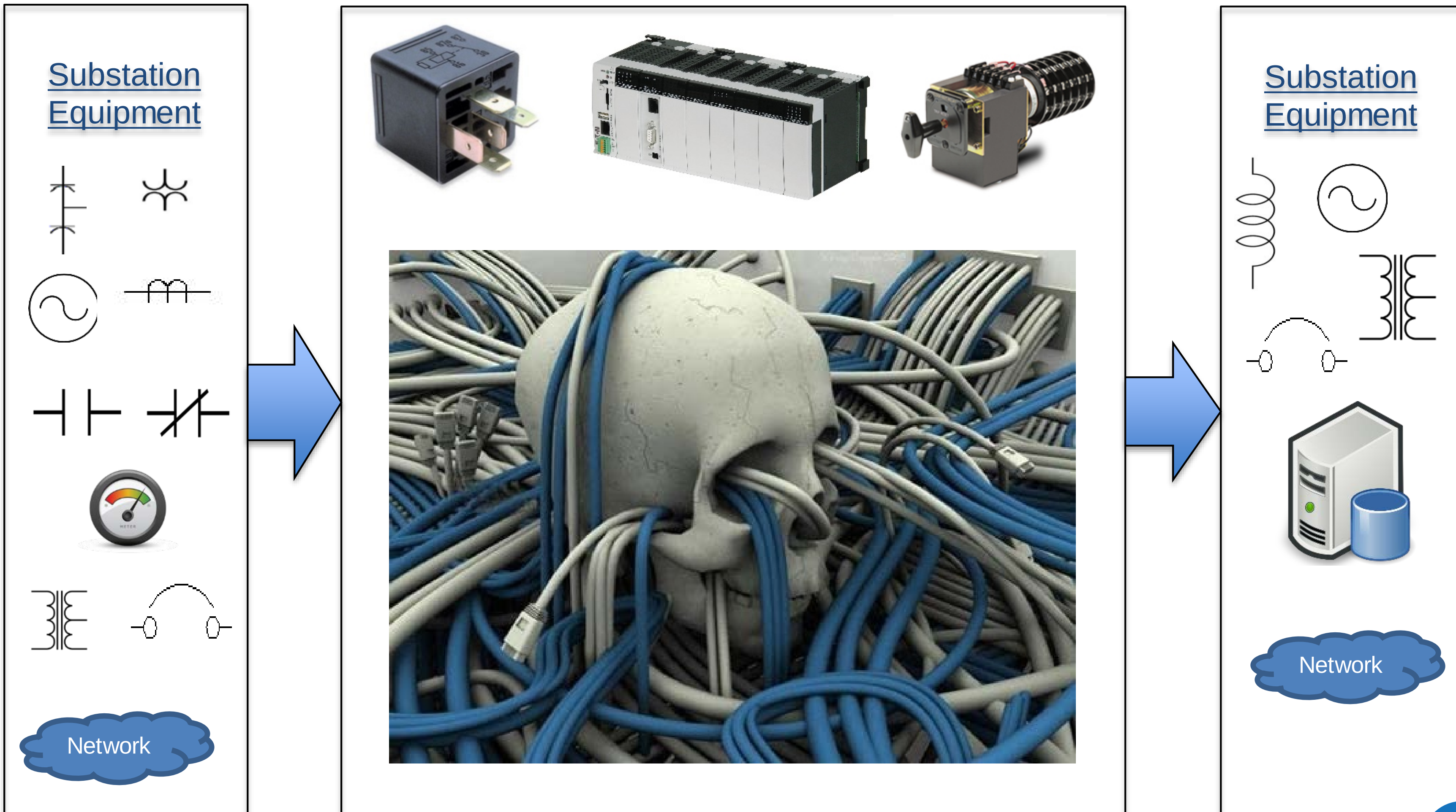
Agenda

- What is IEC 61850?
- What applications do IEC 61850 cover?
- Pros-Cons of IEC 61850 based Substation Automation System
- Architectures
- Time synchronization
- Cyber Security

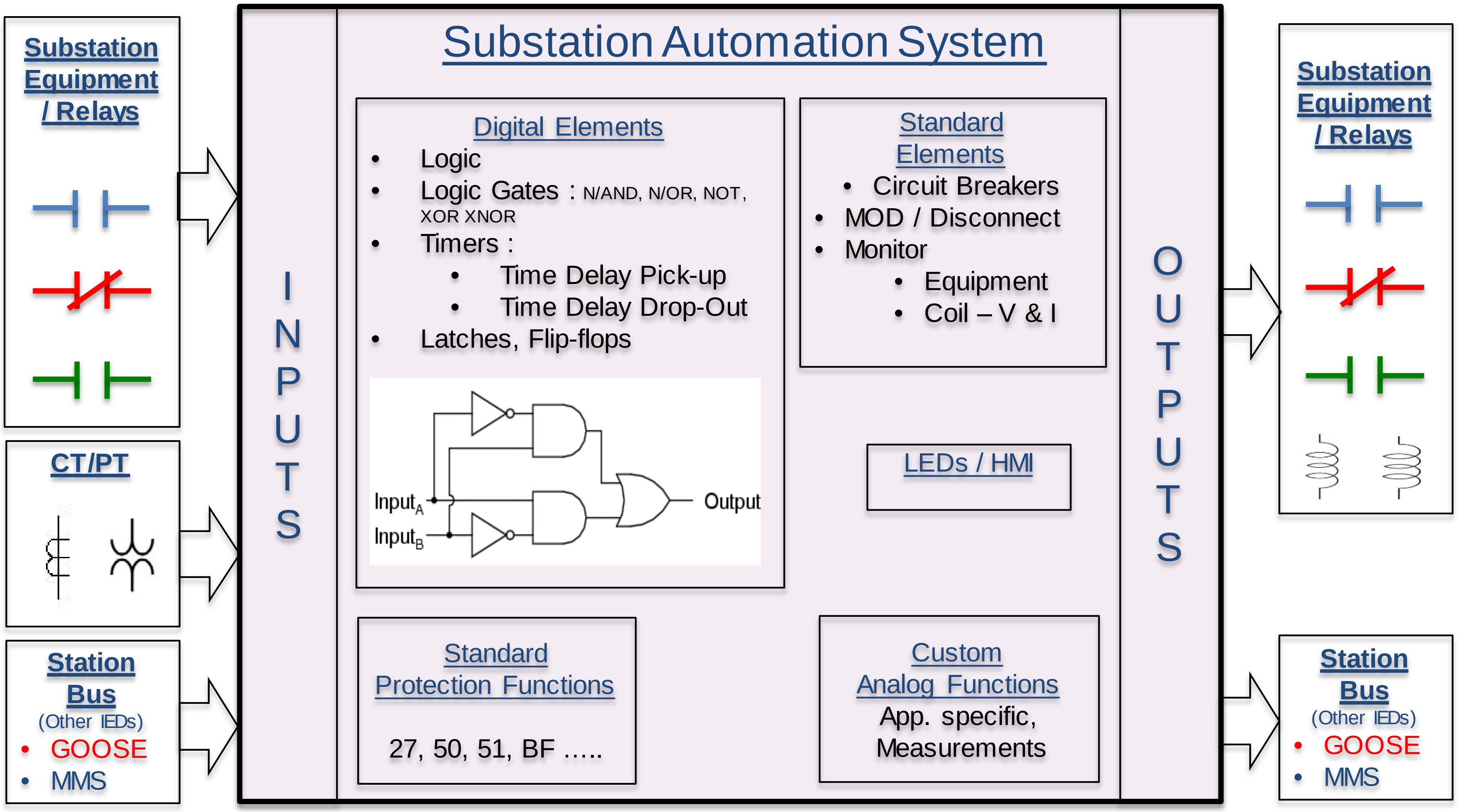


- Perform functions necessary to aid in efficient generation, transmission, distribution of power

General Architecture of Substation Automation System



IEC 61850 based Substation Automation System



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

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

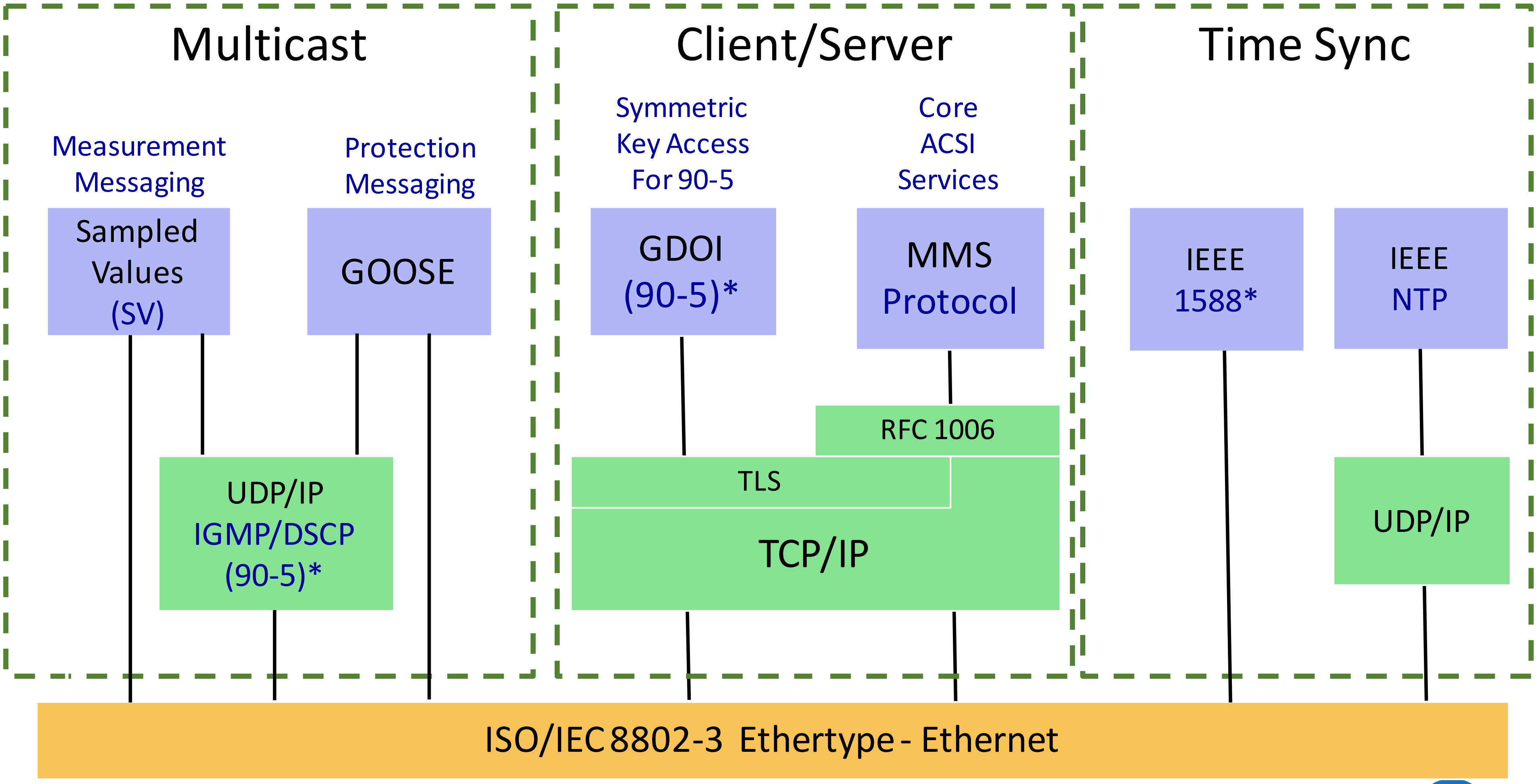
SPS class					
Attribute Name	**Attribute Type**	**FC**	**TrgOp**	**Value/Value Range**	**M/O/C**
DataName	Inherited from Data Class (see IEC 61850-7-2)				
DataAttribute					
				status	
stVal	BOOLEAN	ST	dchg	TRUE | FALSE	M
q	Quality	ST	qchg		M
t	TimeStamp	ST			M
				substitution	
subEna	BOOLEAN	SV			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_DLNDA_M
cdcName	VISIBLE STRING255	EX			AC_DLNDA_M
dataNs	VISIBLE STRING255	EX			AC_DLN_M
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



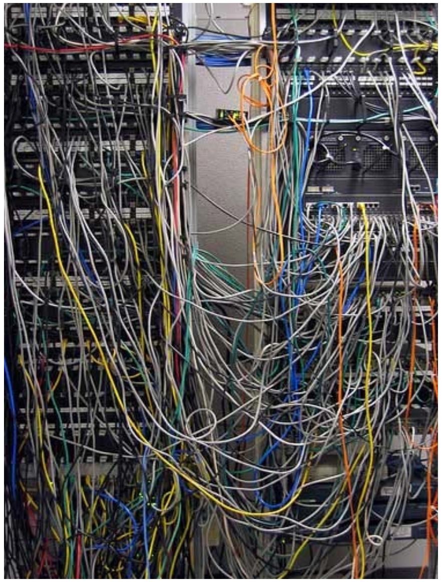
* - Added in Edition 2 Amendment

IEC 61850 Communication Types

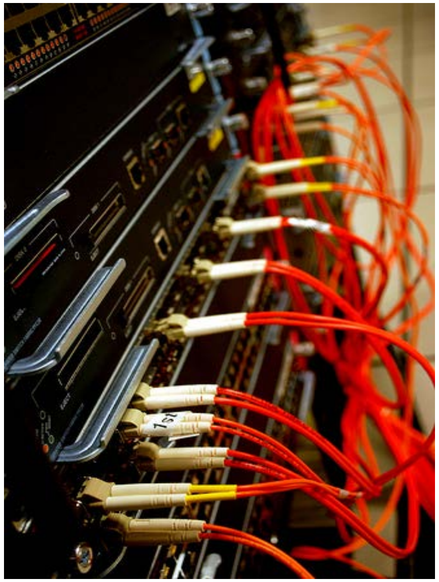
- ❑ Multicast (Publisher ← → Subscriber)
    - Similar to Broadcast
    - GOOSE, SV
  - ❖ Applications:
    - Protection, Monitoring, Recording, Metering..

- ❑ Client – Server
    - Security possible through IEC-62351
      - Encryption, User Authentication, Access Control ...
  - ❖ Applications
    - Control

Traditional P&C System



IEC-61850 based P&C System



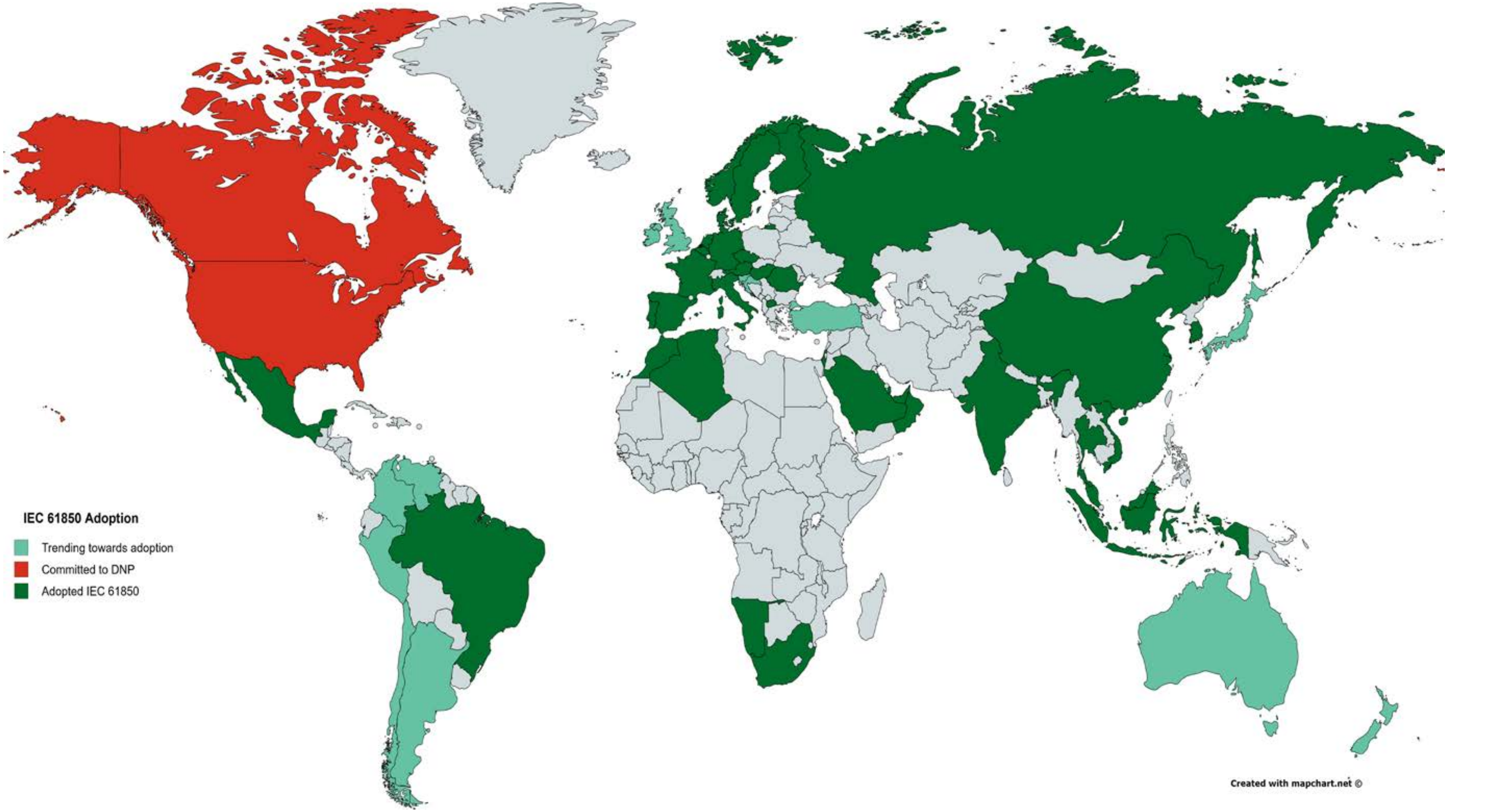
Advantages of IEC 61850 based SAS

- 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 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

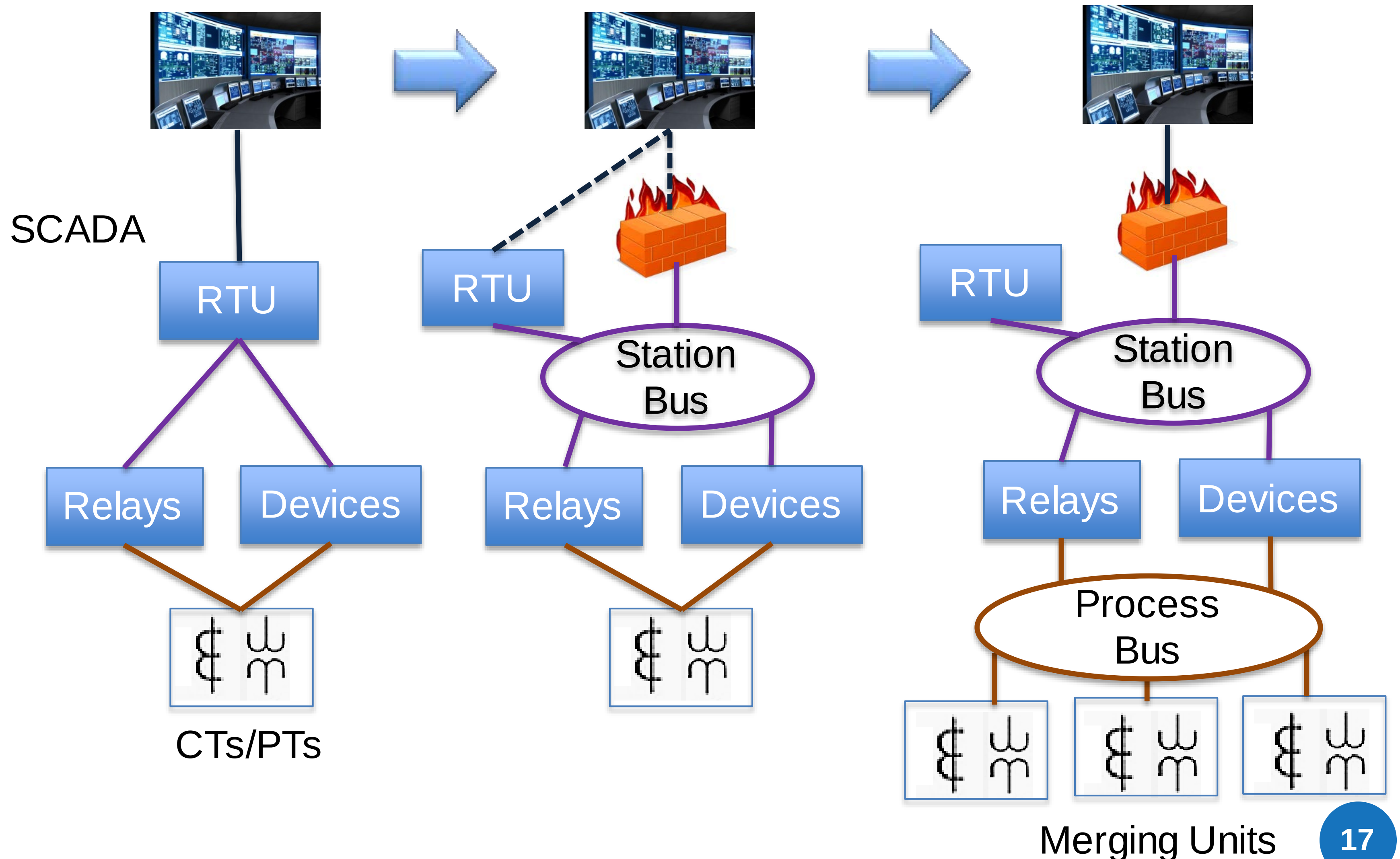
- Substation-to-Substation (IEC/TR 61850-90-1) communication typically used for protection control
  - SCE's, PG&E, SRP, Toronto Airport are examples

- Secure Synchrophasor for WAM**PAC**
  - 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



Station Bus – Performance and Resiliency Considerations

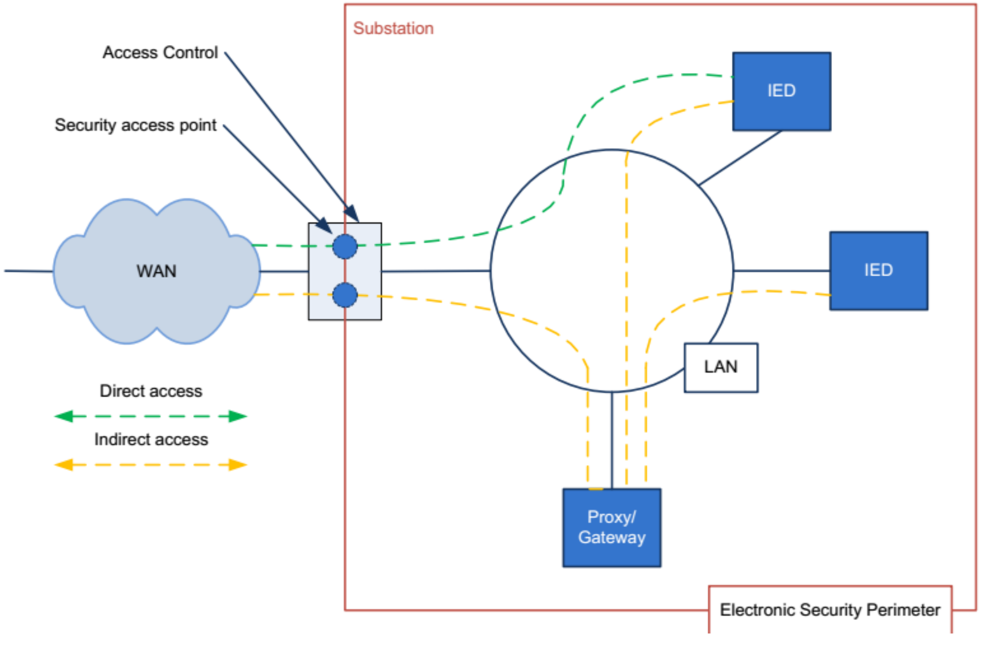
- Performance
  - SCADA traffic
    - "Low" speed — Network Resiliency: RSTP
  - Automation
    - Combination of "Low" and "Medium" (<20 msec) speed — Network Resiliency: HSR or PRP
    - Utilizes GOOSE
  - Protection (3-6 msec) — Network Resiliency: HSR or PRP
    Utilizes GOOSE
  - Time Sync Accuracy — 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

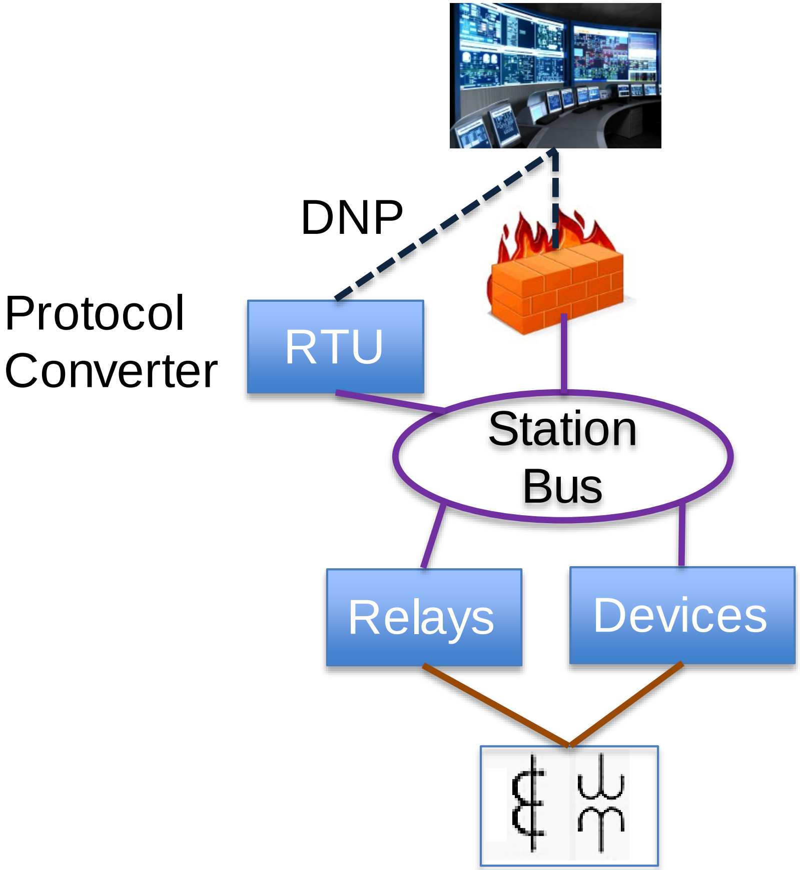
- Performance
  - “High” Speed — Network Resiliency: HSR or PRP
  - Time Sync Accuracy — Resiliency is needed
    - Important for post mortem analysis
    - Important for geographically disperse automation (e.g. out-of-step/synchrophasors)

Substation to Control Center (IEC 61850-90-2)

- Use Cases
  - Telecontrol (SCADA)
  - Synchrophasor
  - Disturbance
  - Counting
  - Power Quality
  - Asset/Condition Based Maintenance
  - Configuration

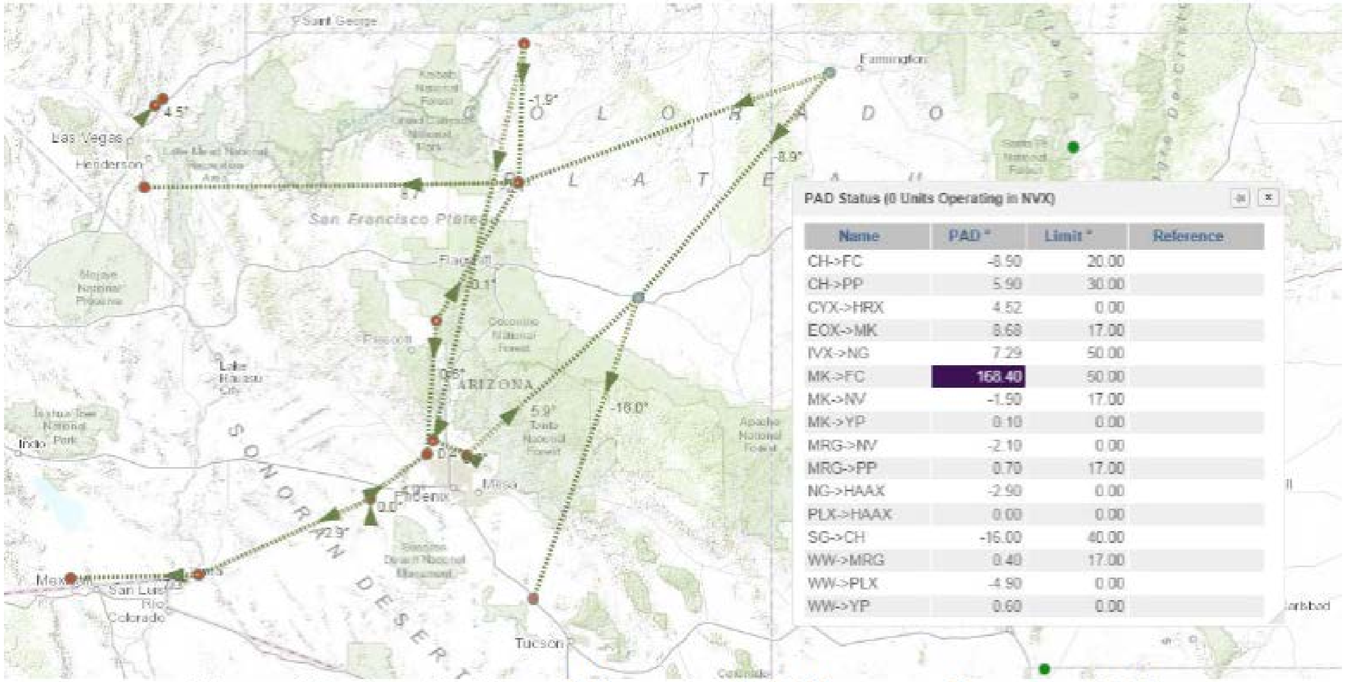


Telecontrol (SCADA)



Newton-Evans reports very low penetration of IEC 61850 in North America.

Synchrophasors



Name	PAD °	Limit °	Reference
CH->FC	-8.50	20.00	
CH->PP	5.90	30.00	
CYX->HRX	4.52	0.00	
EOX->MK	8.68	17.00	
IVX->NG	7.29	50.00	
MK->FC	168.40	50.00	
MK->NV	-1.50	17.00	
MK->YP	0.10	0.00	
MRG->NV	-2.10	0.00	
MRG->PP	0.70	17.00	
NG->HAAX	-2.90	0.00	
PLX->HAAX	0.00	0.00	
SG->CH	-16.00	40.00	
WW->MRG	0.40	17.00	
WW->PLX	-4.90	0.00	
WW->YP	0.60	0.00	

Figure 11: Visualization of Phase Angle Differences [Source: APS]

- Routable IEC 61850 Secure Sampled Values was developed for synchrophasors
- Time Sync accuracy and resiliency is typically needed

Substation-to-Substation

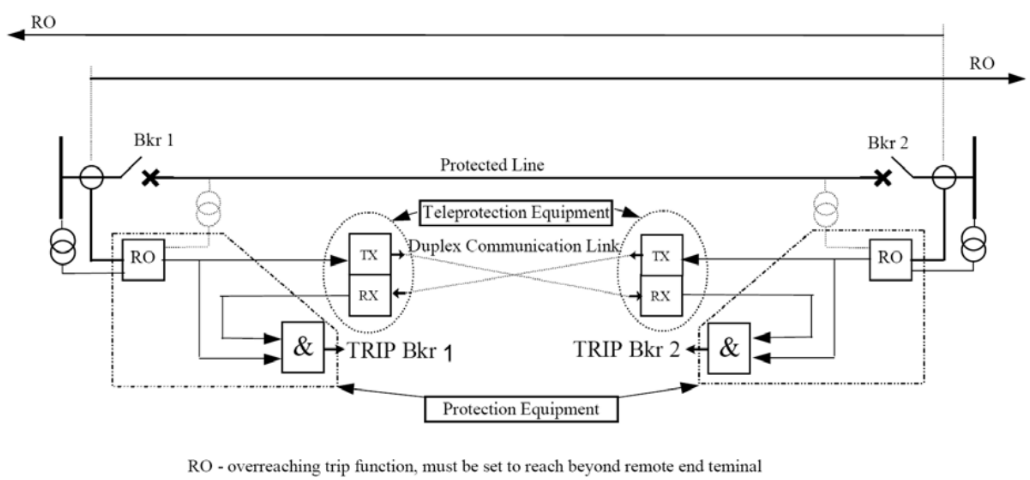


Figure 1 – Distance line protection with permissive overreach tele-protection scheme [1]

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

Substation-to-Substation: Example

4 Overall architecture of a typical Centralized Remedial Action Scheme (C-RAS)

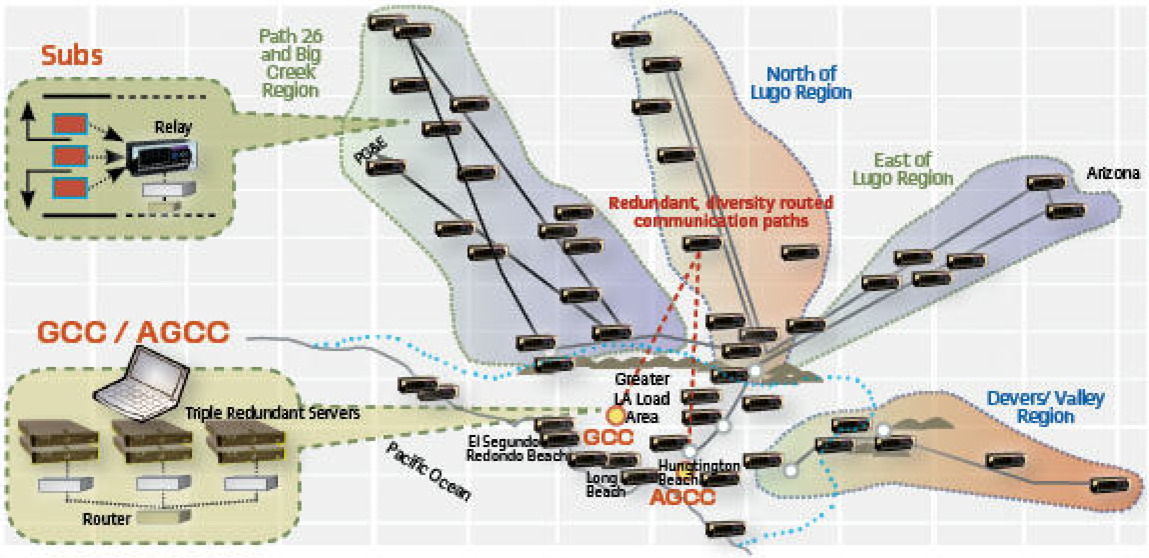


table 1 Synchrophasor versus R-GOOSE

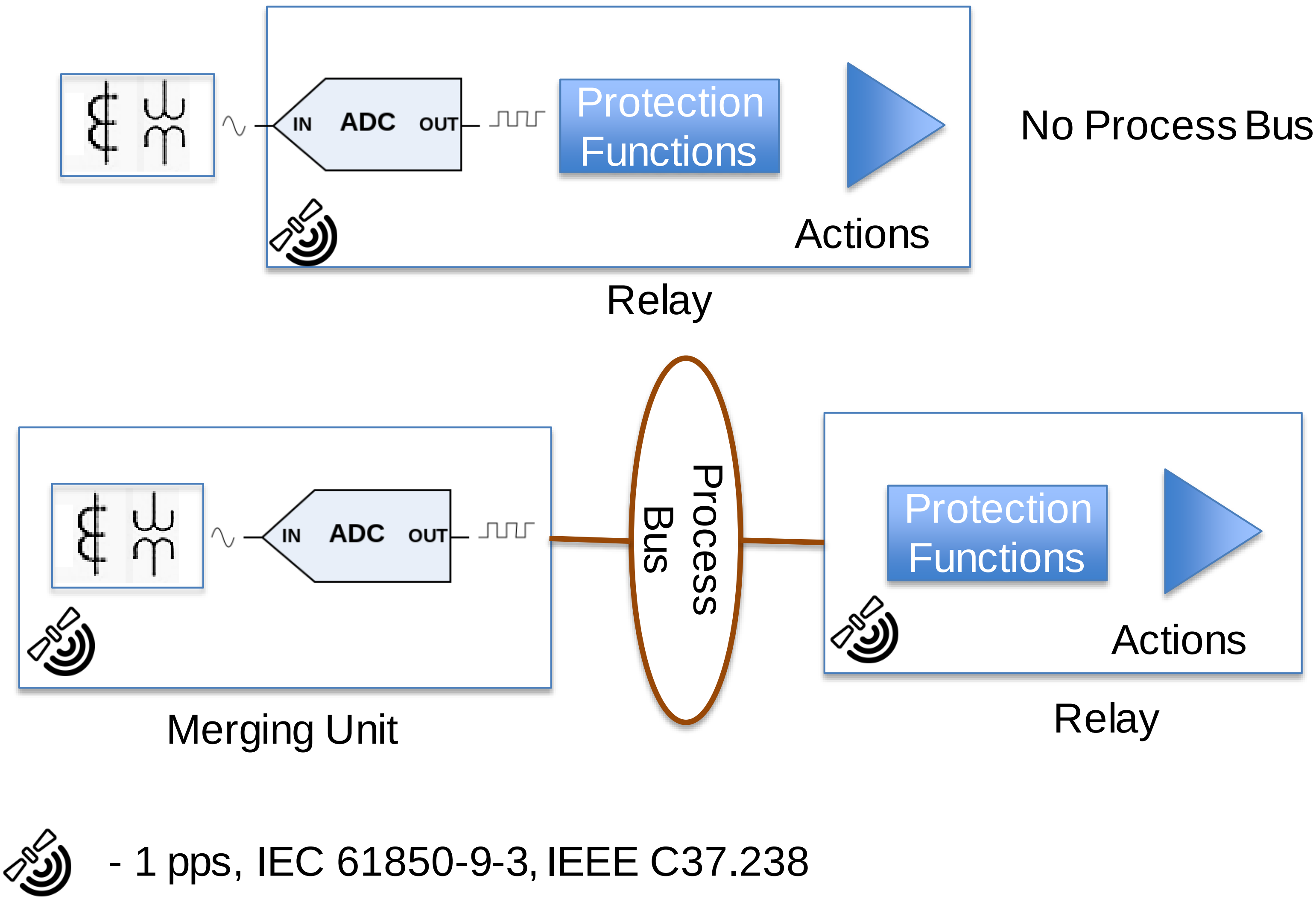
Parameters	Synchrophasors	R-GOOSE
Publications	IEEE C37.118.1/.2 :2012	IEC TR 61850-90-5 :2012
Communication	Client/Server (IP Unicast)	Publisher/Subscriber (IP Multicast)
Data transmission	Specified rate, 1Hz to 120 Hz	Event-driven (1-2 Hz for no event; retransmission for events)
Data items	Synchrophasors, Analog, Digital	Analog and Digital (status)
Security	No	Key Distribution Center (KDC)
Priority	Regular (due to high data rate)	Higher (Event driven)
Networks	Regular IP/Layer-3 Router	IP/Layer-3 Router with IGMPv3 (firewall to support as well)
Configuration	CFG frames (CFG-1, 2)	ICD, CID files; GET services

table 2 Synchrophasor and R-GOOSE comparison on communication

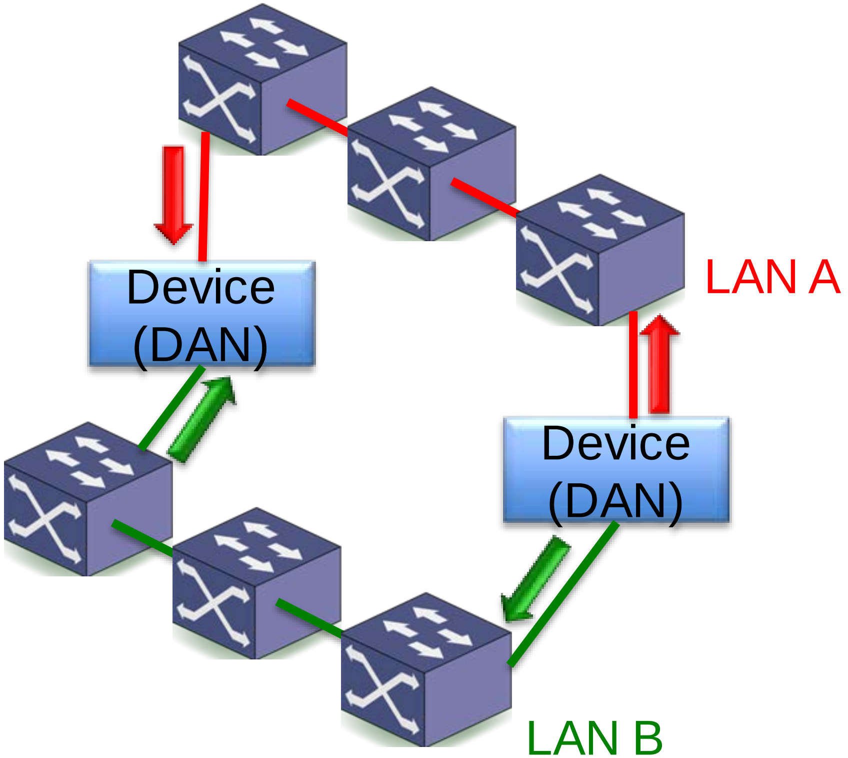
Parameters	Synchrophasors	R-GOOSE
Frame size	100 Byte	100 Byte
Date rate	30 frames/sec	5 frames/sec (worst case-1 event per second per device)
Number of devices transmitting	100 devices	100 devices
Byte Per Second over network	100*30*100=300000 Bytes/sec	100*5*100=50000 Bytes/sec (worst case)
Bandwidth requirements	300000*8=2.4Mbps	50000*8=0.4Mbps (worst case)
Number of locations/devices data received	1	Many (IP multicast)
Storage requirements per Year	300000 *3600*8760= 9.4 Tera Bytes	50000*3600*8760= 1.6 Tera Bytes (worst case)
Typical performance requirements	100 milliseconds to few seconds	<10 ms

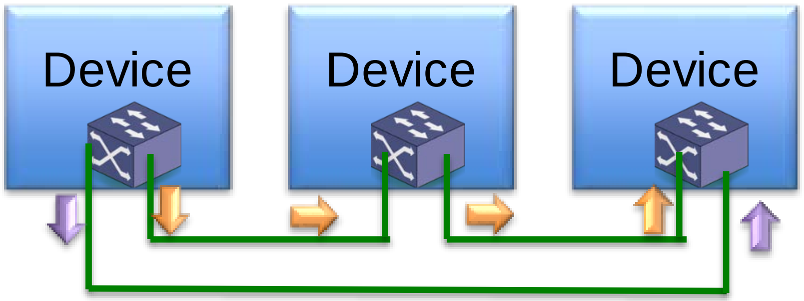
Information courtesy of pacworld. Article can be found at:
http://www.pacw.org/issue/june_2016_issue/secured_routable_goose_mechanism.html

Sampled Values for CT/PT sharing (Merging Units)



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

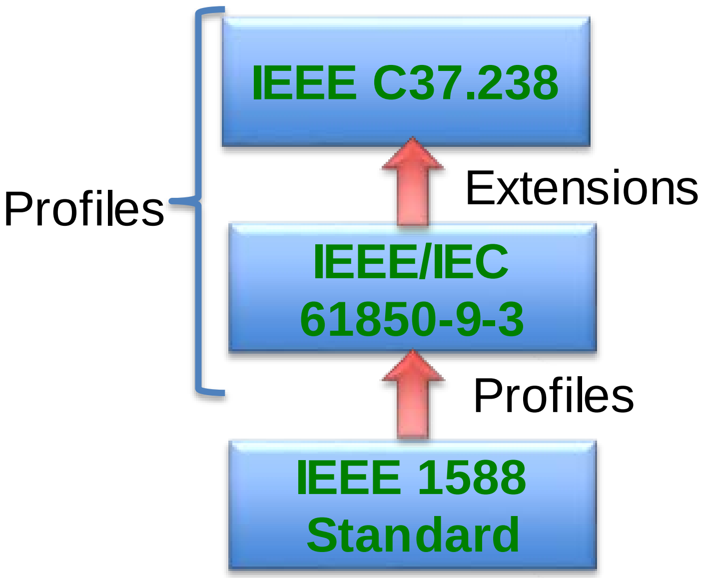
TimeStamp is UTC Time down to 60 nsec. Similar format to NTP except for Time Quality (last 8 bits of fractions of second)

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

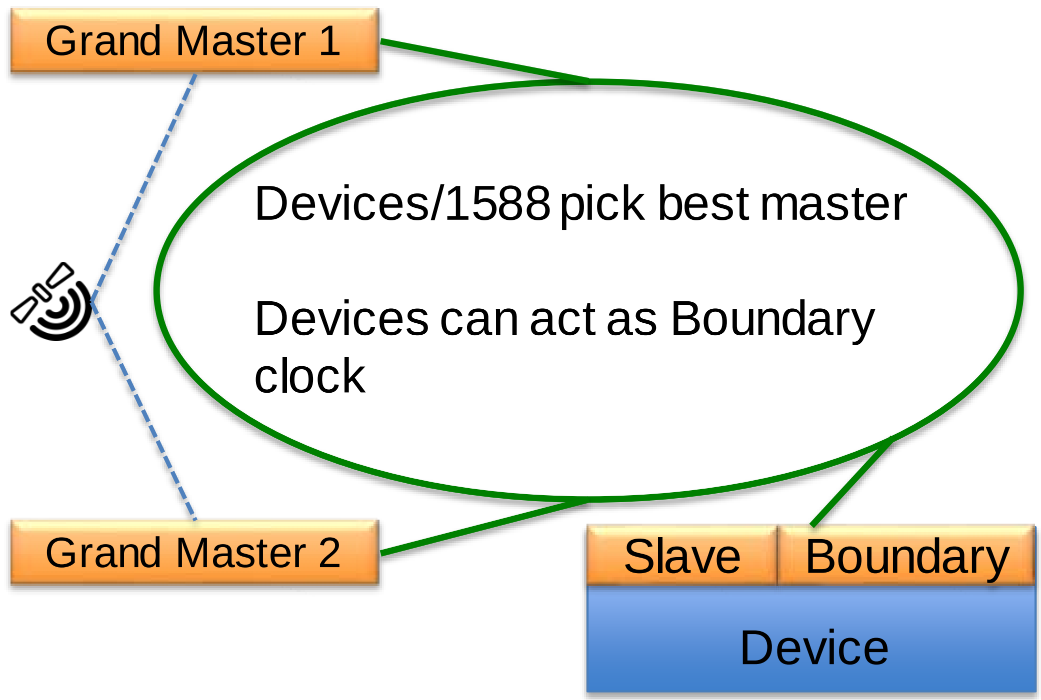
- Leap Seconds Known (TRUE)/ Leap second being processed (FALSE)
  Clock Not Synchronized
- Clock Failure (for internal clock failure)
- Time Accuracy (may change depending upon internal or source drift)

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.

IEC 61850 and Time Synchronization: 1588



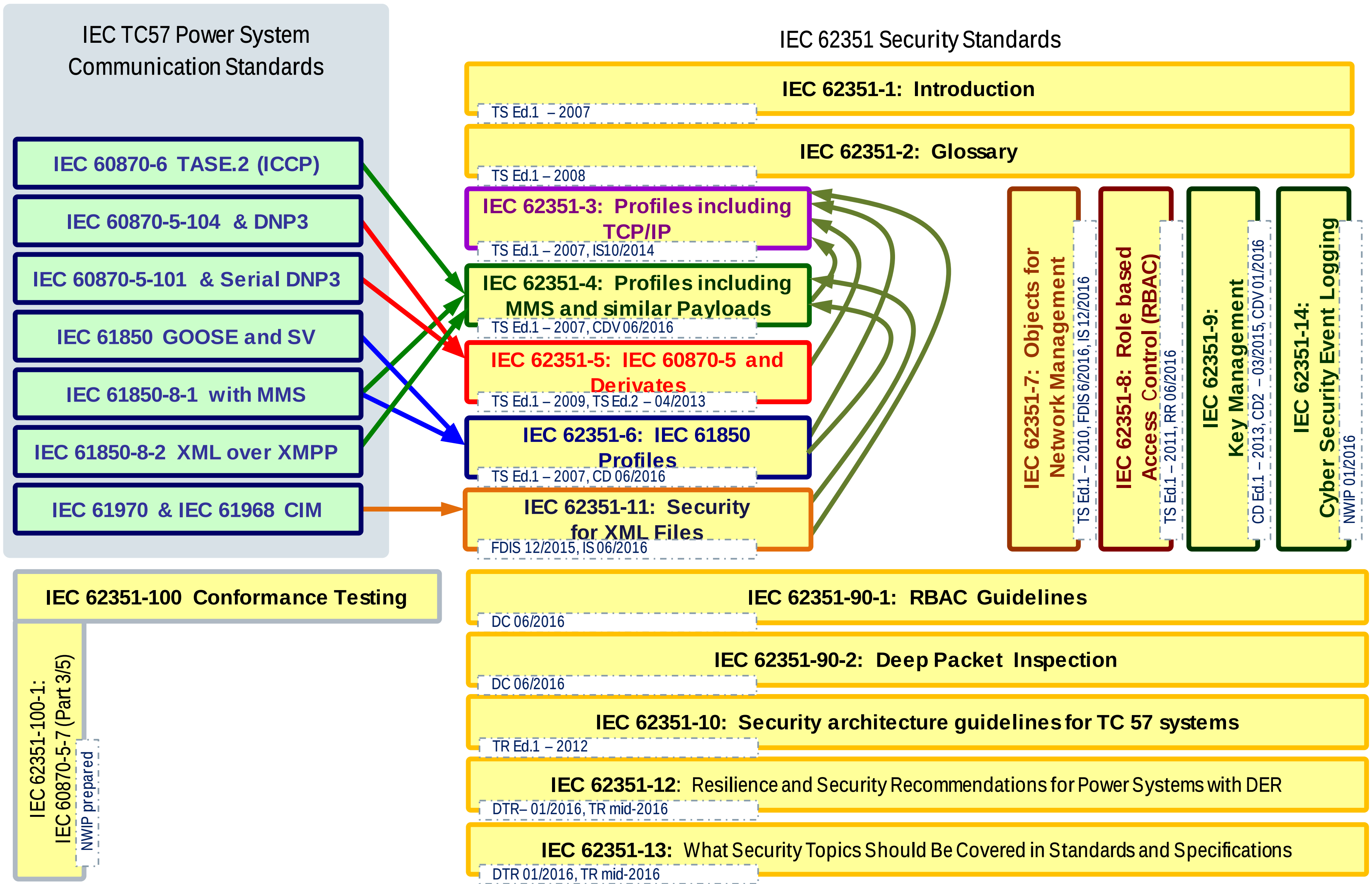
Time Synchronization Resiliency



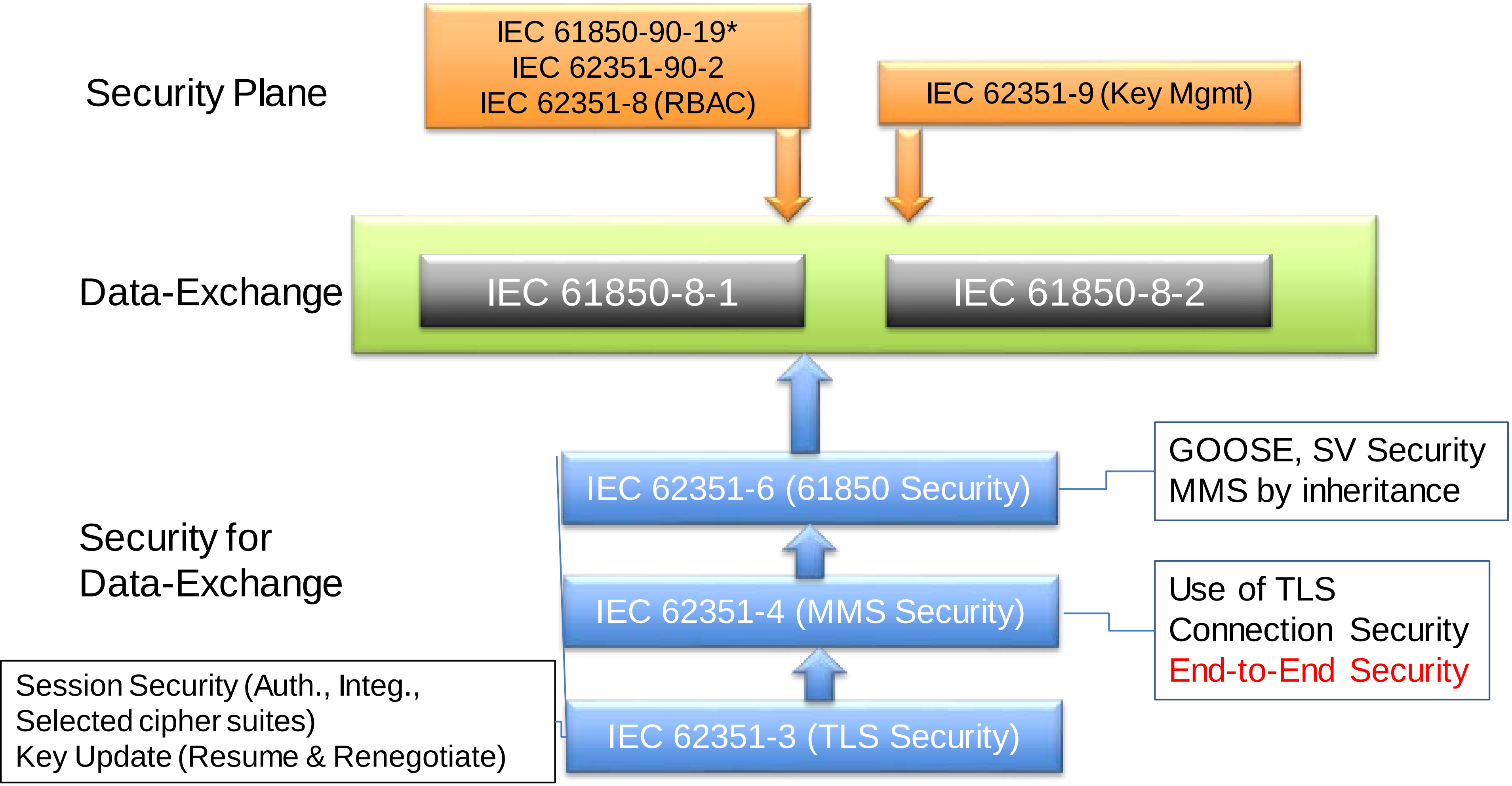
Network fault tolerance/resiliency provided by HSR or PRP

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

Mapping of TC57



IEC 61850 Security: Client/Server



IEC 61850 Security: Client/Server RBAC

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

Value	Right / Role	VIEW	READ	DATASET	REPORTING	FILEREAD	FILEWRITE	FILEMNGT	CONTROL	CONFIG	SETTINGGROUP	SECURITY
<0>	VIEWER	X			X							
<1>	OPERATOR	X	X		X				X			
<2>	ENGINEER	X	X	X	X		X	X		X		
<3>	INSTALLER	X	X		X		X			X		
<4>	SECADM	X	X	X			X	X	X	X	X	X
<5>	SECAUD	X	X		X	X						
<6>	RBACMNT	X	X					X		X	X	
<7...32767>	Reserved	For future use of IEC defined roles.										
<-32768 .. -1>	Private	Defined by external agreement. Not guaranteed to be interoperable.										

RBAC infrastructure allows:

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

IEC 61850 Security: GOOSE and SV

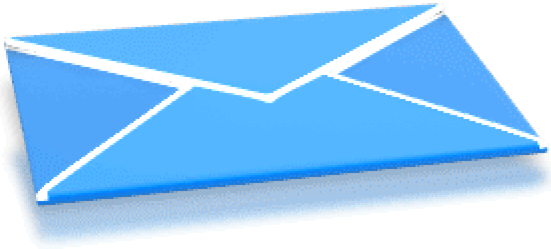
	GOOSE		SV for CT/PT		Synchrophasors
	L2	UDP/IP	L2	UDP/IP	SV over UDP/IP
Authentication	x	x	x	x	x
Tamper Detection	x	x	x	x	x
Confidentiality	x	x	Not Suggested	Not Suggested	x

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

UCA International Users Group		Provides: • Members with access to draft standards • Supports user feedback and answering questions • Sponsoring of the 4th IEC 61850 IOP • Other benefits
UCA International Users Group	IEC 61850 Boot Camp	Co-located with the 2017 IEC 61850 IOP. Scheduled October 12-13, 2017 in New Orleans.
UCA International Users Group	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

SOUTHERN CALIFORNIA EDISON®
An EDISON INTERNATIONAL® Company

61850 Business Drivers

Digital Re-Invention at Southern California Edison

Jeff Gooding
IT Principal Manager
Enterprise Architecture & Strategy

November, 2016

SOUTHERN CALIFORNIA EDISON®
An EDISON INTERNATIONAL® Company

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

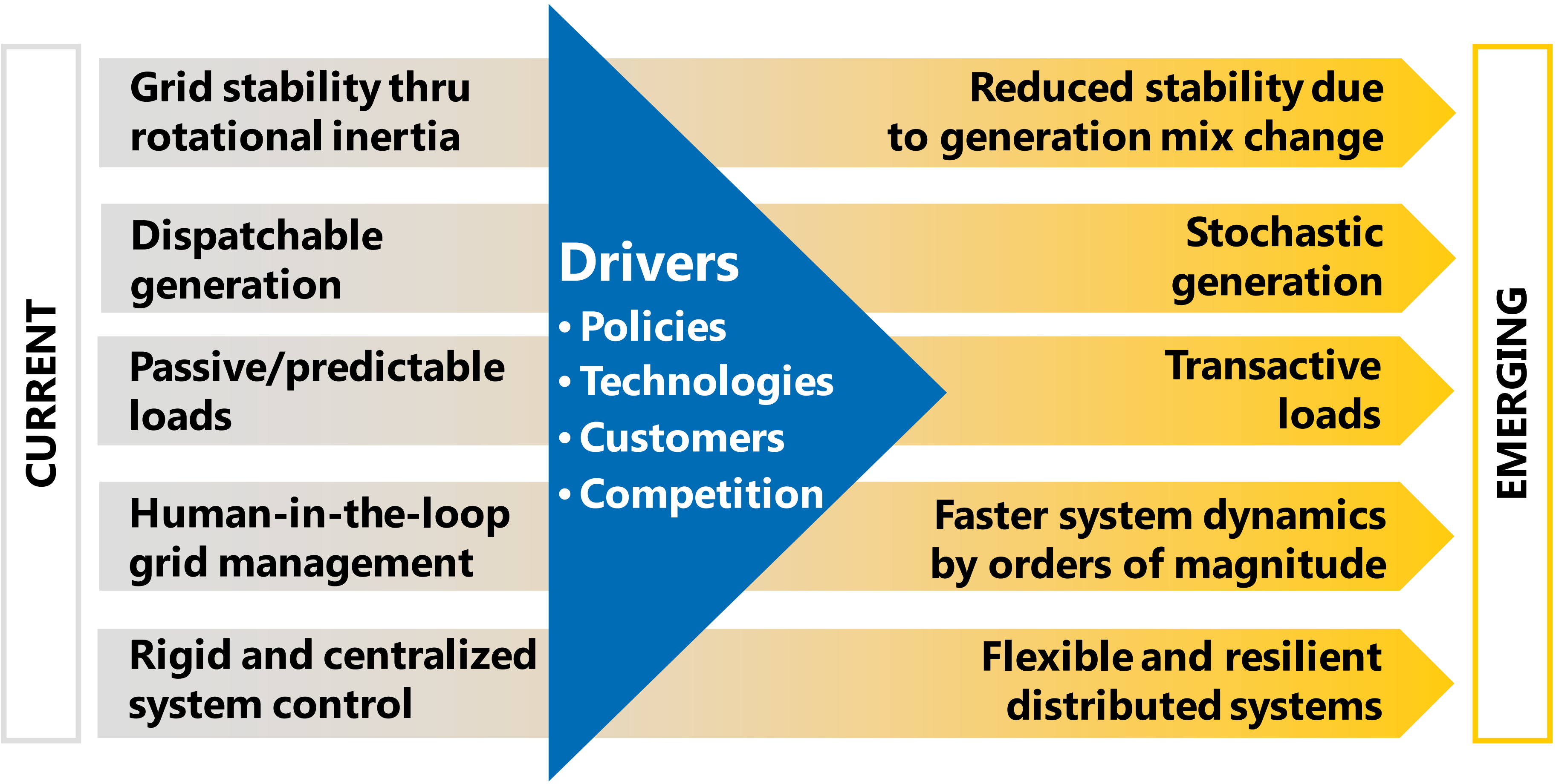
Customers

- 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



…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

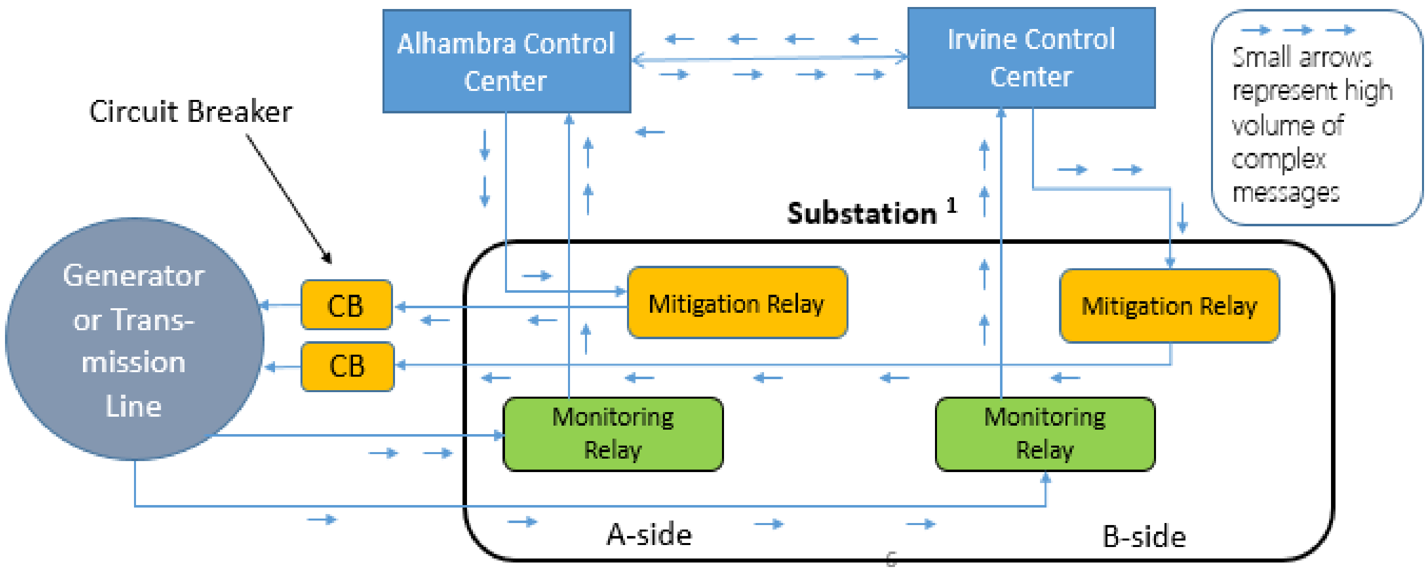
To make the right decisions at the right time

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

Courtesy DOD office of CIO

C-RAS Simplified System Diagram



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

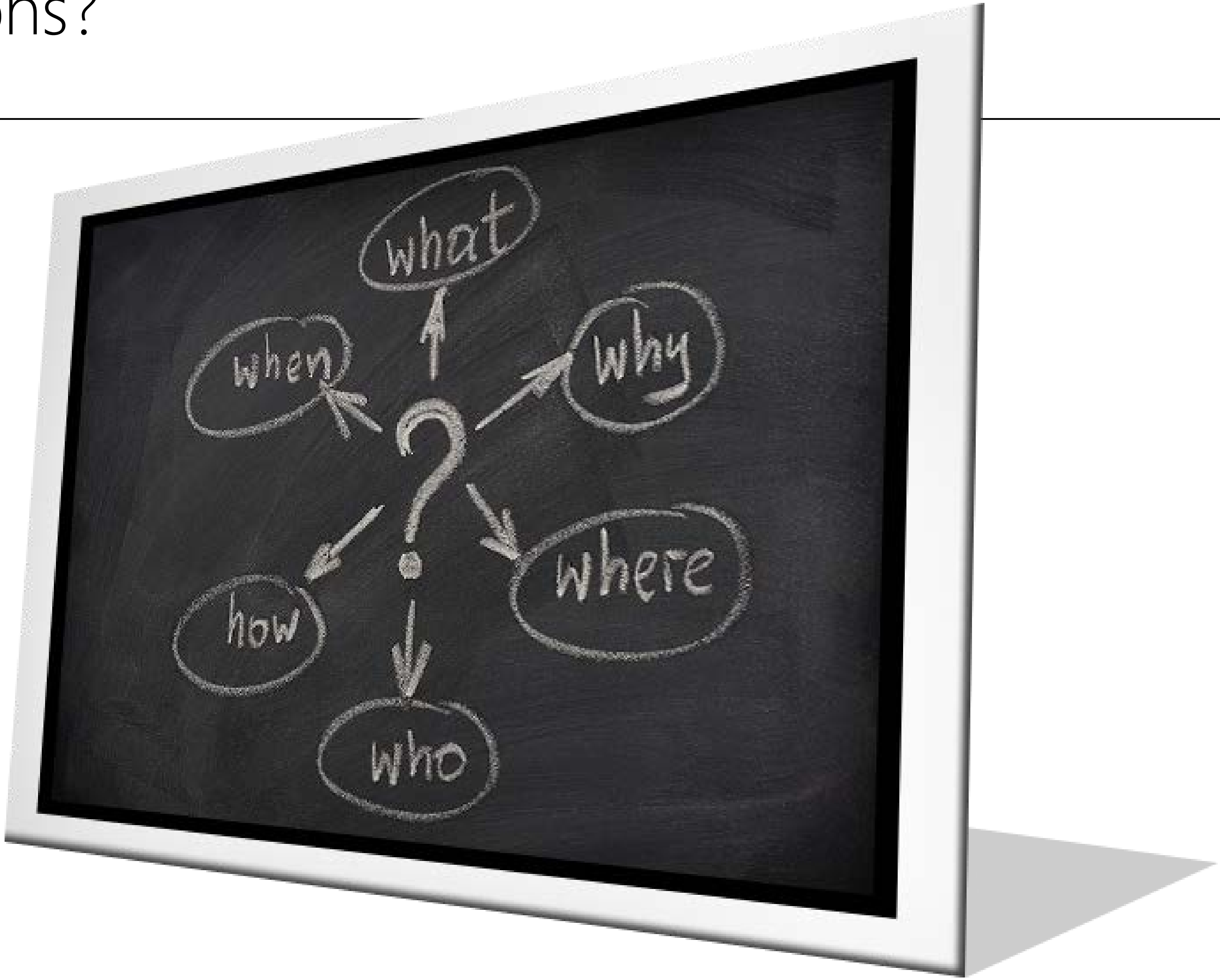
Common Substation Platform:

- 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?



SOUTHERN CALIFORNIA EDISON
An EDISON INTERNATIONAL® Company

IEC 61850
Next Gen Substation Automation

Chan Wong

cwong@entergy.com

Entergy

Transmission

Engineering

WE POWER LIFE℠

Core Team

Transmission Engineering
Willie Wilson
Erik Guillot
Mark Bruckner
Tom Lanigan

Design Basis
Chan Wong

Grid
David Zulauf (Supv)
Bruce Leagan (Supv)
Allen Clark
Brent Vickers
Wesley Earl
Mike Mcdonough

Design
Chris Taylor (Supv)
David Daigle (Supv)
Josh Bonfiglio
Scott Waguespack
Jerry Berndsen

Settings
Cat Wong (Supv)
Tu Nguyen
David Nguyen
Paul Scanlon
Mike Walcott
Shreyas Pawale

OIT
Matt Briggs
George Raesis
Becky Montgomery
Robert Lewis
Chris Crayton

While the project moving forward, we will be encourage more Entergy family members to join us for this venture

Collaborators

EPRI | ELECTRIC POWER RESEARCH INSTITUTE

ABB

SEL

SIEMENS

ALSTOM

SUBNET SOLUTIONS INC.

CISCO

doble®

OMICRON

NovaTech.

HIRSCHMANN
A BELDEN BRAND

CONDUX

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

iS5 COMMUNICATIONS
SERVICES • SUPPORT • SECURITY • SOLUTIONS • SYSTEMS

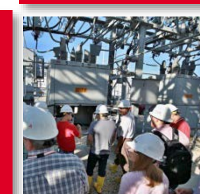
OMNI

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
    - o Bundle of copper wires replaced by fiber optic cable
    - o 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

Copper Wires

Conventional cabling
Cables: 768
Conductors: 4500
Terminations: 9000

Test/Debug – Labor intensive

Maintenance – Drawings up to date?

Reliability – Many connections

Digital Communications

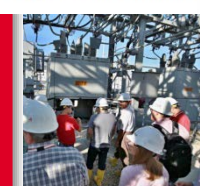
Digital Communications
Cables: 256
Conductors: 1500
Terminations: 3000

Test/Debug – Easier to test/debug using digital tools

Maintenance – Digital record of connections and much simpler wiring improves maintenance

Reliability – Less connections and units to fail improves reliability (receive digital notification of an issue)

Entergy Transmission Engineering



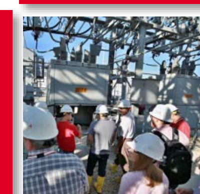
WE POWER LIFE℠

Current system with Copper wires

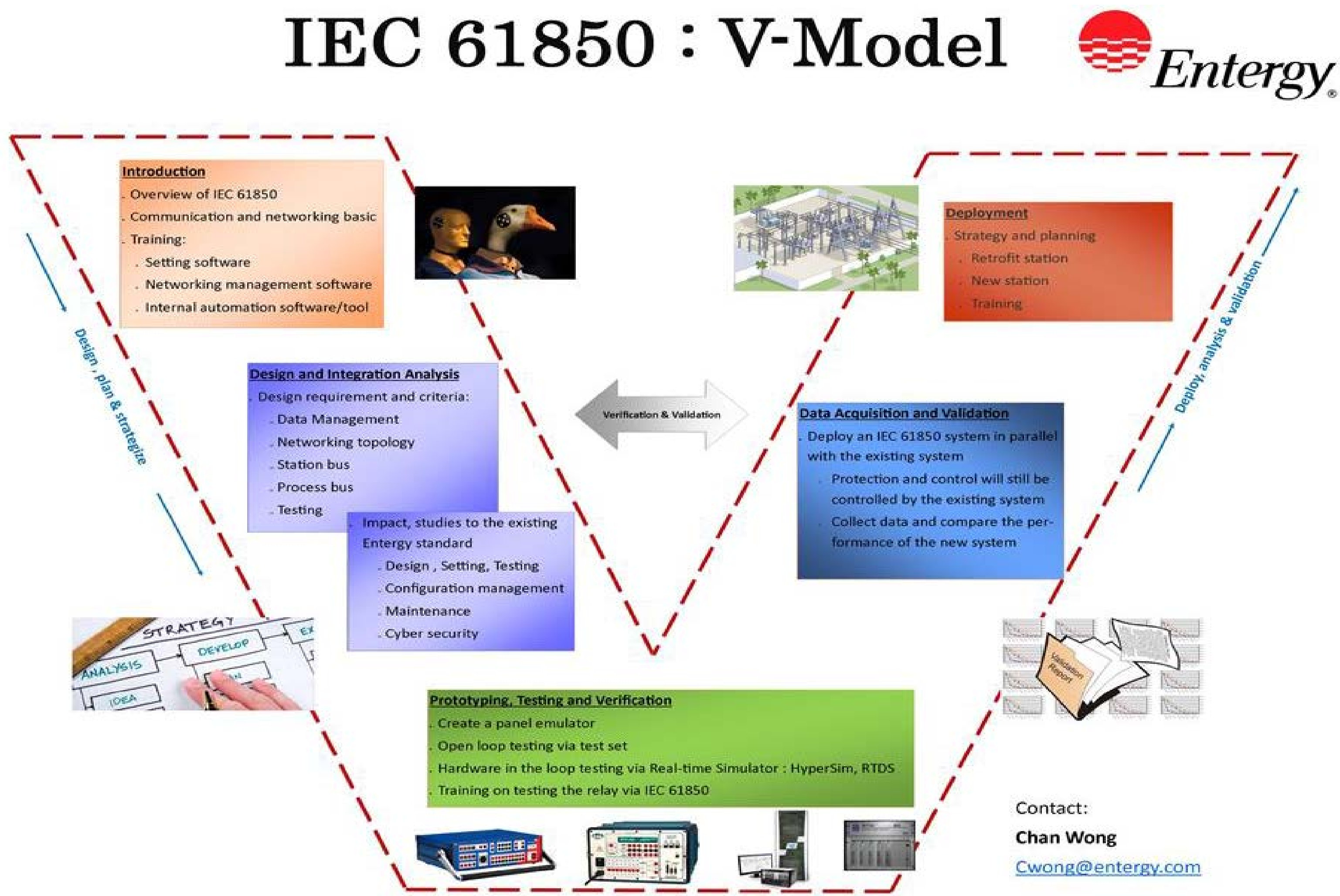
y

Fiber blowing and Microducts

- Collaborate with OptiCOMand Condux to test the Microducts MICRO-COM
- Save time, cost
- Improve safety
- 140 feet in 40 seconds

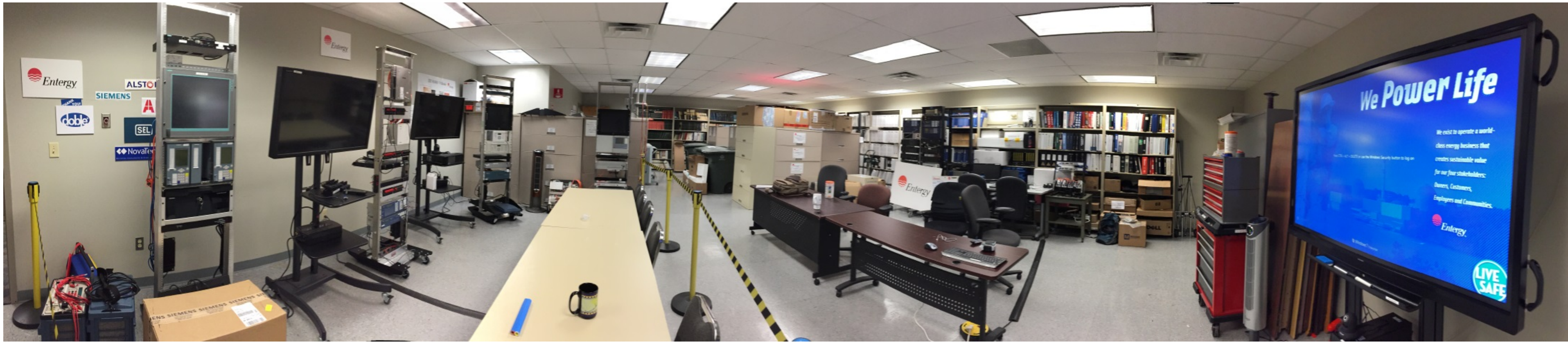


V-Model System : Integration



- 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

Entergy

Entergy Transmission Engineering

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

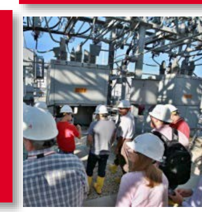
Plugfest 1.0 -July 2014

LIFE℠

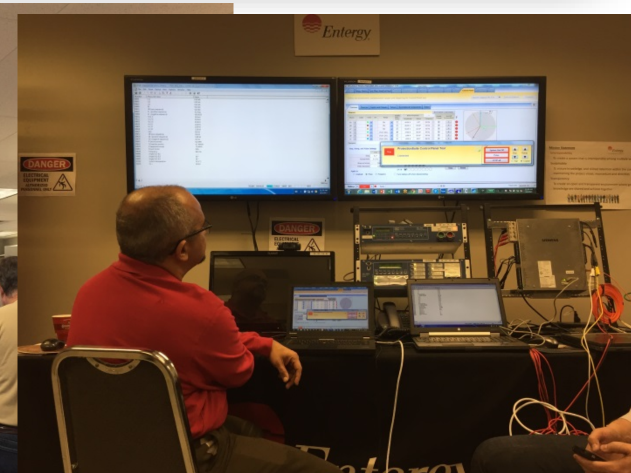
Entergy
Transmission
Engineering

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 2.0 – March 2015



Transmission
Engineering

Plugfest 3.0 – June 2015

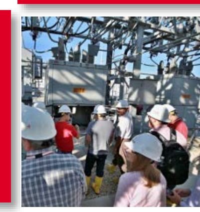
- New Collaborators
  - SUBNET
  - HIRSCHMANN
  - Condux International

- 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

Entergy

Entergy Transmission Engineering



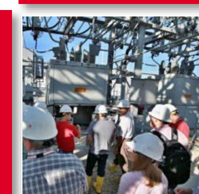
Plugfest 3.0 – June 2015


Entergy
ALSTOM
Entergy
SIEMENS

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

Deployment da

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

Experience sharing and learning

“It Depends.”

COO and VP visit the Pilot Sub

SubstationAutomation

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.

By **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 substations quickly while maintaining the reliability and stability of the grid.

Historically, powerful hurricanes and superstorms have battered the regions served by Entergy. August 2015 marked the 10-year anniversary of Hurricane Katrina, one of the most significant natural disasters to hit New Orleans, Louisiana, U.S. It was a catastrophe for residents and companies in the city. Around 200 Entergy substations and 1,550 feeders were damaged by Hurricane Katrina.

Storm hardening and grid resiliency have never been more important for Entergy, which has received multiple awards and recognition for storm-recovery efforts. Furthermore, the utility always explores multiple ideas and is determined to improve the recovery time of affected facilities, and restore power back to customers as quickly as possible. Recently, the utility has begun designing mobile control houses and raised control houses for certain substations in Louisiana to address the flooding challenges there.

During Hurricane Katrina, Entergy's Joliet substation was submerged in 5 feet of water.

Paradigm Shift

At Entergy Transmission Engineering, a group of young and enthusiastic engineers thinks there should be a paradigm shift in how future substations are designed and built: smarter, leaner and more secure.

In early 2014, Entergy Transmission took the initiative to further explore IEC 61850 to evaluate the suitability and benefit of this standard for the next-generation substation and grid with an eye to high resiliency from natural disasters. With the implementation of the IEC 61850 and IEC 61869 standards, data communications within the control house and substations are much more lean and organized.

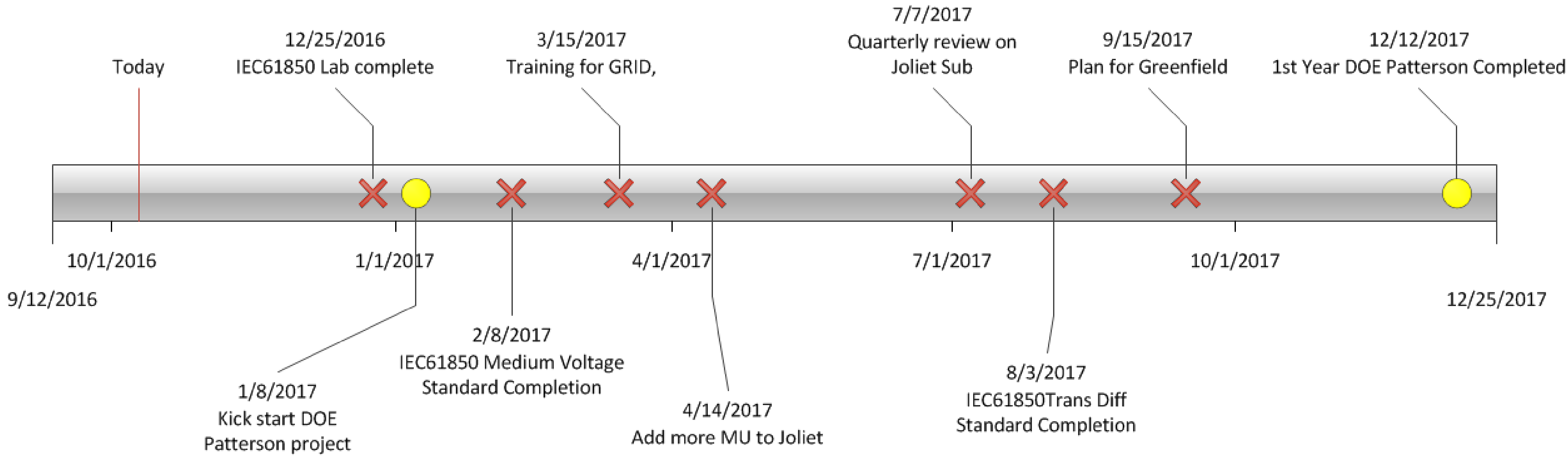
Compared to the traditional copper-cable-based design, the new fiber-optic-based process bus technology promises to provide better flood resistance, superior safety performance and much faster storm recovery for the protection, control and automation infrastructure in substations. Furthermore, the fiber-optic-based solution will minimize copper wire use, which should not only reduce the construction and maintenance cost but also optimize the design and configuration process.

First Steps

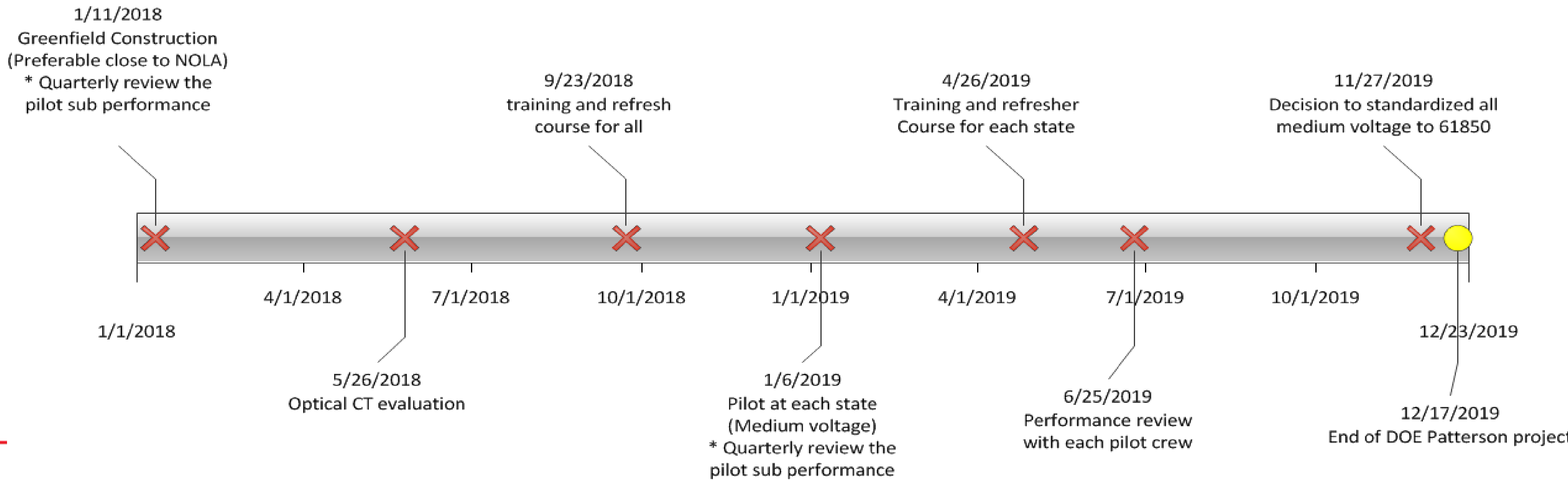
A future-substation core group consisting of protection and control engineers, field/grid engineers and technicians, and operation information technology (OIT) and transmission management was formed to perform research and devel-

Projected Schedule and deliverables

2016-2017



2018-2019



ONE MORE THING !!!

UCA Interoperability – NEW ORLEANS OCT 2017

UCA IOP New Orleans

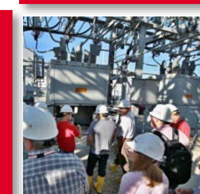
- The IOP test will take place in New Orleans in October 2017. It will be hosted by Entergy.
- The Boot Camp training
  - October 12 - 13.
- IOP testing
  - October 14 - 19.
- IEC TC57 WG10
  - Follow after IOP
- Marriott Arts District / Convention Center

UCA International Users Group

IEC 61850 users group

Entergy

Entergy Transmission Engineering



Entergy

Thanks

Chan Wong
cwong@entergy.com

Entergy
Transmission
Engineering

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	Quantity	Cost / Unit	Totals	Benefits
Copper System Costs				
Trenching	600	7.5 $/SF	$ 4,500	
10 # 12 SIS wires, terminated	1800	28.0 $/SF	$ 50,400	
20 # 14 SIS wires, terminated	1800	50.0 $/SF	$ 90,000	
Schedule 80 & boxes	1800	18.0 $/SF	$ 32,400	
Total			**$ 177,300**	**Reference**
Fiber System Costs (PRP topology)				
Trenching	1600	1.0 $/SF	$ 1,600	
Tubing	1600	2.5 $/SF	$ 4,000	
Hardened Fiber	1600	2.5 $/SF	$ 4,000	
GPS clock cabling	1600	2.5 $/SF	$ 4,000	
Fiber Optic Terminations	128	$ 78	$ 9,984	
GPS Clock	1	$ 2,500	$ 2,500	**Savings (%)**
SIPROTEC 8MU80 Merging Units	16	$ 4,000	$ 64,000	**15%**
SIPROTEC PB201 Process Bus Modules	16	$ 3,800	$ 60,800	**Savings ($)**
Total			**$ 150,884**	**$ 26,416**
Fiber System Costs (HSR topology)				
Trenching	1600	1.0 $/SF	$ 1,600	
Tubing	400	2.5 $/SF	$ 1,000	
Hardened Fiber	533	2.5 $/SF	$ 1,333	
GPS clock cabling	1600	2.5 $/SF	$ 4,000	
Fiber Optic Terminations	34	$ 78	$ 2,652	
GPS Clock	1	$ 2,500	$ 2,500	**Savings (%)**
SIPROTEC 8MU80 Merging Units	16	$ 4,000	$ 64,000	**22%**
SIPROTEC PB201 Process Bus Modules	16	$ 3,800	$ 60,800	**Savings ($)**
Total			**$ 137,885**	**$ 39,415**

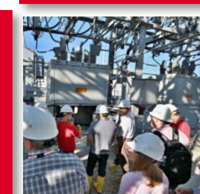
Entergy

Entergy Transmission Engineering

A:Benchmarking

- 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



BUILDING A WORLD OF DIFFERENCE

3/28/2016

IEC 61850 ARCHITECTURE AND GOOSE

CRAIG PREUSS

ENGINEERING MANAGER,
TELECOM – PRIVATE NETWORKS

SECRETARY IEEE PES POWER SYSTEM COMMUNICATIONS AND CYBERSECURITY COMMITTEE

BLACK & VEATCH
Building a world of difference.®

IEC 61850 ARCHITECTURE AND GOOSE

Pieces, parts, and protocols

Architecture

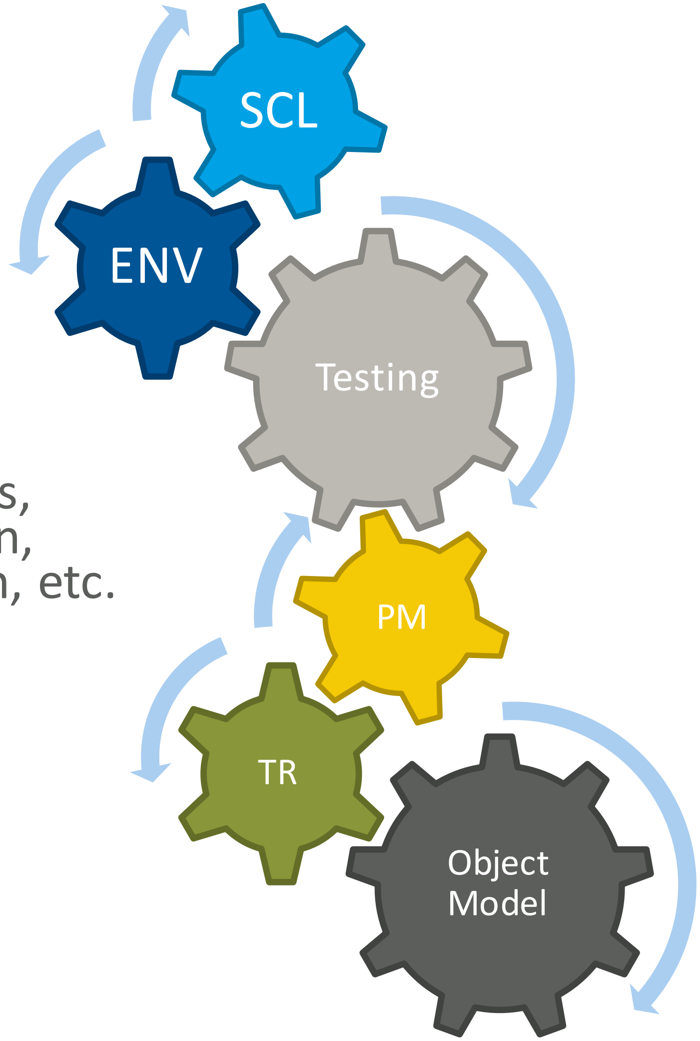
THE BASIC CORE

Impact RFPs and Products	Basic Principles			Part 1
	Glossary			Part 2
	General Requirements			Part 3
	System and project management			Part 4
	Communication requirements			Part 5
Impact engineering & implementation	System Configuration Language			Part 6
	Basic Communication Structure			Part 7
	Part 8	Mapping to MMS and Ethernet	Sampled Values	Part 9
			Precision Time Protocol	
	Conformance testing			Part 10

The core parts easily demonstrate that any a reference to a 61850 protocol is incorrect.

"OTHER STUFF" BESIDES PROTOCOLS

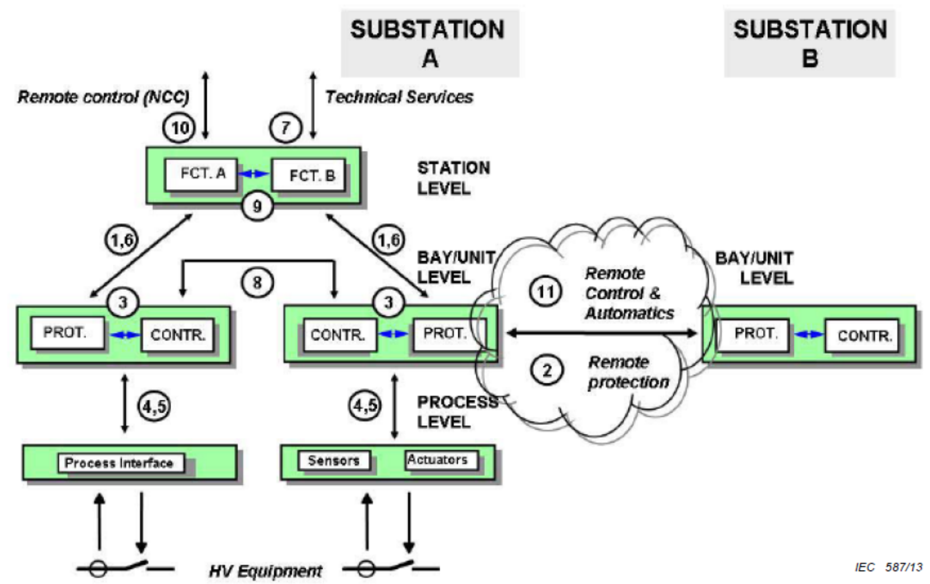
- **System configuration language (61850-6)**
- **General requirements (61850-3)**
  - Edition 1 primarily environmental
  - Edition 2 adds ratings, marking, documentation, packaging, dimensions, functional performance, safety, burden, mechanical, enclosure, documentation, etc.
- **Testing (61850-10)**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



NOTE Interface numbers are for notational use in other parts of the IEC 61850 series and have no other significance.

Figure 4 – Interface model within substation and between substations

90-5-2012 introduces IF12 (between control centers) and IF13 (WAMS), then adds condition monitoring and diagnosis to IF7

MMS

61850-5:2003

Sampled Values

61850-9-2:2003

GOOSE

High speed communication of analogs and digitals (61850-8-1:2004)

Synchrophasors

61850-90-5

R-SV (routable sampled values)

R-GOOSE (routable GOOSE)

Time synchronization

SNTP (61850-8-1:2003)

1588v2 PTP

61850-9-3

File transfer

MMS file transfer

FTP/sFTP is "local issue"

61850-8-1:2011

Rapid Spanning Tree Protocol
(RSTP)
61850-8-1:2011

PRP (Parallel Redundancy Protocol) and HSR
(High availability Seamless Ring)

(61850-8-1:2011)

ARP

Address Resolution Protocol

61850-8-1:2004

mandatory

ICMP

Internet Control Message Protocol

61850-8-1:2011

Mandatory

OTHER PROTOCOLS

61850-90-4

SNMP, Syslog, FTP, SSH

And others

FUNCTION PERFORMANCE REQUIREMENTS AND 61850 PROTOCOLS

Table 37 – IEC 61850-5 interface traffic

Function Type/Message		Interface (Table 1)	Protocol	Max. delay ms	Bandwidth	Priority	Application
1A. Trip	GOOSE	3,8	L2 Multicast	3	Low	High	Protection
1B. Other	GOOSE	3,8	L2 Multicast	10 to100	Low	Medium High	Protection
2. Medium Speed	MMS	6	IP/TCP	<100	Low	Medium Low	Control
3. Low Speed	MMS	6	IP/TCP	<500	Low	Medium Low	Control
4. Raw Data	SV	4	L2 Multicast	4	High	High	process bus
5. File Transfer	MMS	6,7	IP/TCP/FTP	>1 000	Medium	Low	Management
6. Time Sync	Time Sync		IP (SNTP) L2 (PTP)		Low	Medium High	General Phasors, SVs
7. Command	MMS	6	IP		Low	Medium Low	Control

Taken from 61850-90-4-2013

Abuse of GOOSE – using it for Type 2 or 3 functions when MMS should be used

WHERE ARE THESE PROTOCOLS EXPECTED TO BE SEEN ON A LAN?

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
X		X	X	X	X	X	X	X	X	X			MMS
	X	X		X			X			X			GOOSE
	X		X				X						SV
X			X	X	X	X			X				MMS
X		X	X	X	X	X	X	X	X				SNTP/PTP

Red is "station bus" and green is "process bus"

VIEWING GOOSE FROM THE OSI STACK

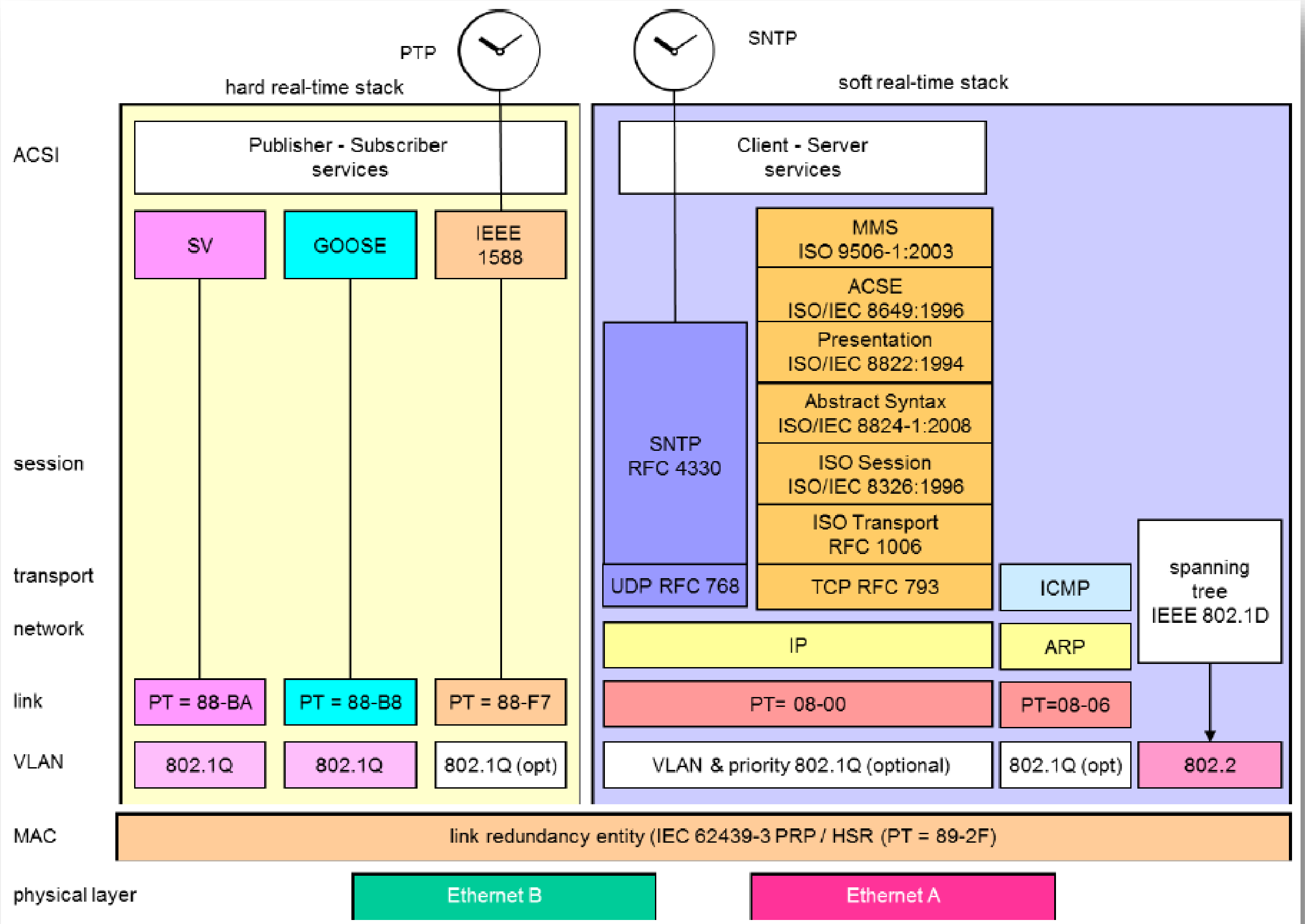


Figure 6 – IEC 61850 protocol stack

GOOSE PACKET

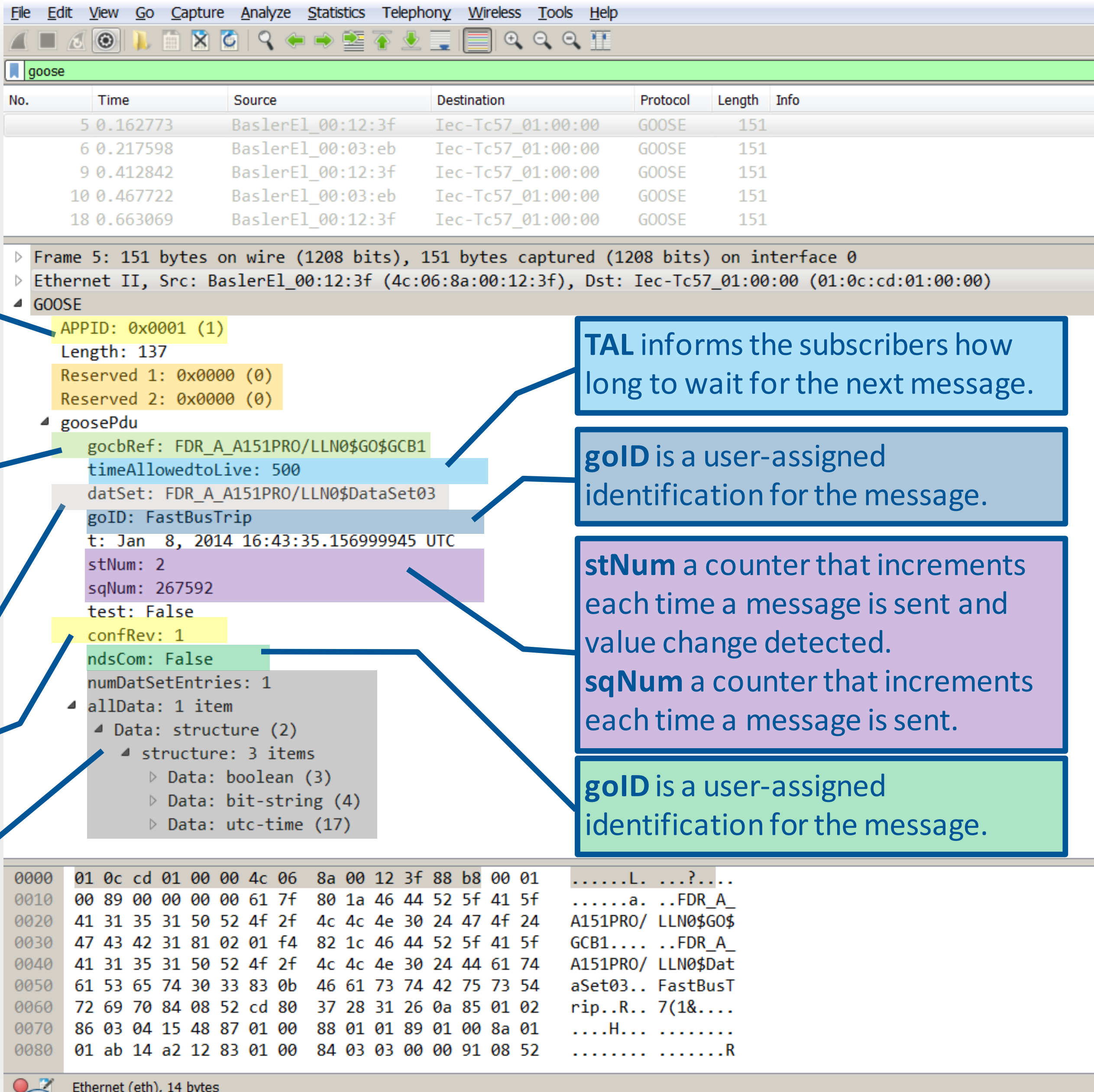
APPID is from the GOOSE control block and is a system wide unique identifier of the application for the message.

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.

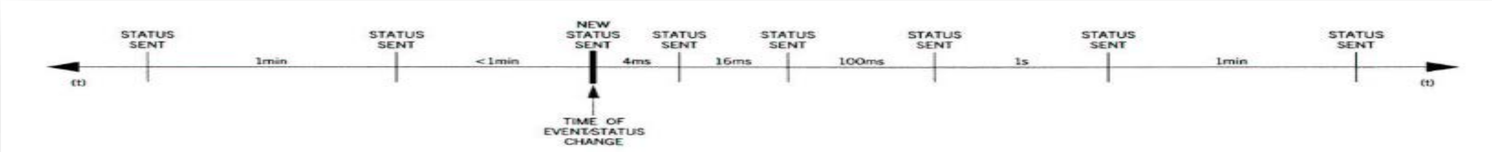
goID is a user-assigned identification for the message.

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.

GOOSE and SV are similar as defined in Annex C of 8-1-2011

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				MMS
P5	TT2	X		X	X	X	X	X	X	X	X				MMS
P4	TT3		X	X					X	X		X			MMS
P3	TT4 (20)		X	X					X			X			GOOSE
P2	TT5 (10)		X	X								X			GOOSE
P1	TT6 (3)			X		X			X						GOOSE
P7	TT6				X				X						SV
P8	TT5		X		X				X						SV
P9	TT0	X			X	X	X	X			X				MMS
P10	TT2	X		X	X	X	X	X	X	X	X				SNTP/PTP
P11	TT1	X		X	X	X	X	X	X	X	X				SNTP/PTP
P12	TT0	X			X	X	X	X			X				SNTP/PTP

PERFORMANCE IN IEC 61850-5:2013

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

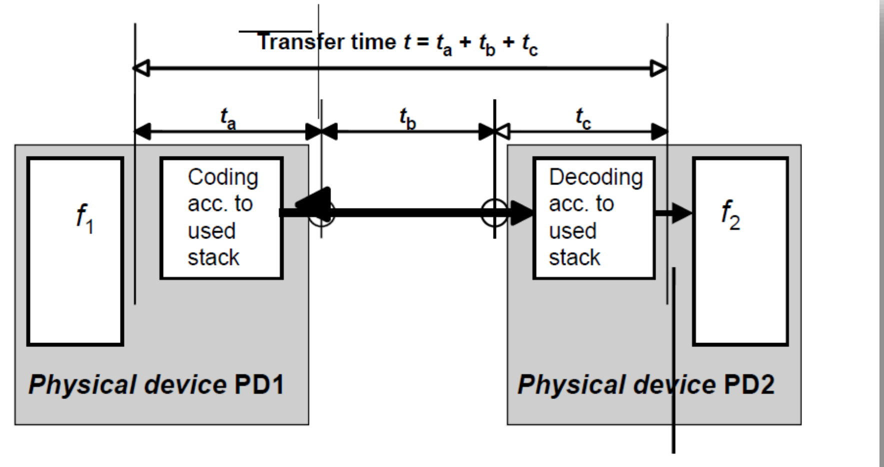


Figure 13 – Definition of "overall transfer time" t and indication of processing times

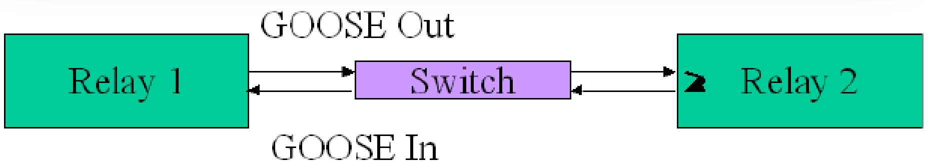


Figure 30 —GOOSE performance test

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

GOOSE CYBERSECURITY

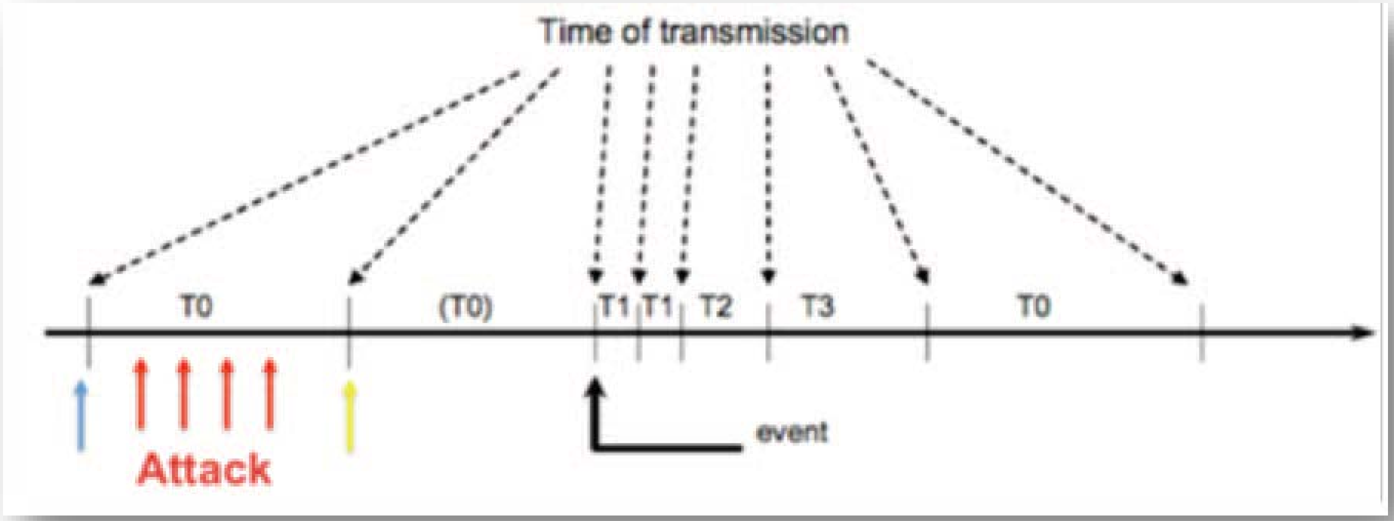
- **GOOSE message structure has an optional framework to support cybersecurity**
  - Based on IEC 62351-6
  - Uses Reserved1 and Reserved2 fields from the message
  - Uses an extension to the message that contains the message authentication code
- **Research indicates**
  - The authentication using 1024-bit 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



Juan Hoyos, et al, "Exploiting the GOOSE Protocol: A Practical Attack on Cyber-infrastructure", GC'12 Workshop: Smart Grid Communications: Design for Performance

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

61850-90-4-2013 EXAMPLE LAN ARCHITECTURES

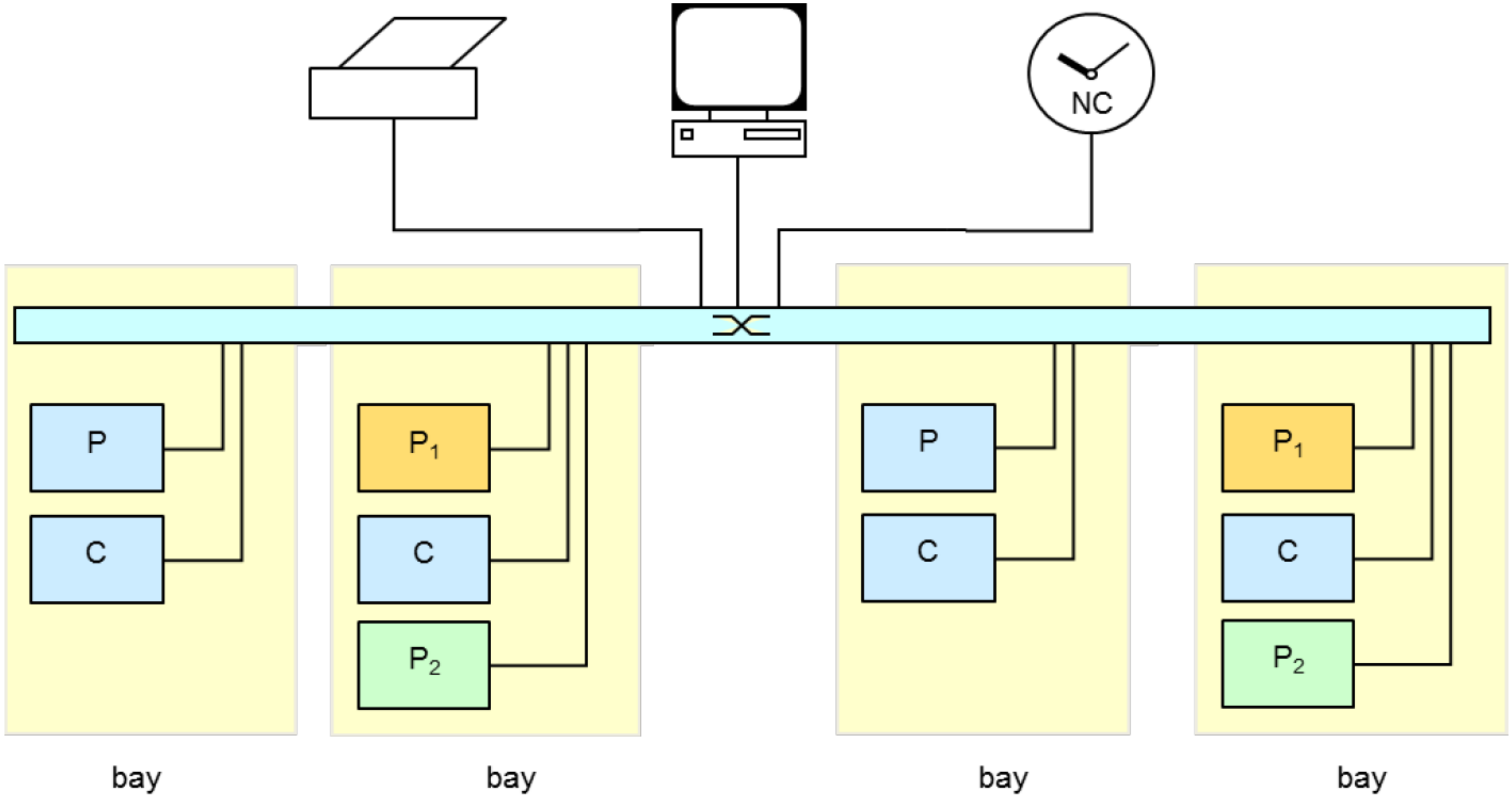


Figure 24 – Station bus as single bridge

61850-90-4-2013 EXAMPLE LAN ARCHITECTURES

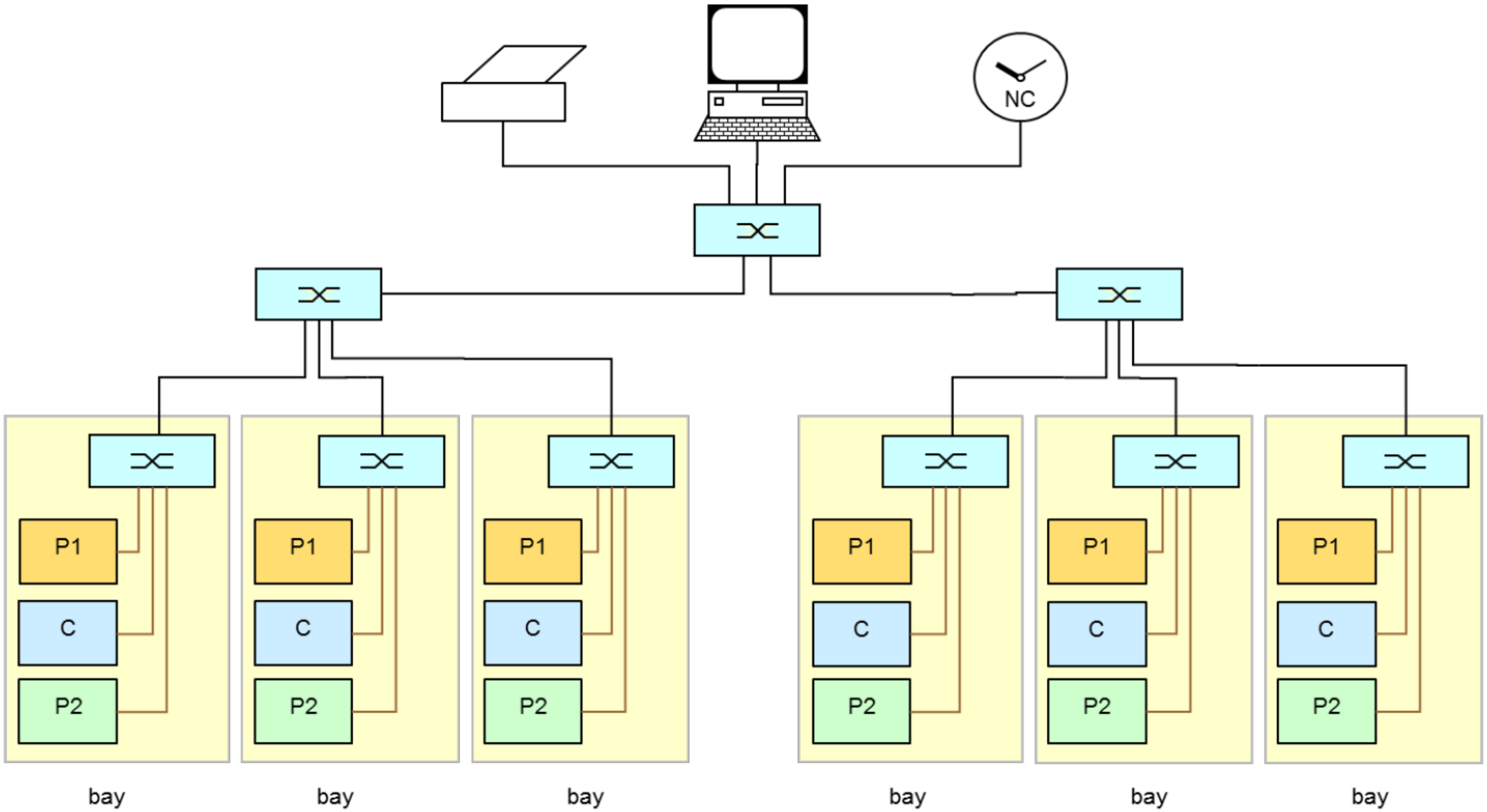


Figure 25 – Station bus as hierarchical star

61850-90-4-2013 EXAMPLE LAN ARCHITECTURES

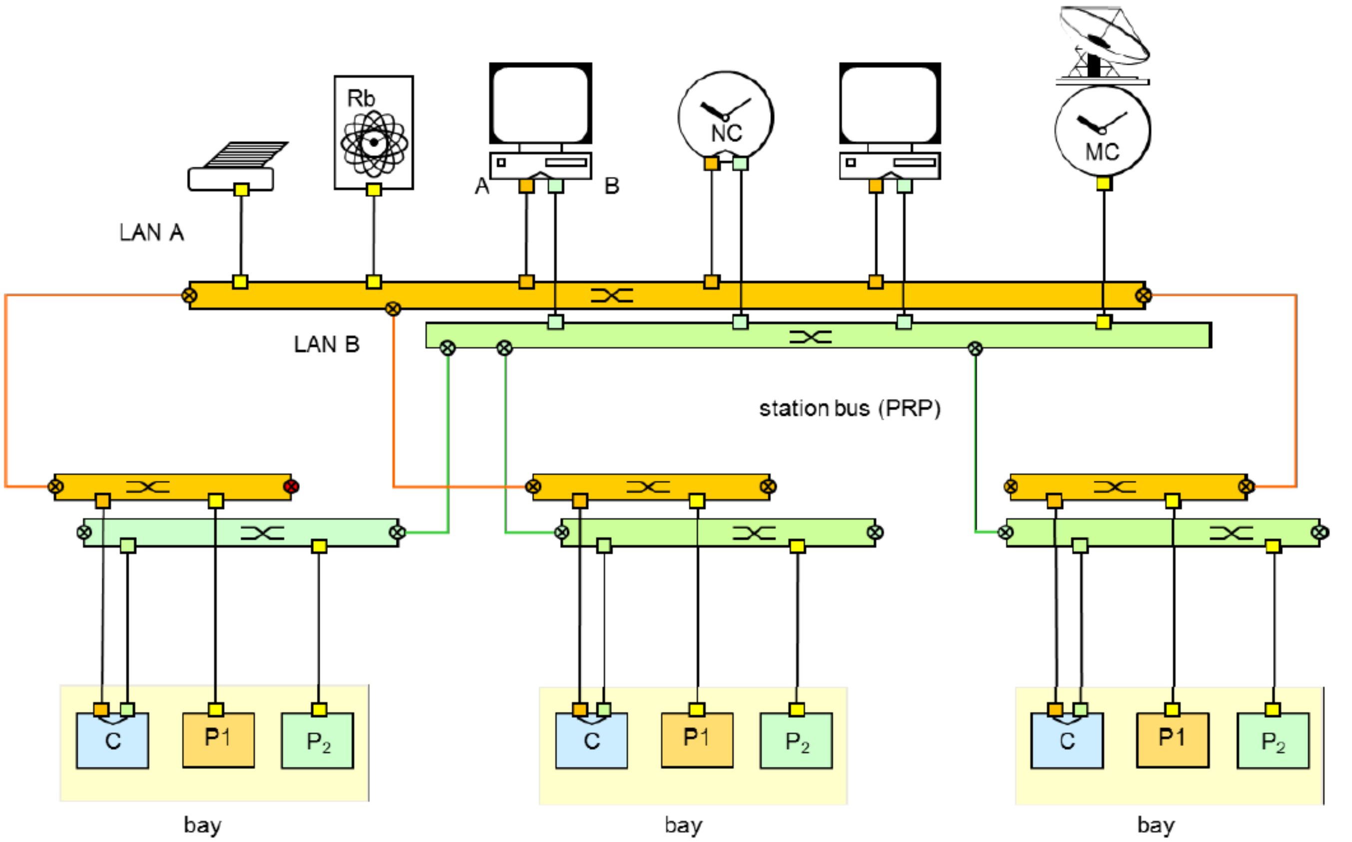


Figure 26 – Station bus as dual star with PRP

61850-90-4-2013 EXAMPLE LAN ARCHITECTURES

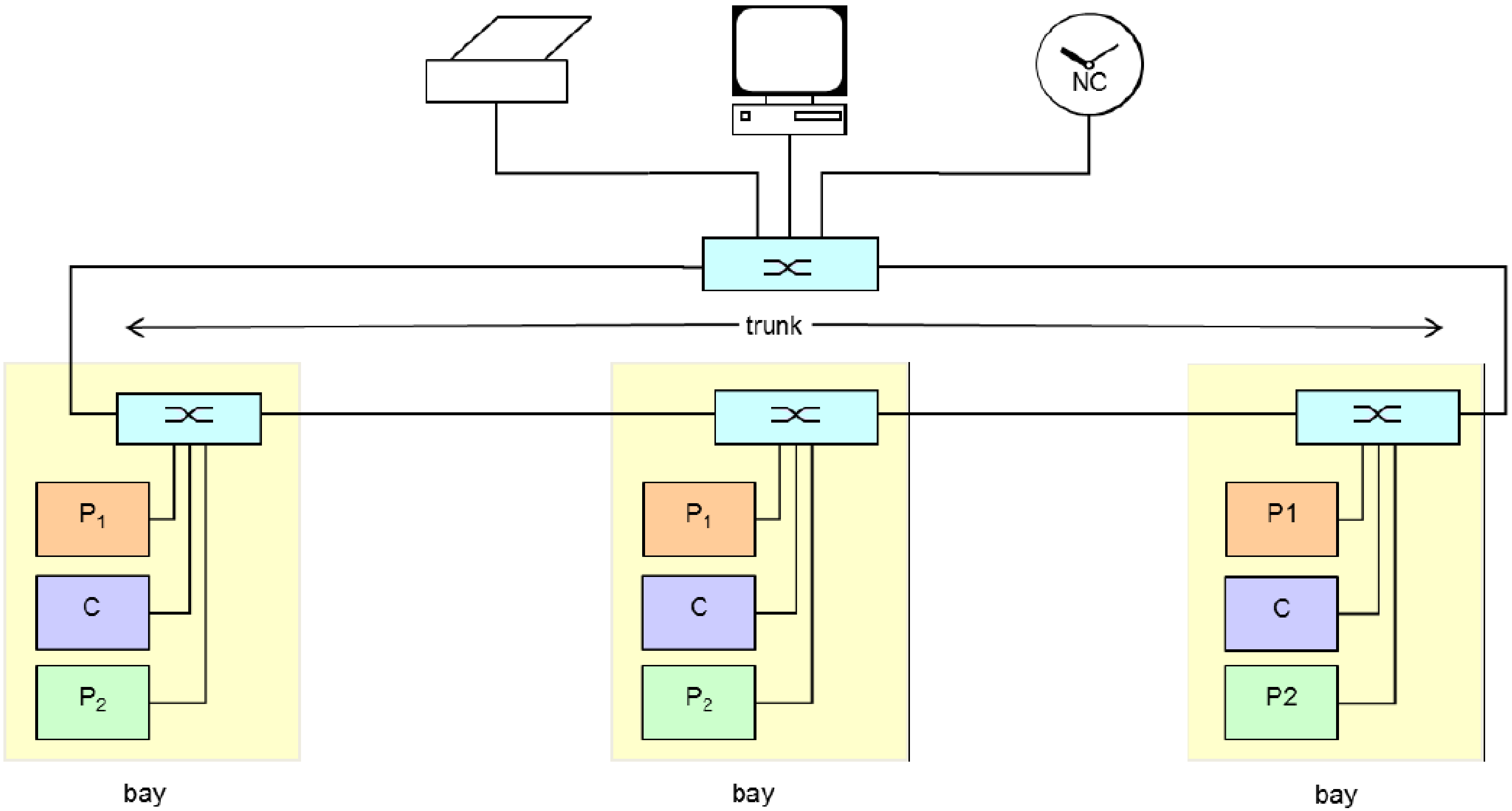


Figure 27 – Station bus as ring of RSTP bridges

61850-90-4-2013 EXAMPLE LAN ARCHITECTURES

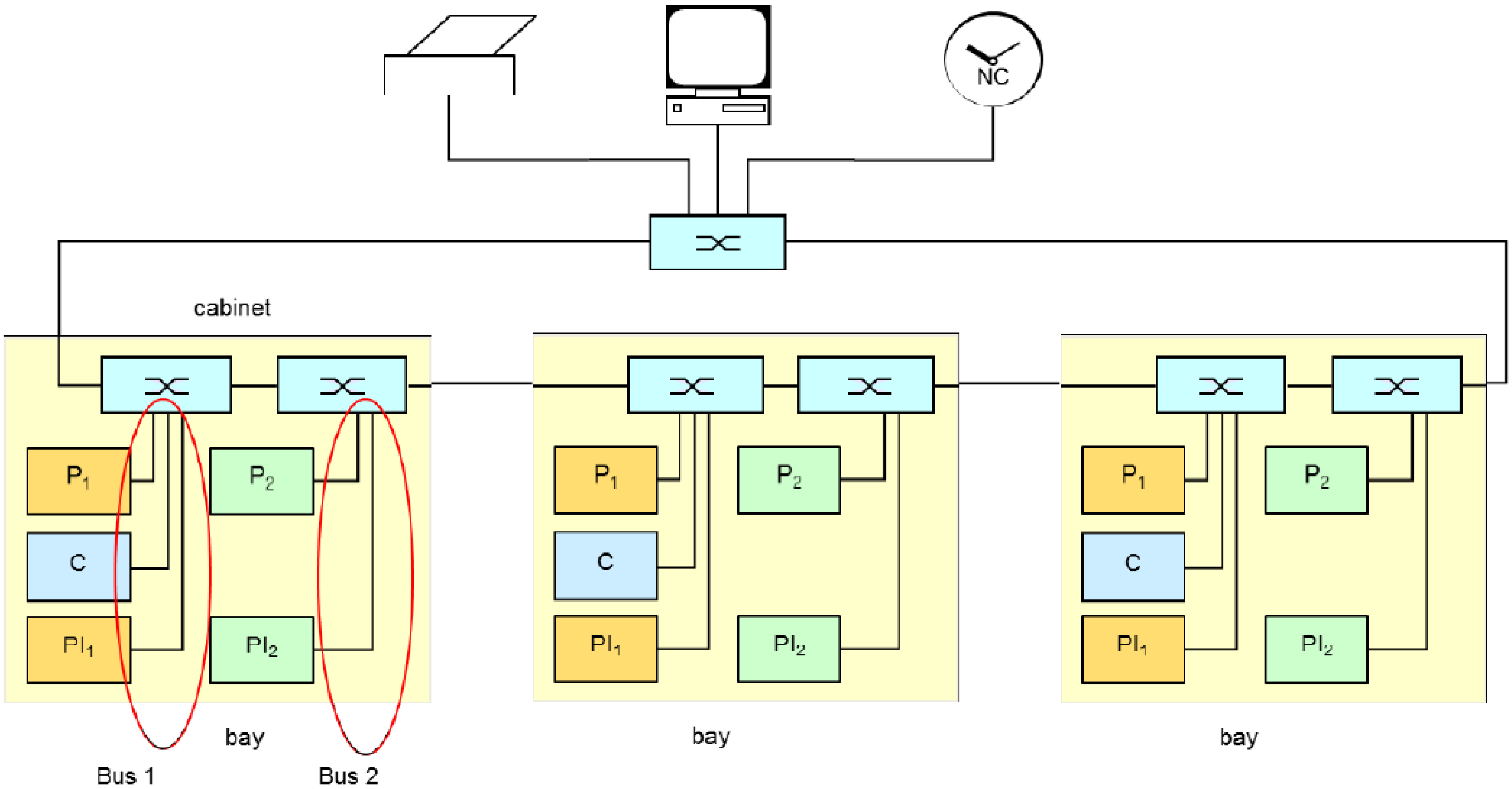


Figure 28 – Station bus as separated Main 1 (Bus 1) and Main 2 (Bus 2) LANs

61850-90-4-2013 EXAMPLE LAN ARCHITECTURES

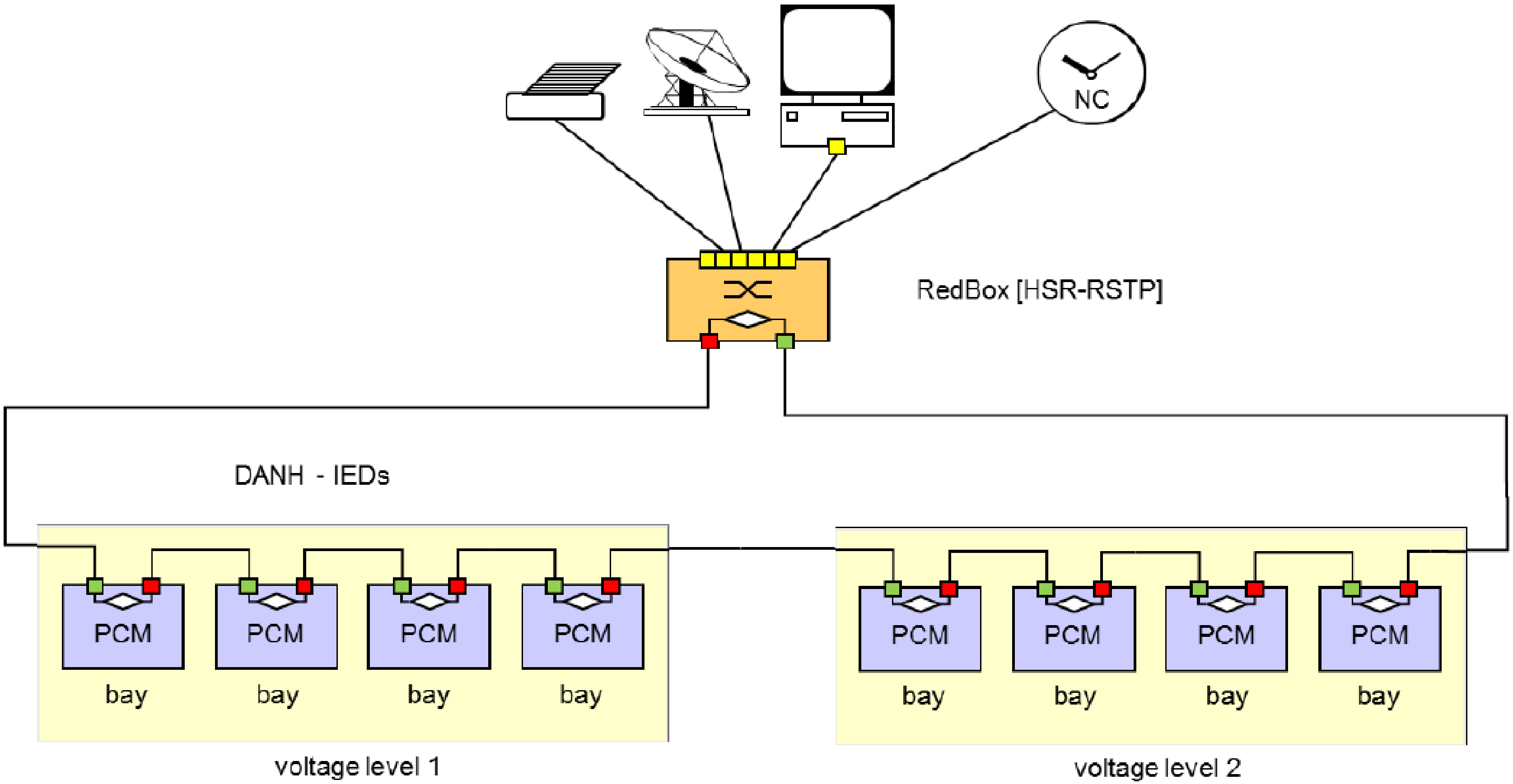


Figure 29 – Station bus as ring of HSR bridging nodes

61850-90-4-2013 EXAMPLE LAN ARCHITECTURES

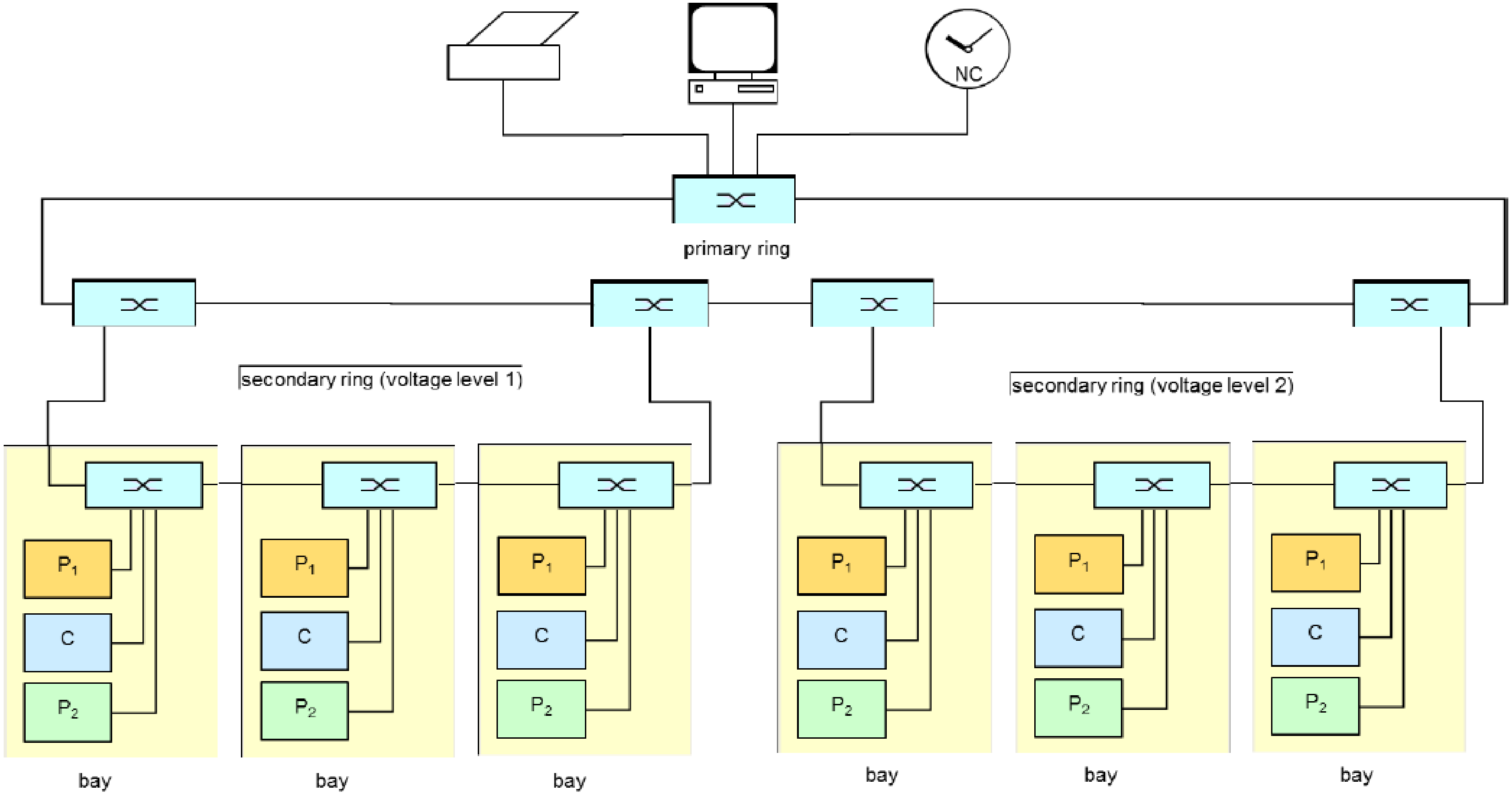


Figure 30 – Station bus as ring and subrings with RSTP

61850-90-4-2013 EXAMPLE LAN ARCHITECTURES

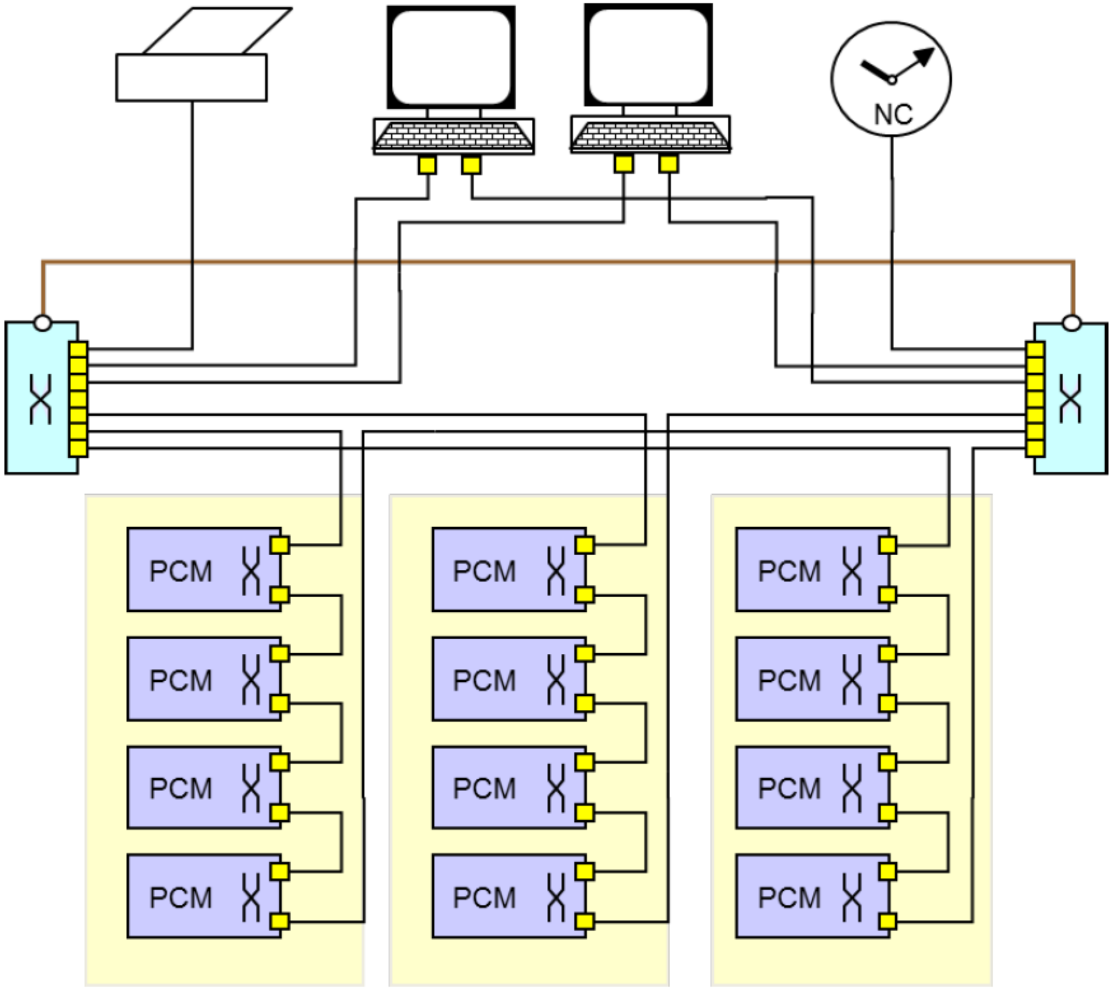


Figure 31 – Station bus as parallel rings with bridging nodes

61850-90-4-2013 EXAMPLE LAN ARCHITECTURES

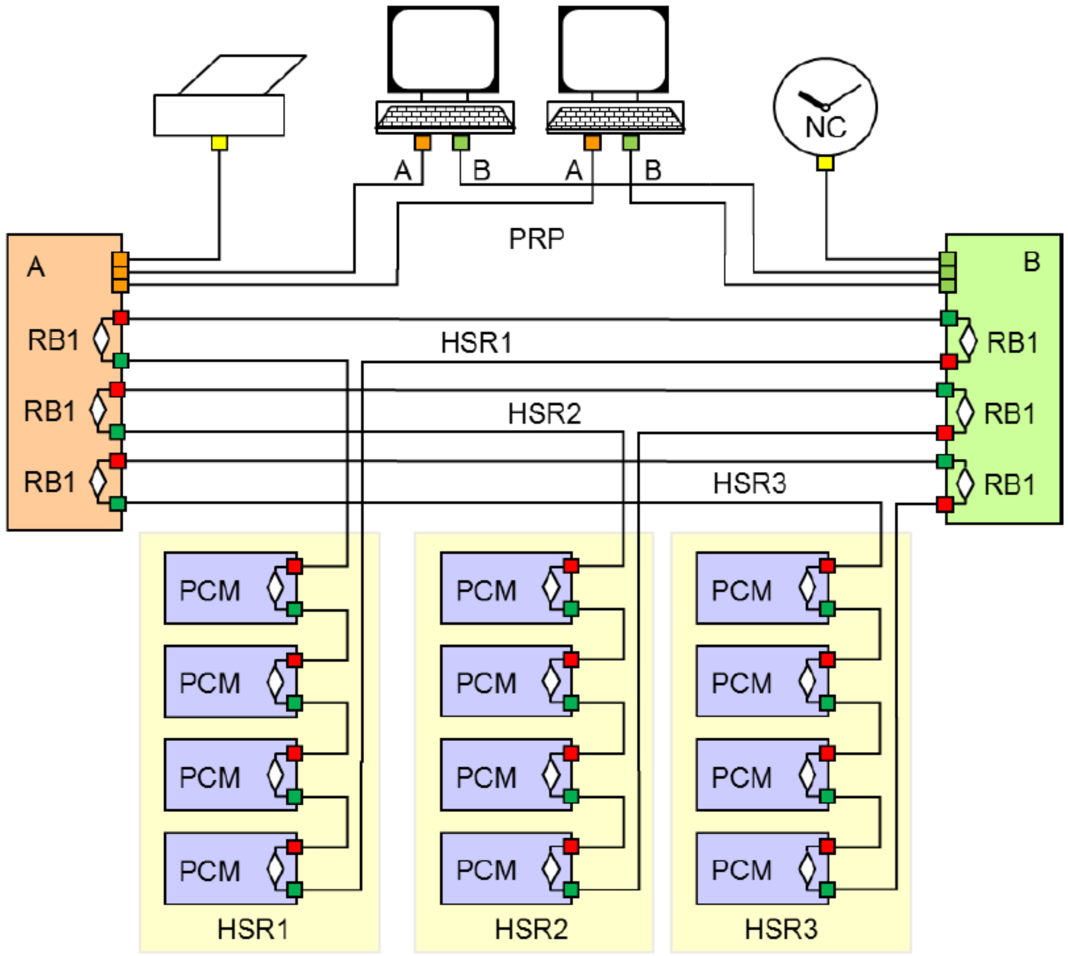


Figure 32 – Station bus as parallel HSR rings

61850-90-4-2013 EXAMPLE LAN ARCHITECTURES

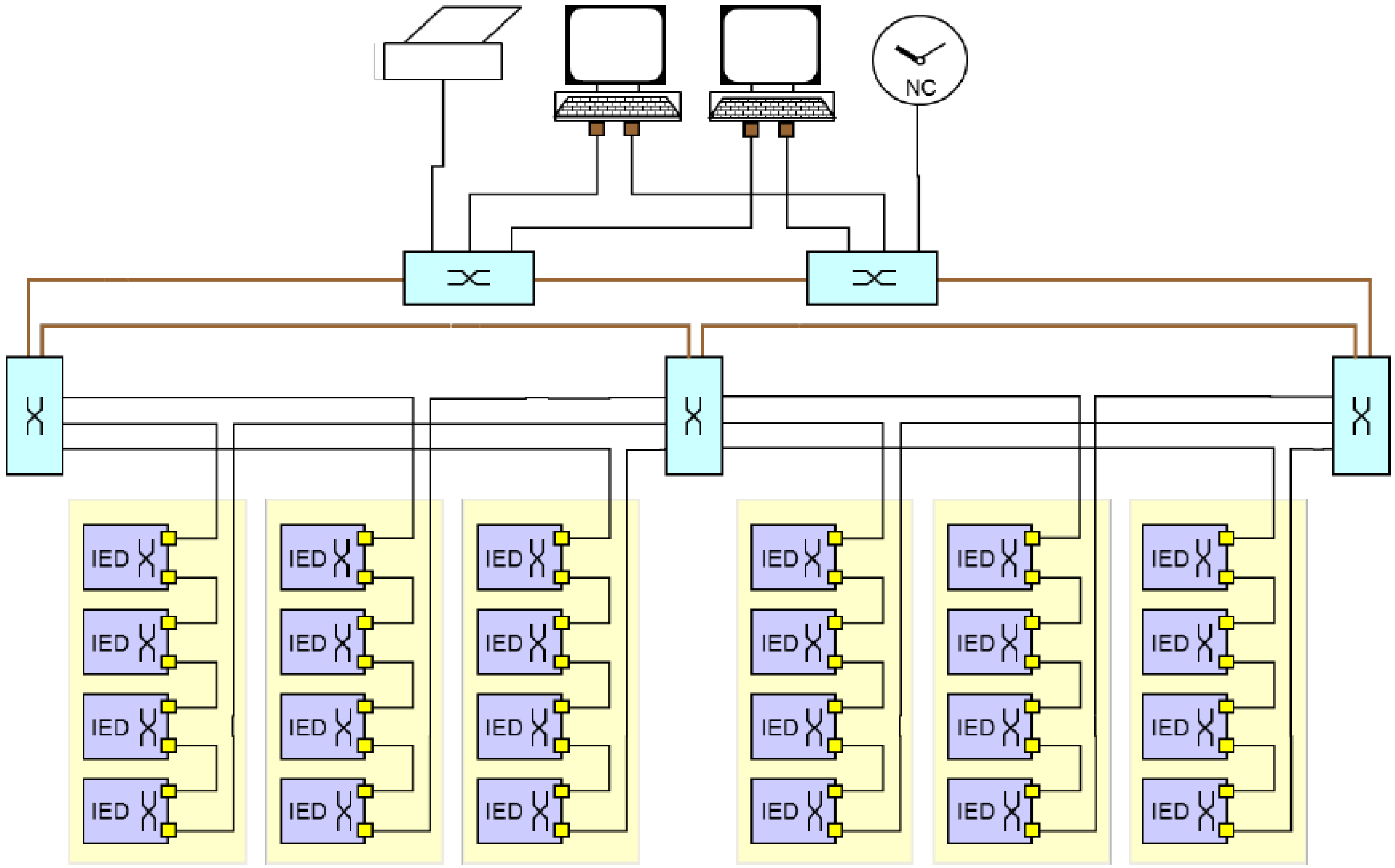


Figure 33 – Station bus as hierarchical rings with RSTP bridging nodes

61850-90-4-2013 EXAMPLE LAN ARCHITECTURES

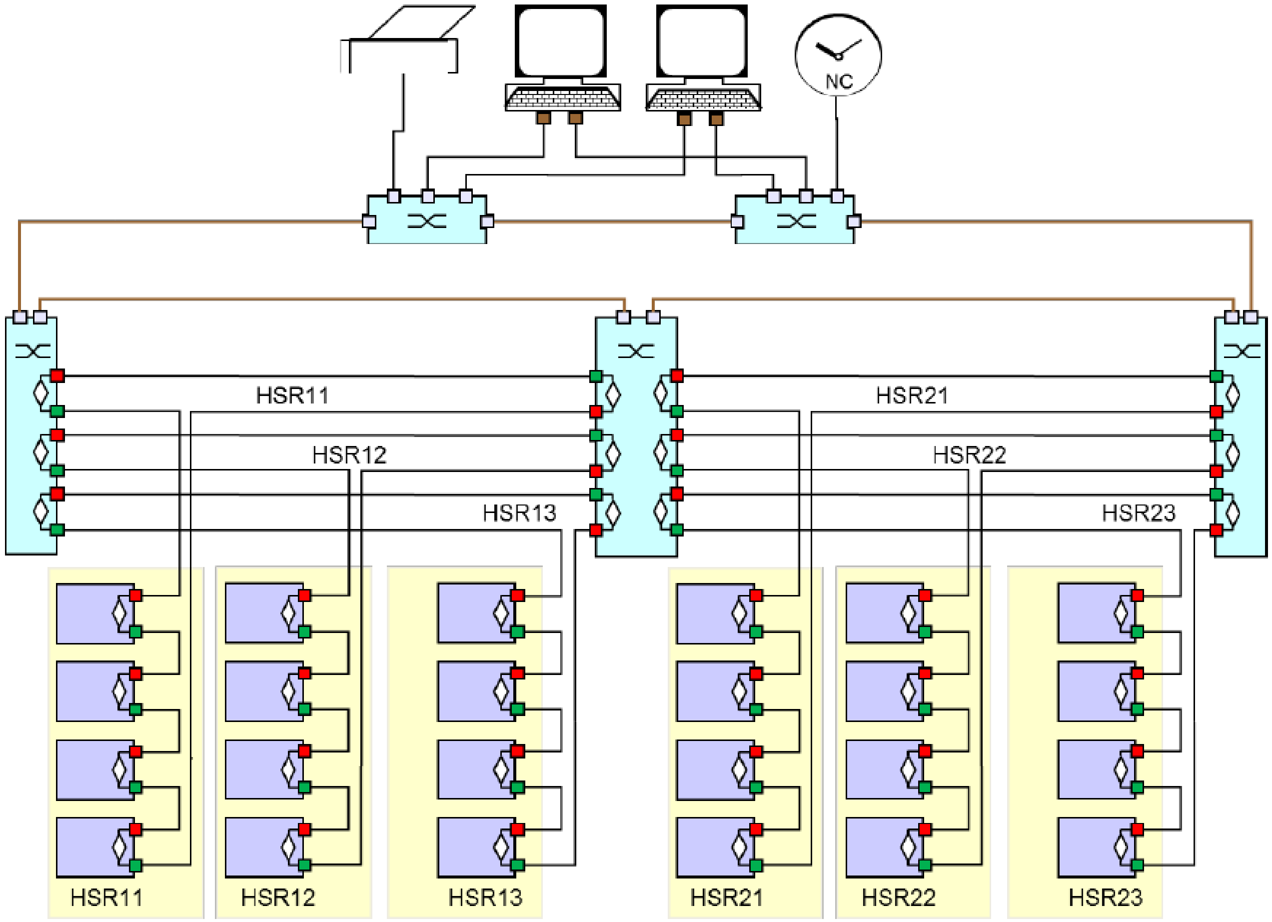


Figure 34 – Station bus as hierarchical rings with HSR bridging nodes

61850-90-4-2013 EXAMPLE LAN ARCHITECTURES

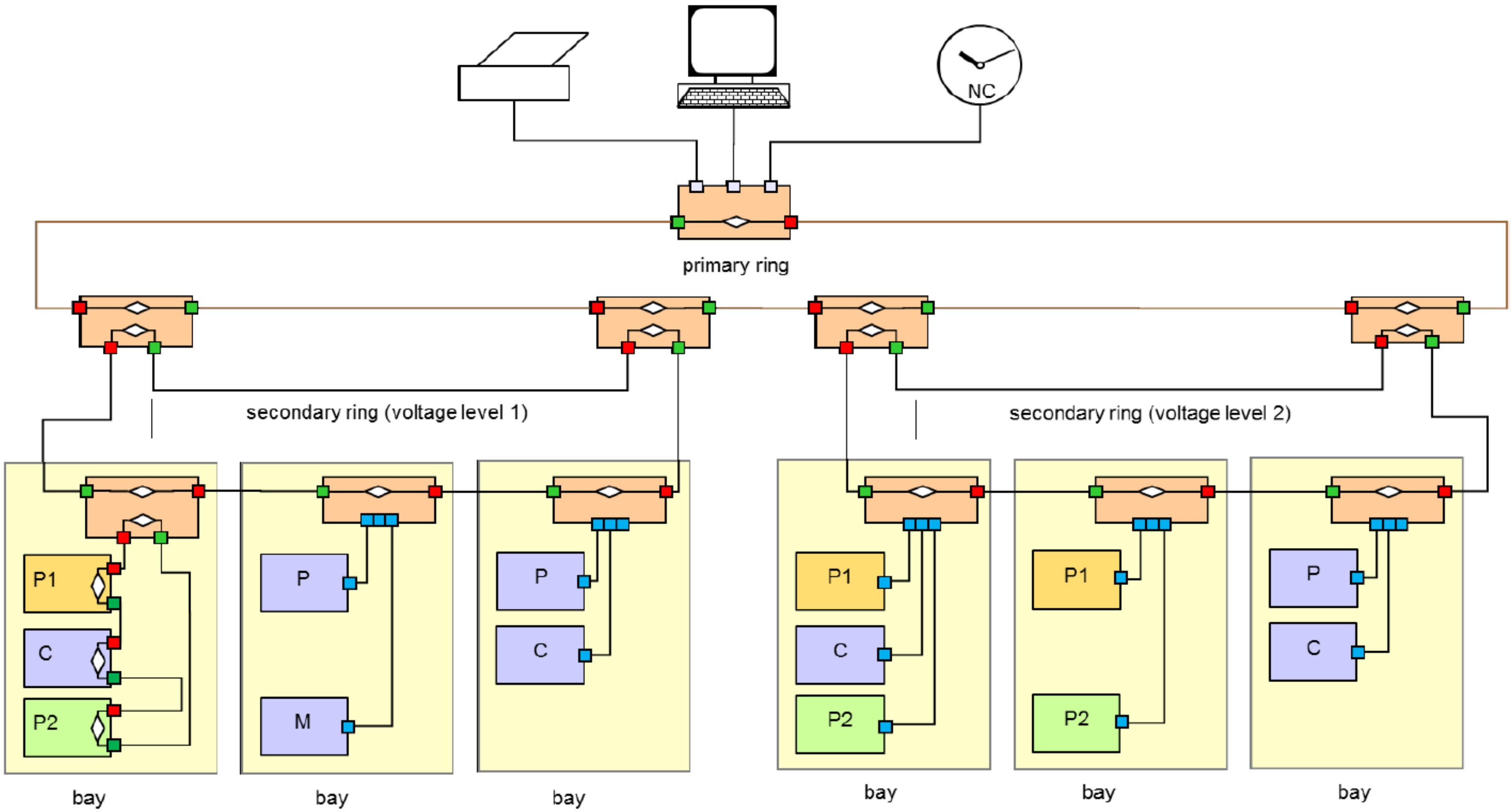


Figure 35 – Station bus as ring and subrings with HSR

61850-90-4-2013 EXAMPLE LAN ARCHITECTURES

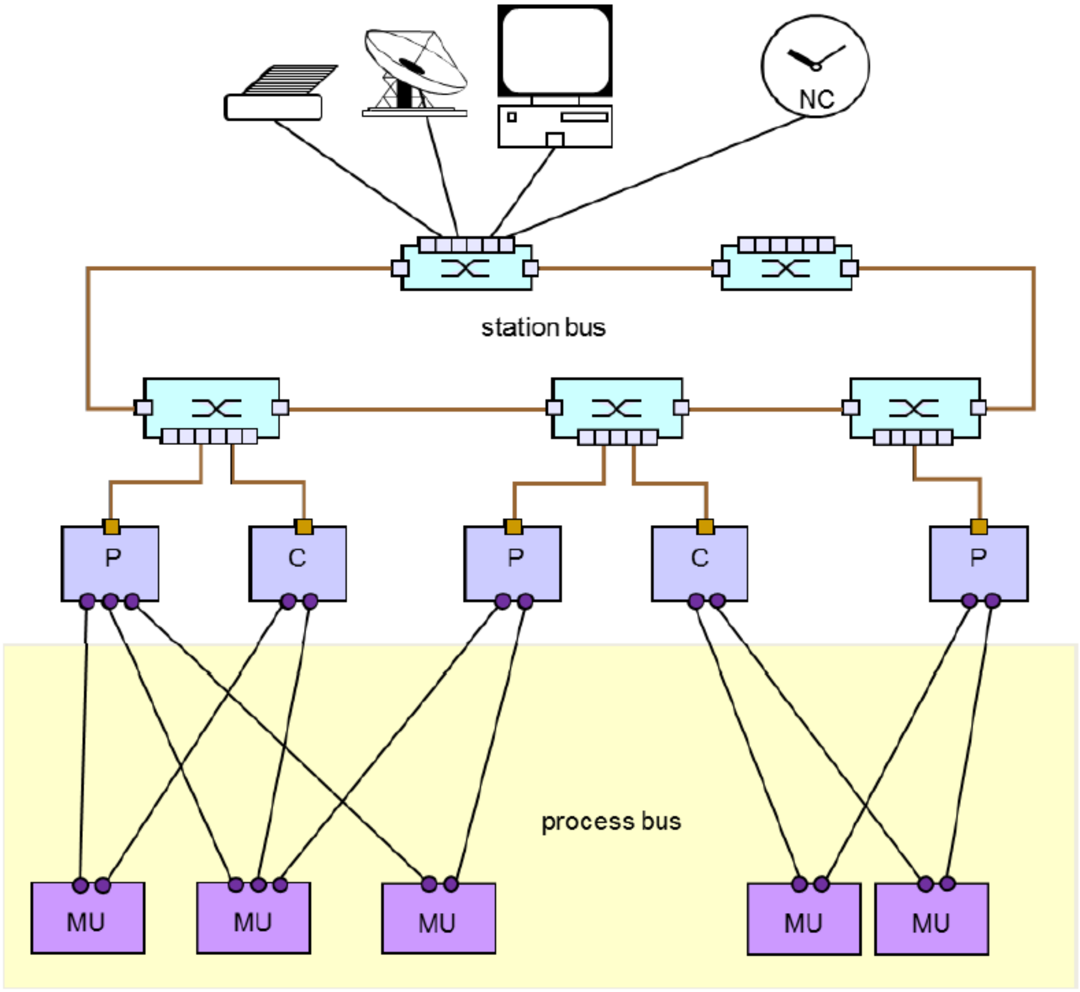


Figure 48 – Process bus as star to merging units and station bus as RSTP ring

61850-90-4-2013 EXAMPLE LAN ARCHITECTURES

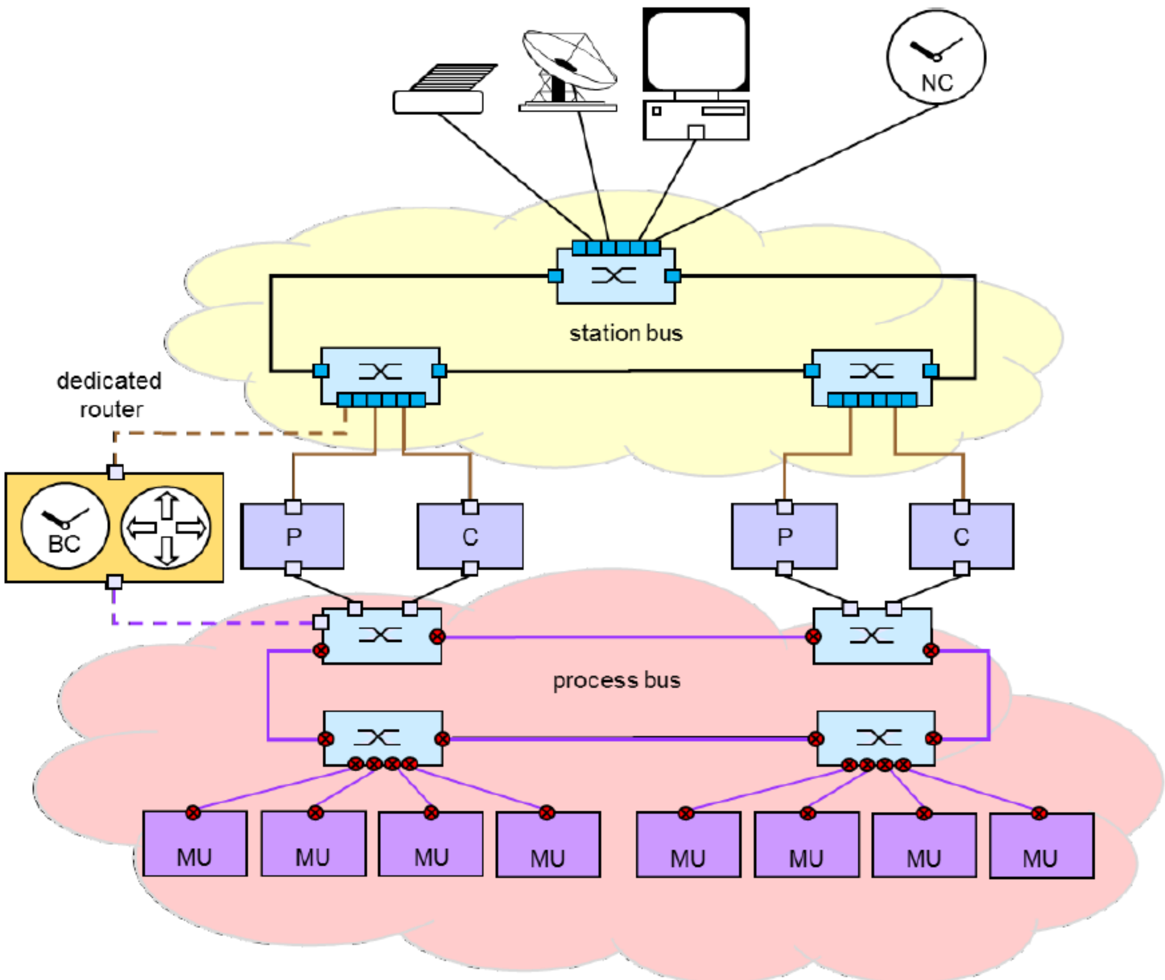


Figure 49 – Station bus and process bus as rings connected by a router

61850-90-4-2013 EXAMPLE LAN ARCHITECTURES

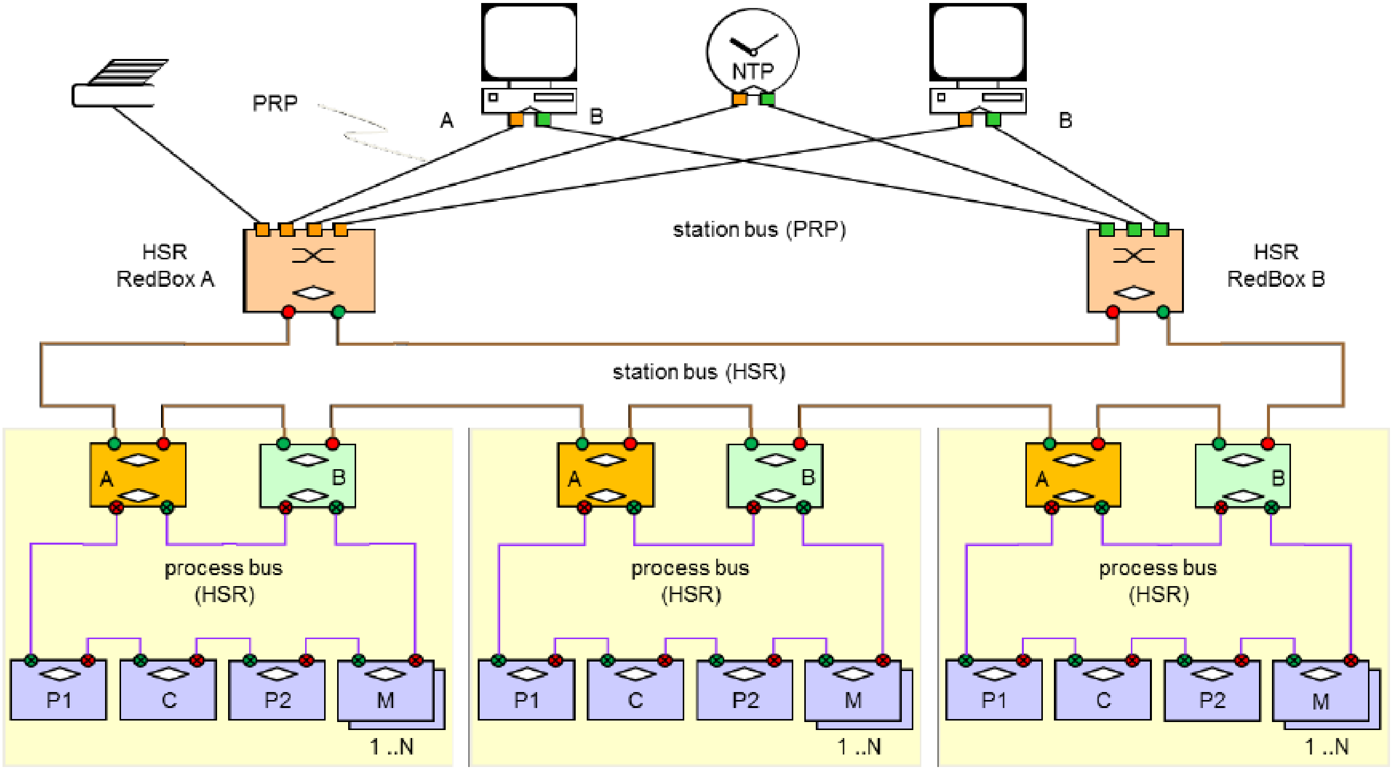


Figure 50 – Station bus ring and process bus ring with HSR

61850-90-4-2013 EXAMPLE LAN ARCHITECTURES

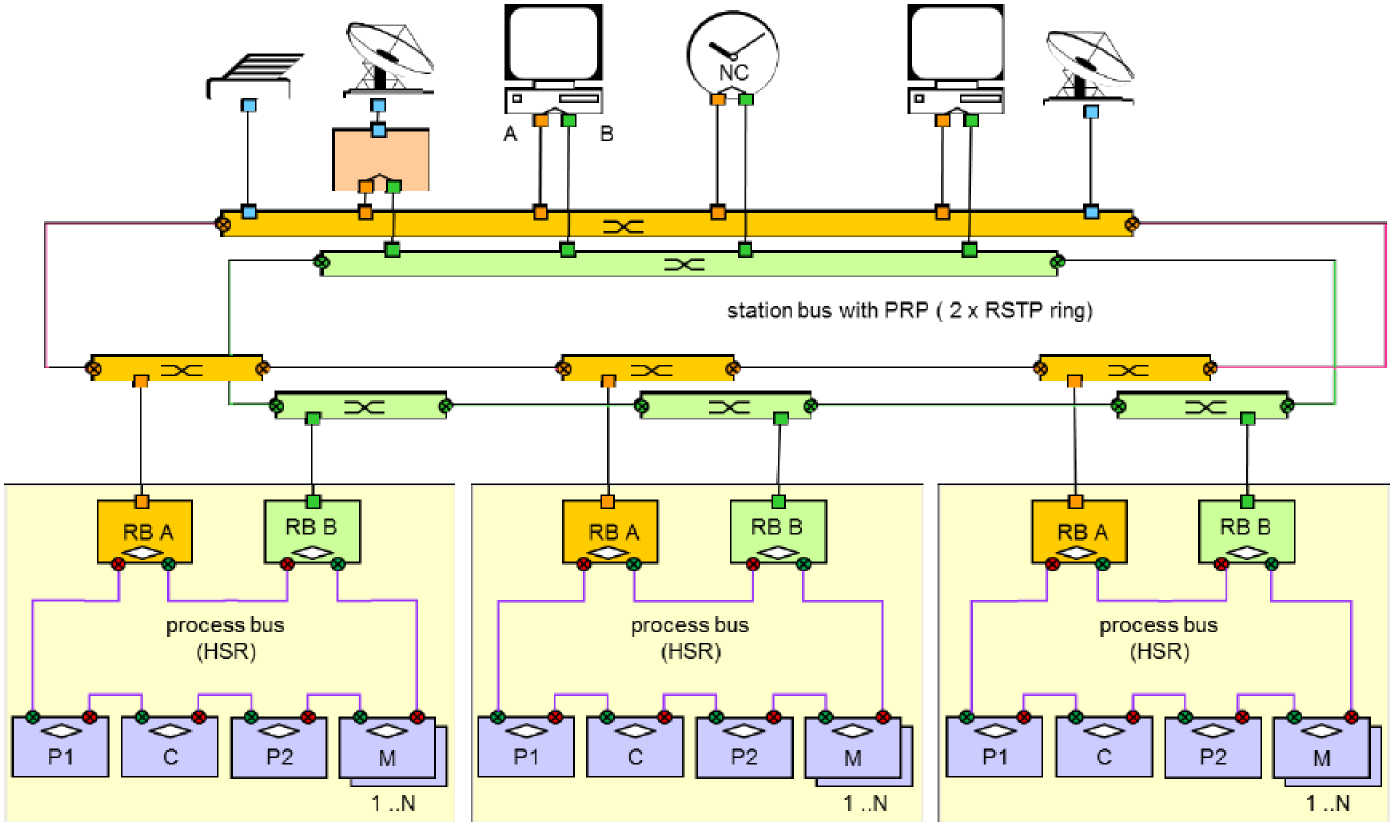
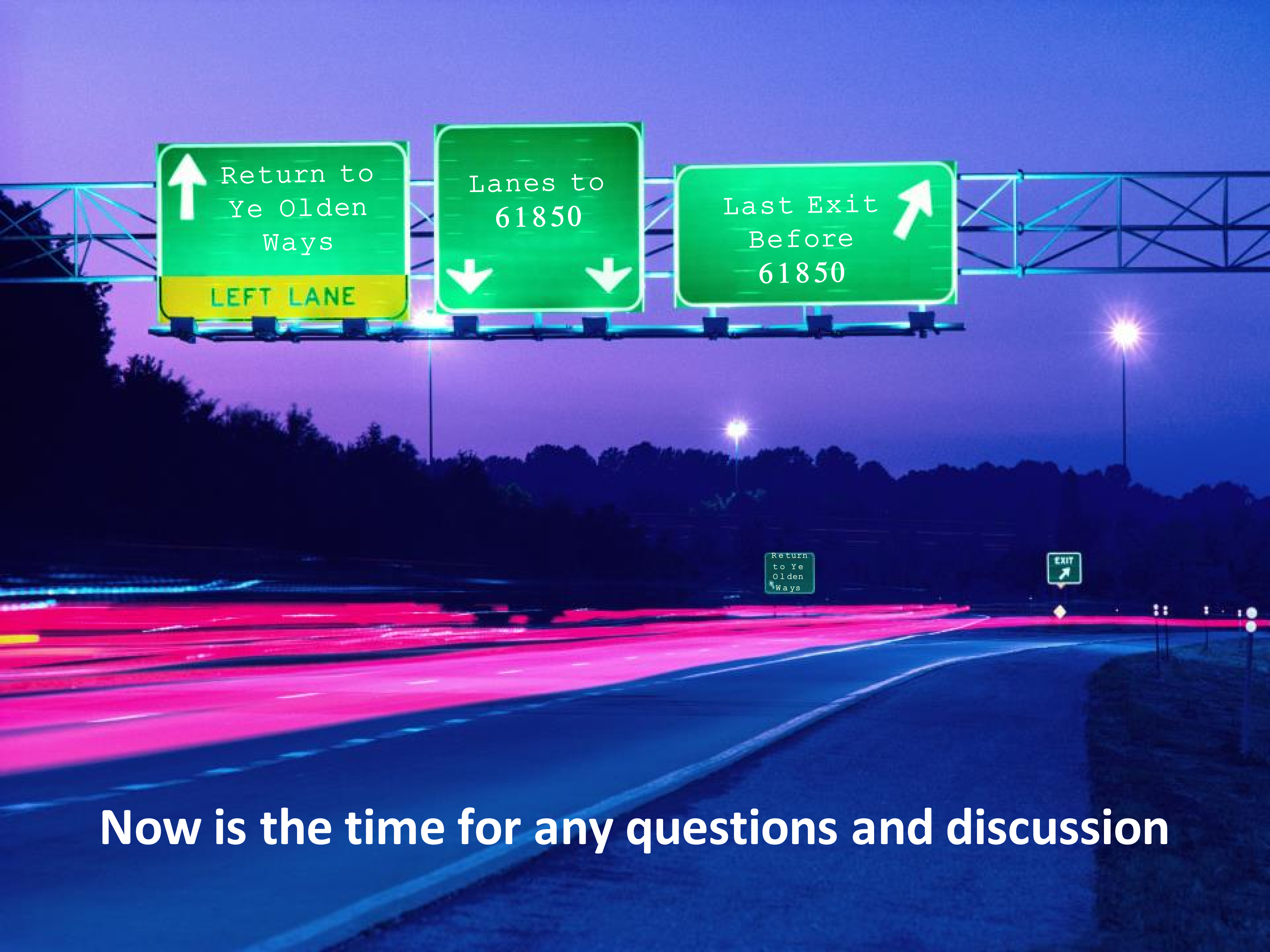


Figure 51 – Station bus as dual PRP ring and process bus as HSR ring

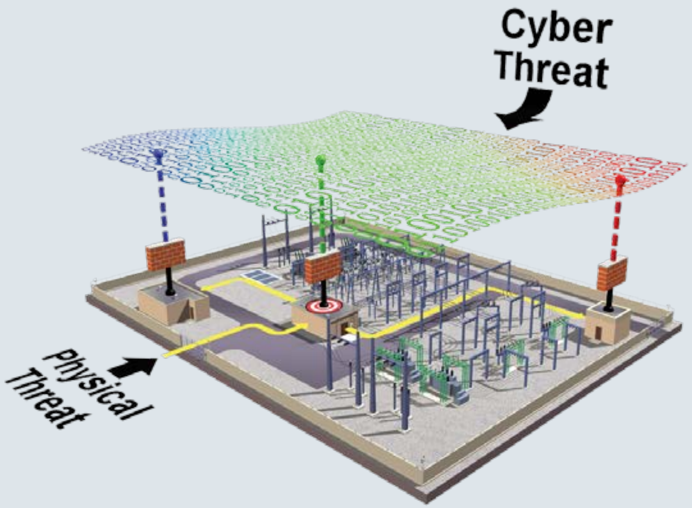
CONCLUSIONS

- 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



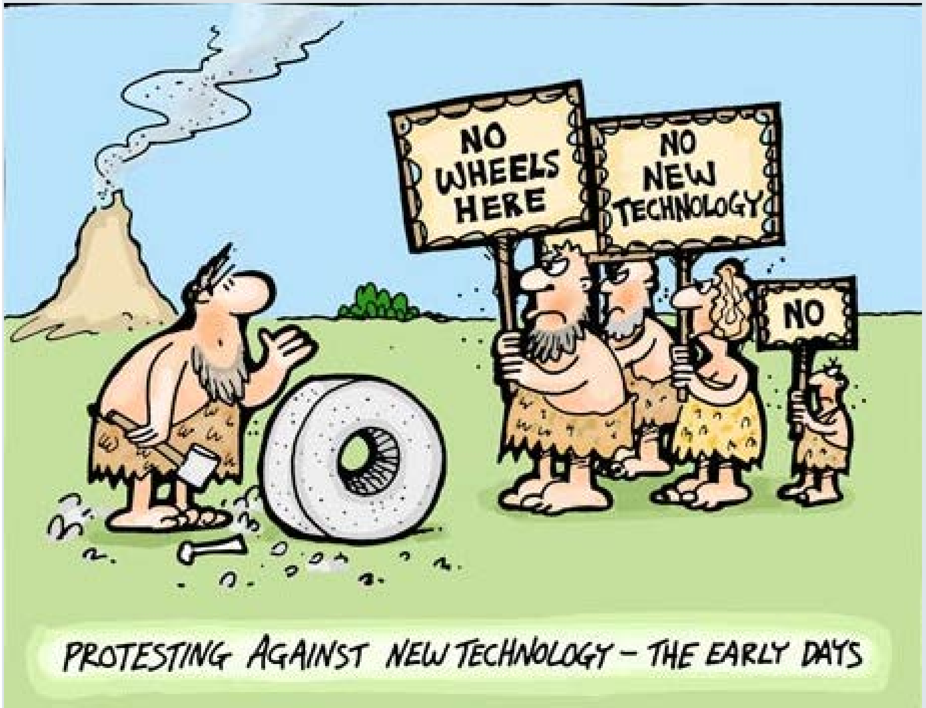
Now is the time for any questions and discussion

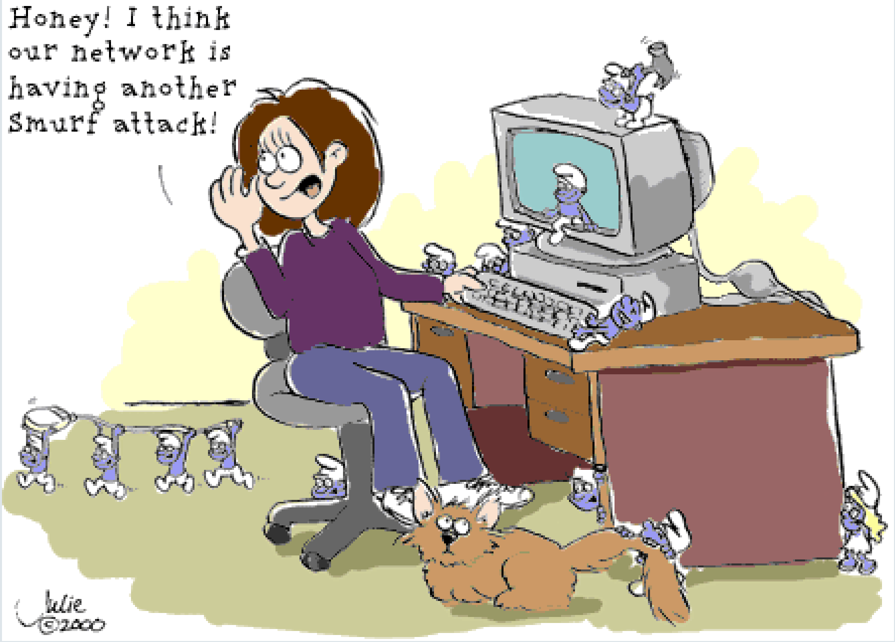
NERC Roundtable Forum



Authors:
Eric Stranz, Business Development Manager, Siemens

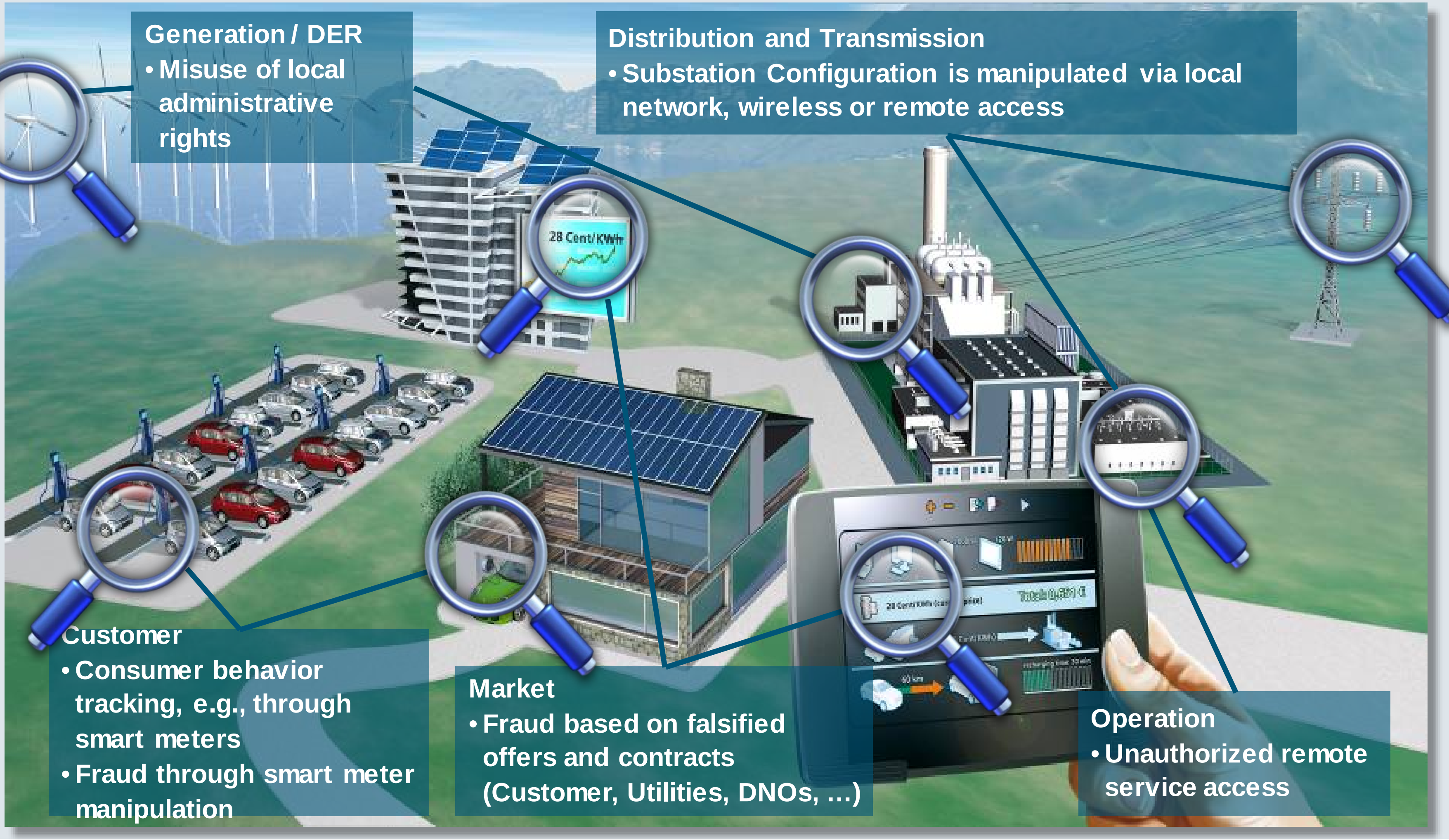
Motivation


NO WHEELS HERE
NO NEW TECHNOLOGY
NO
PROTESTING AGAINST NEW TECHNOLOGY – THE EARLY DAYS

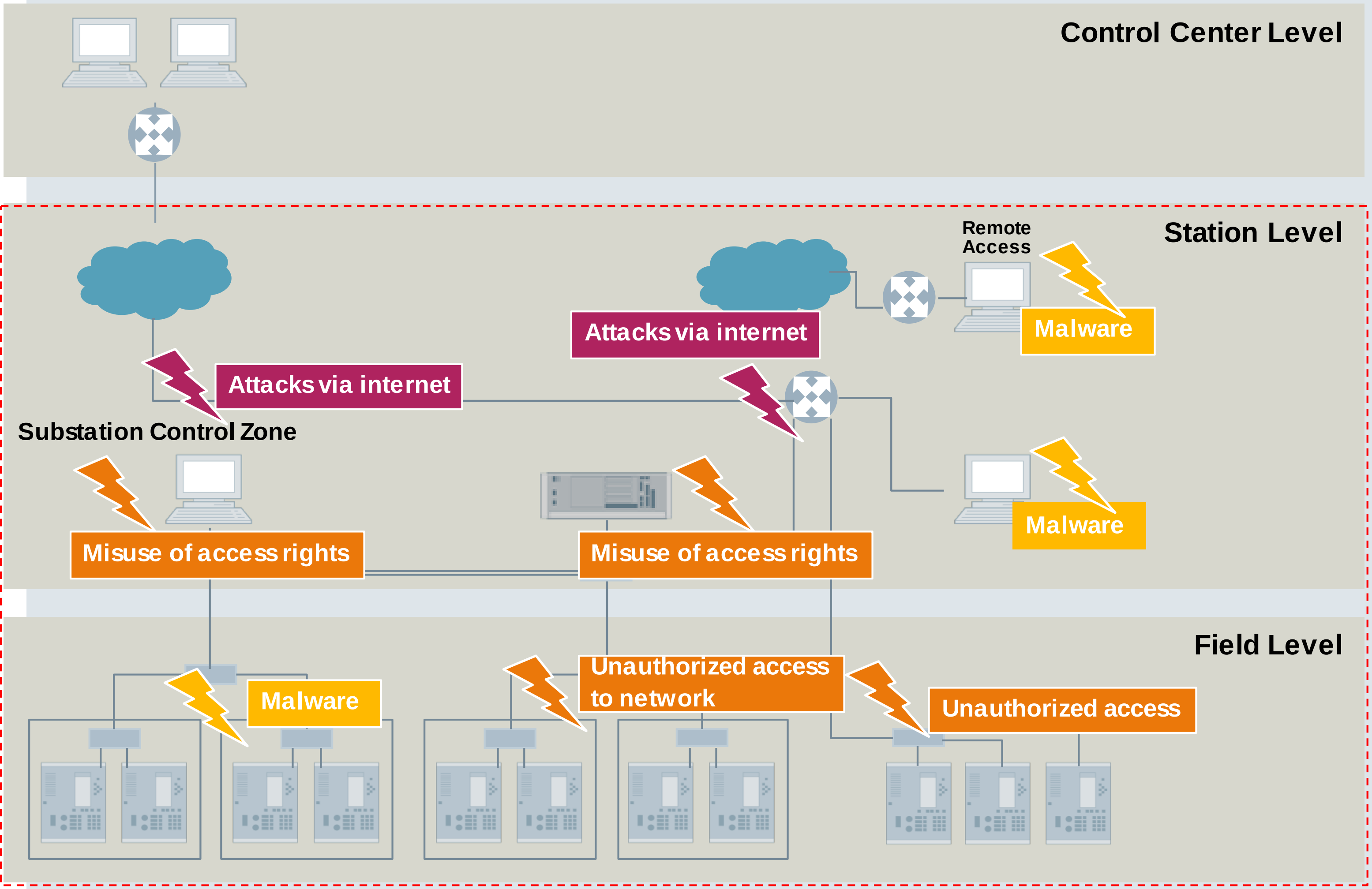

Honey! I think our network is having another Smurf attack!

NERC Roundtable Forum

NERC CIP – Cyber security for TSO and Generation



Cyber Threat Potential

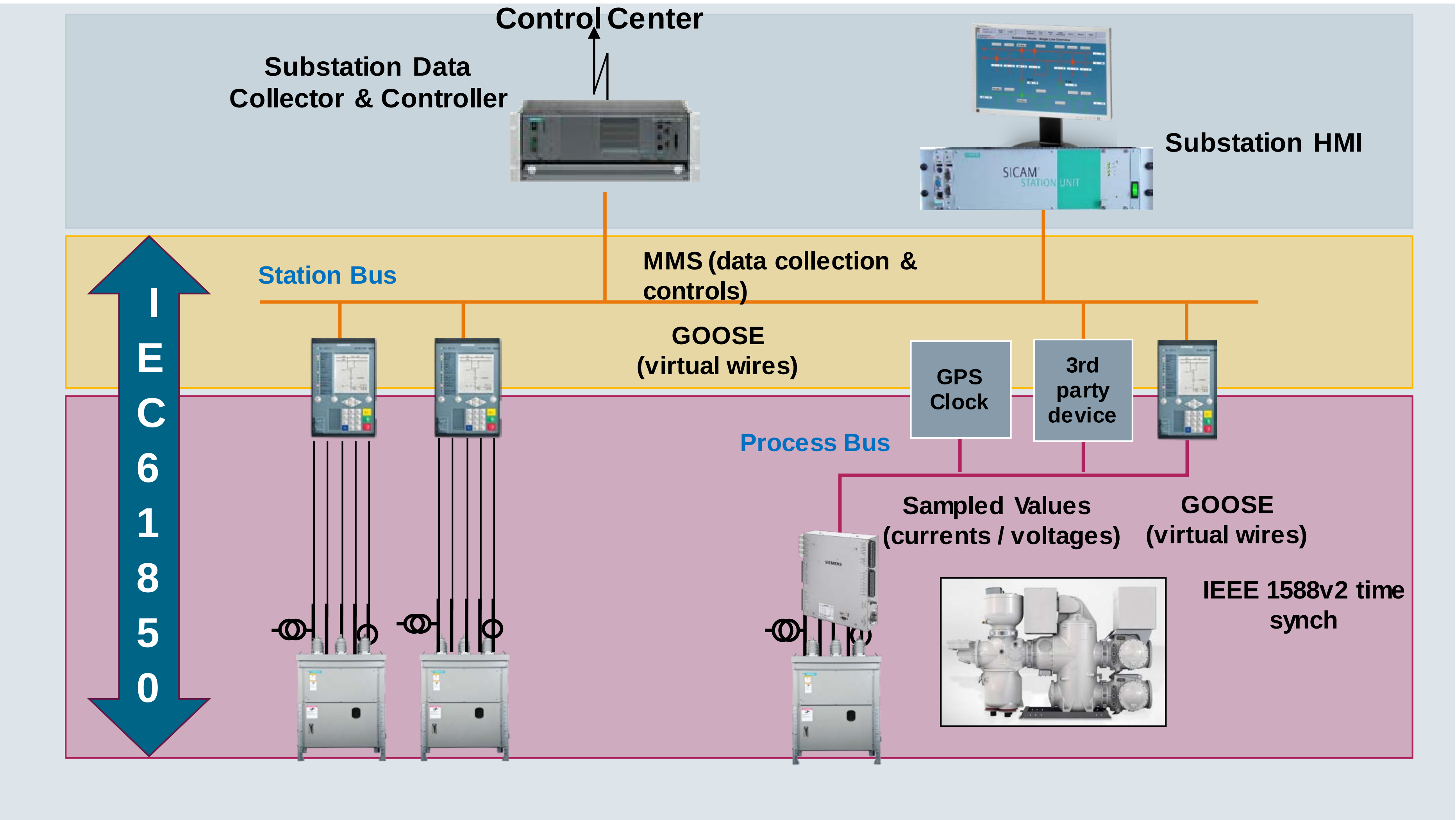


Possible Attackers:

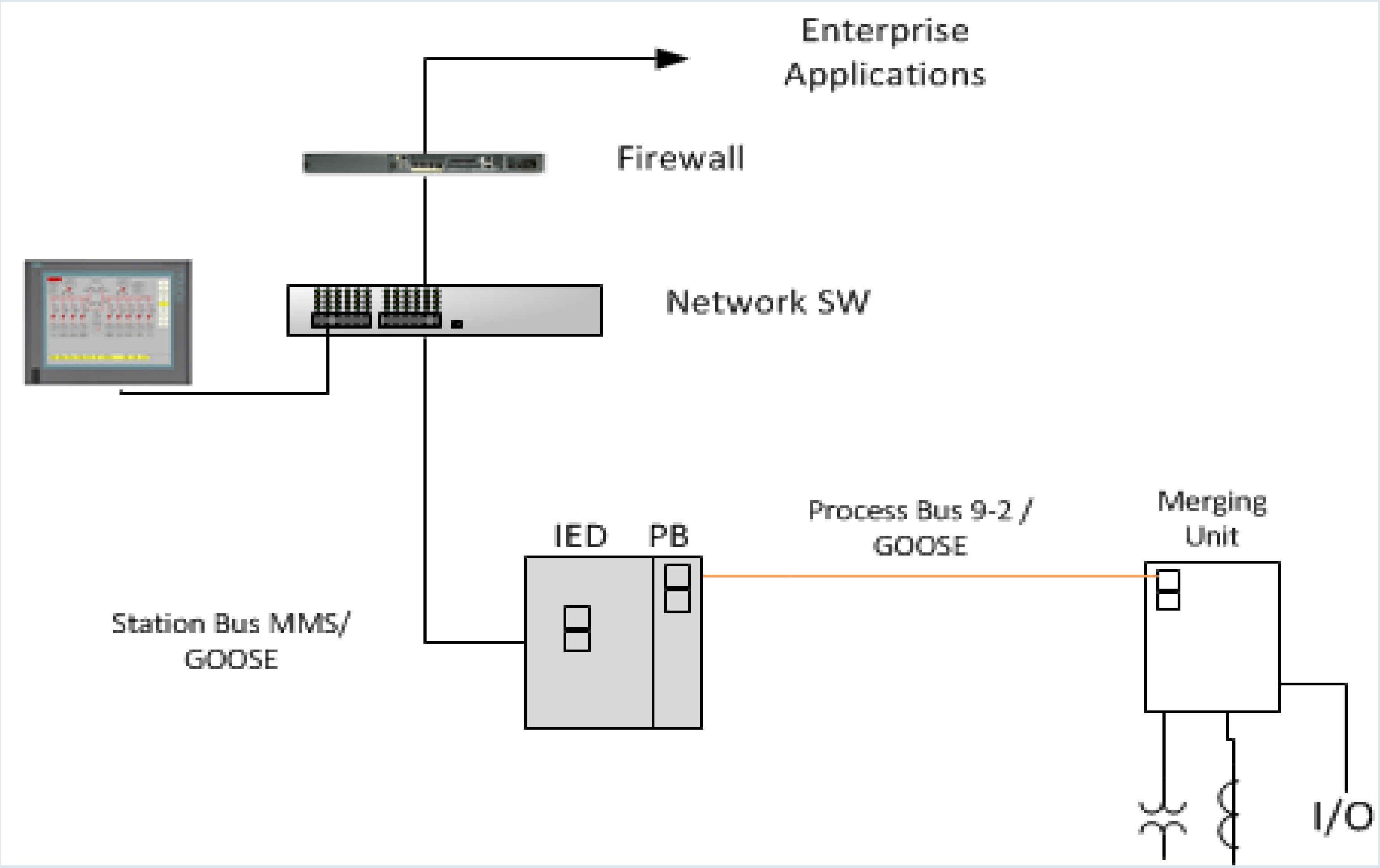
- Countries
- Criminal organizations
- Script kiddies
- Insider
- Spoofing
- Malware
- Viruses
- .....

NERC Roundtable Forum

IEC-61850



Network Segmentation – Process and Station Bus Networks



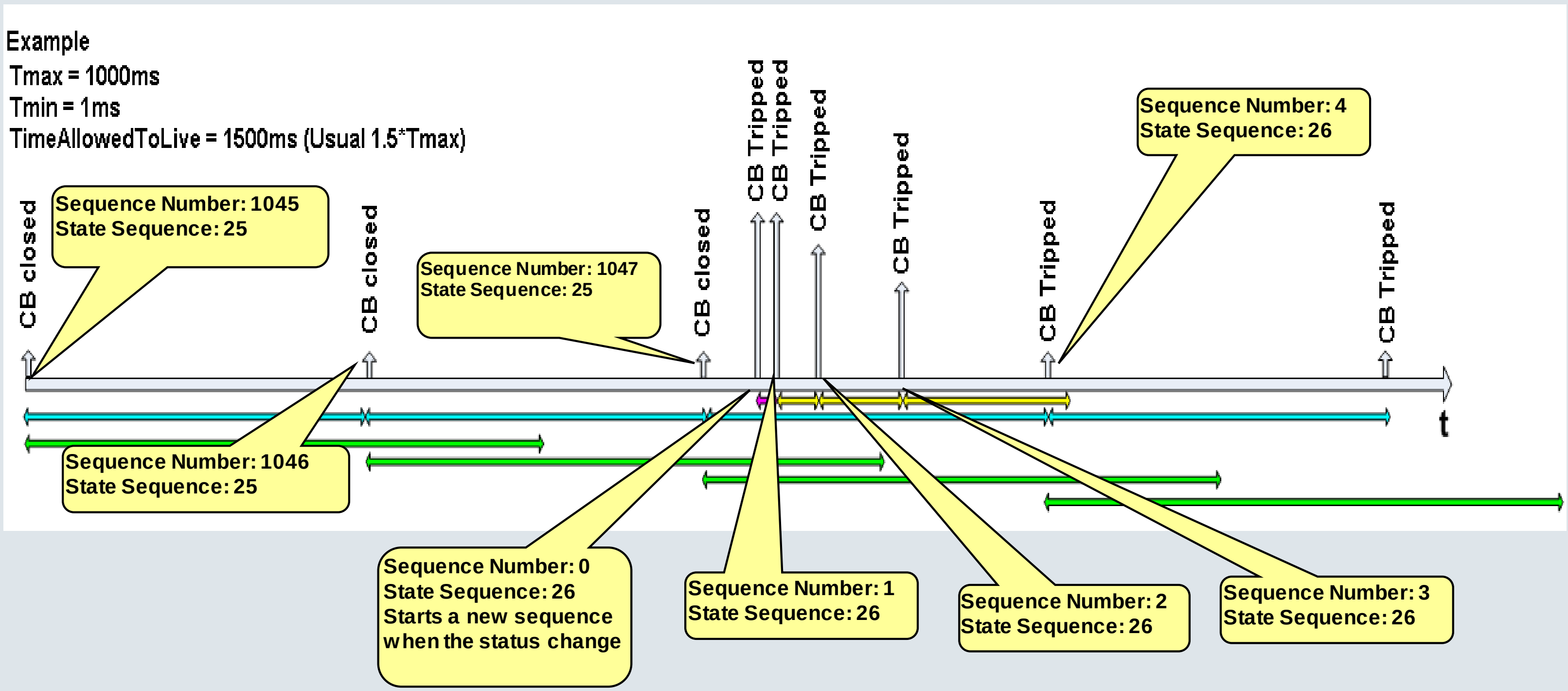
CIP 5 Standards Consolidated FAQ Oct. 2015 # 23

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.

A proposed re-write of CIP 5 Standards Consolidated FAQ Oct. 2015 # 23

IEC 61850 is an **architecture for utility automation systems, including substations, that includes several protocols. T**hus 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 t**ime-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** protocol**s** to determine **what R**outable communication exists. **Any** TCP/IP network **supporting communication protocols above layer 2** is considered **R**outable 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.**

IEC 61850 Monitoring– GOOSE and SV



A well designed Substation system can determine the health of the network by monitoring sequence or state alarms and indications for fast network diagnosis

NERC Roundtable Forum

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?

Process

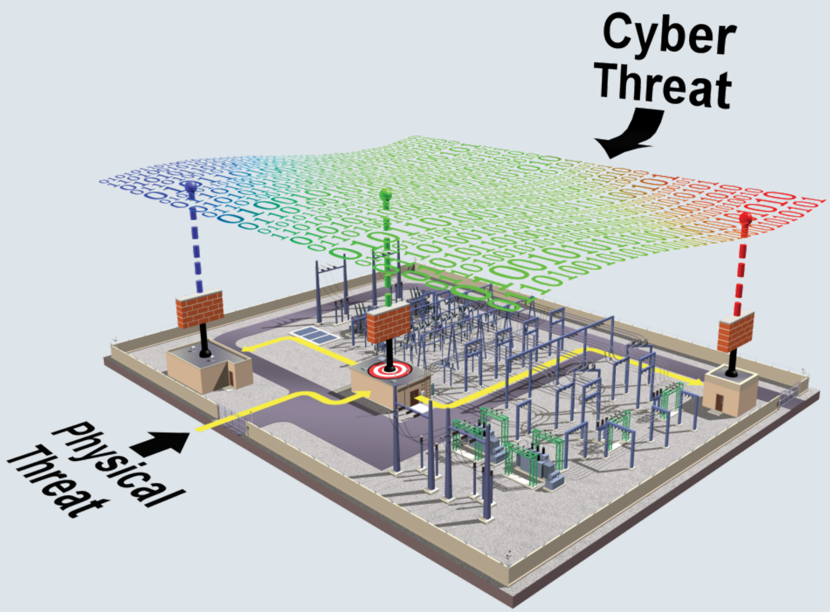
1.) Assess stations designations based on the CIP -014-01 (4.1.1.2)
2.) Define the (BES) Cyber System (formerly Critical Cyber Assets)
3.) Define Physical Security Perimeter (PSP)
4.) Define Electronic Security Perimeter(s) (ESP)
5.) Provide a Cyber Security Framework to Cyber Assets per CIP Standards
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.

NERC Roundtable Forum

Physical & Cyber security

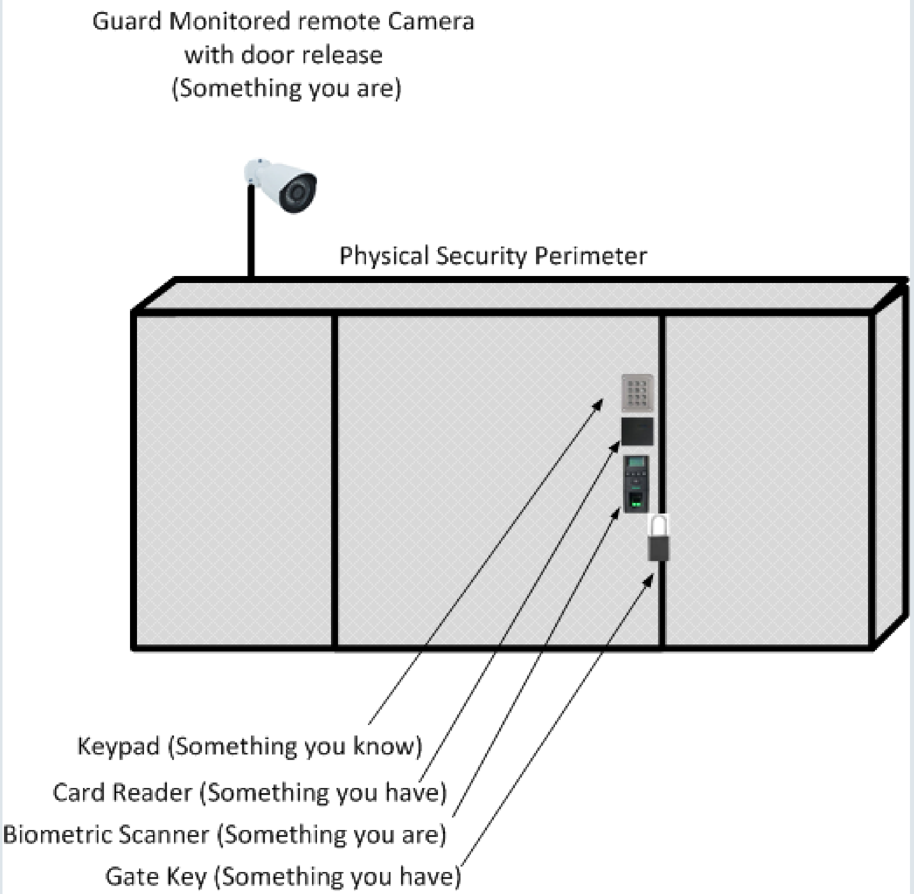
- The physical security requirements
  - Need of authentication before entrance of station
  - Recognize and Alarm in case of unauthorized access
  - Protection against unauthorized access
- Cyber security
  - Mitigate misuse of access rights
  - Authentication of access
  - Prevents from outside threads and attacks on infrastructure



NERC Roundtable Forum

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)

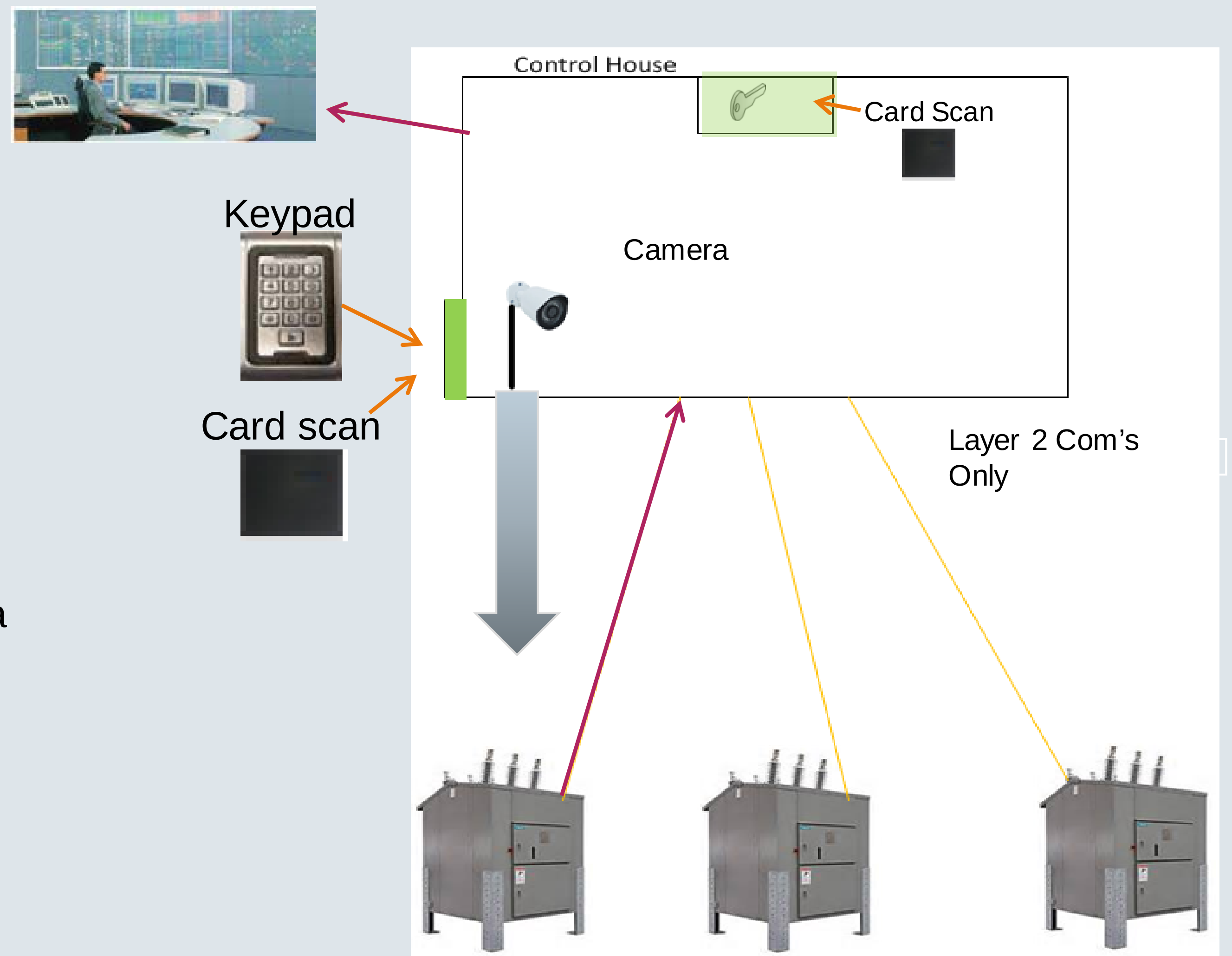
Card Scanners, Cameras, Authentication Systems typically are already in place for a NERC CIP Station

ESP at the Control House

2 Factor Authentication

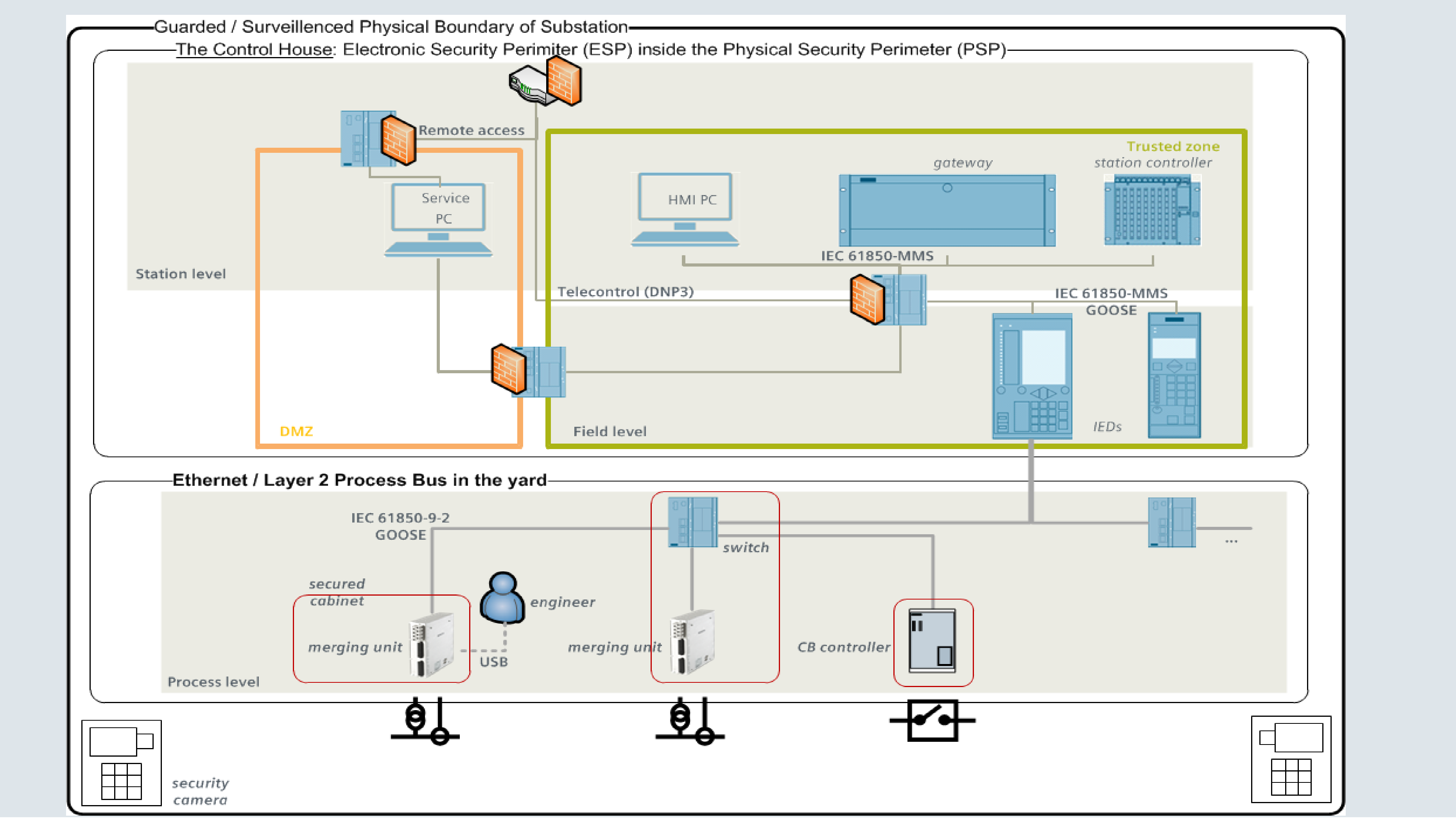
Card Scan to Retrieve Key for Breakers

Door switch triggers alarm where camera monitors activity



NERC Roundtable Forum

Network Design

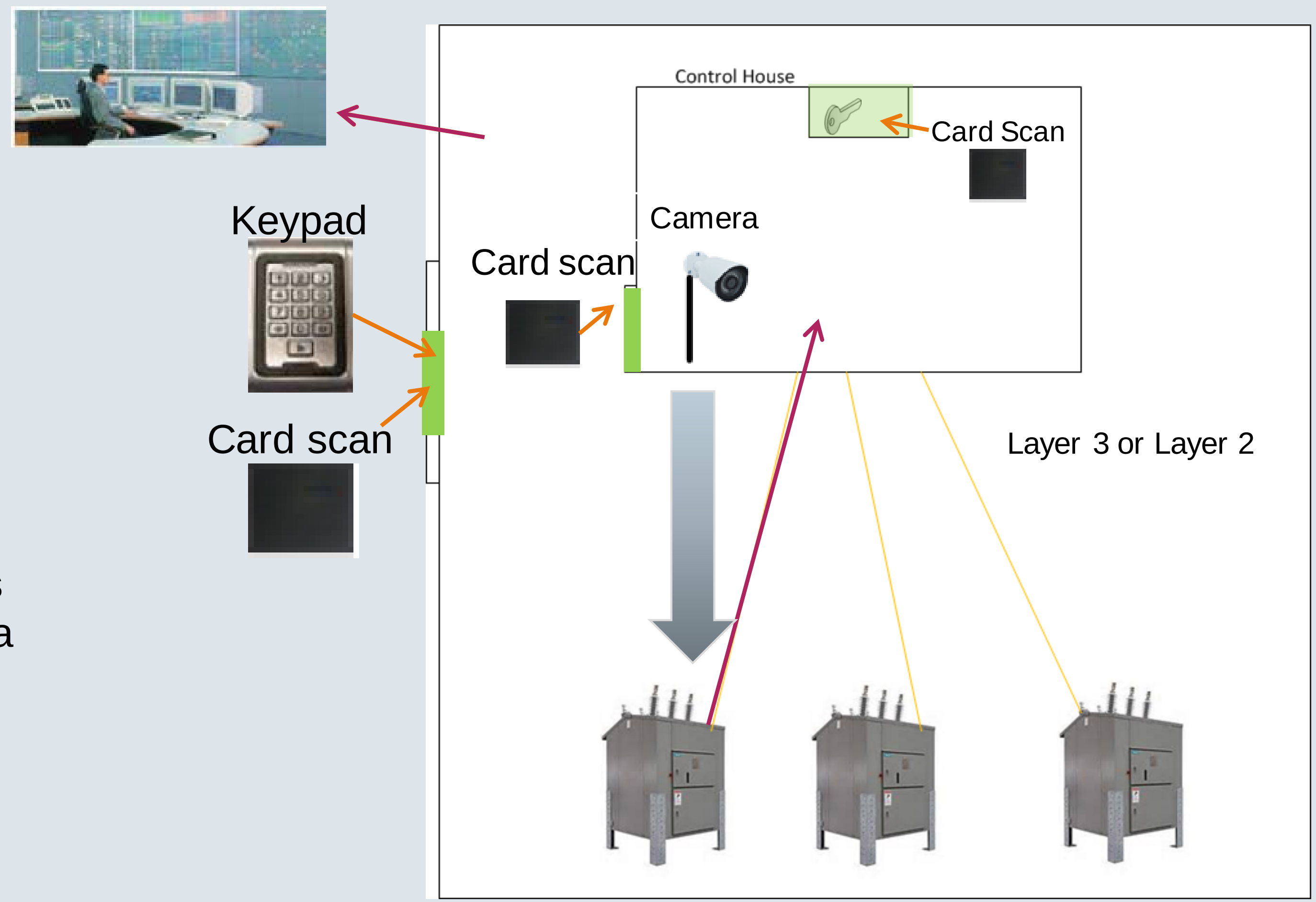


ESP at the Substation Fence

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
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

NERC CIP Implications of IEC 61850 in Transmission Stations

Scott R Mix, CISSP, CIP Technical Manager, NERC

RELIABILITY | ACCOUNTABILITY




Agenda

- Application of NERC Standards
- NERC Definitions
- What Does it Mean? (Compliance Implications)
- Effective Dates (Implementation Timeframes)

Application of NERC Standards

- 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
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Application of NERC CIP Standards

- 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

Definitions

- ***Cyber Asset***: Programmable electronic devices, including the hardware, software, and data in those devices.

Definitions

- ***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.

Definitions

- ***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

Definitions

- ***Electronic Security Perimeter (ESP)***: The logical border surrounding a network to which BES Cyber Systems are connected using a routable protocol.

Definitions

- ***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

Definitions

- ***Electronic Access Point (EAP)***: A Cyber Asset interface on an Electronic Security Perimeter that allows routable communication between Cyber Assets outside an Electronic Security Perimeter and Cyber Assets inside an Electronic Security Perimeter.
  - 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

Definitions

- ***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

Definitions

- ***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

Definitions

- CIP-003-7, Attachment 1, Section 3:

__Section 3.__ <u>Electronic Access Controls</u>: 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.

Exclusions

- **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 issues 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

Compliance Implications

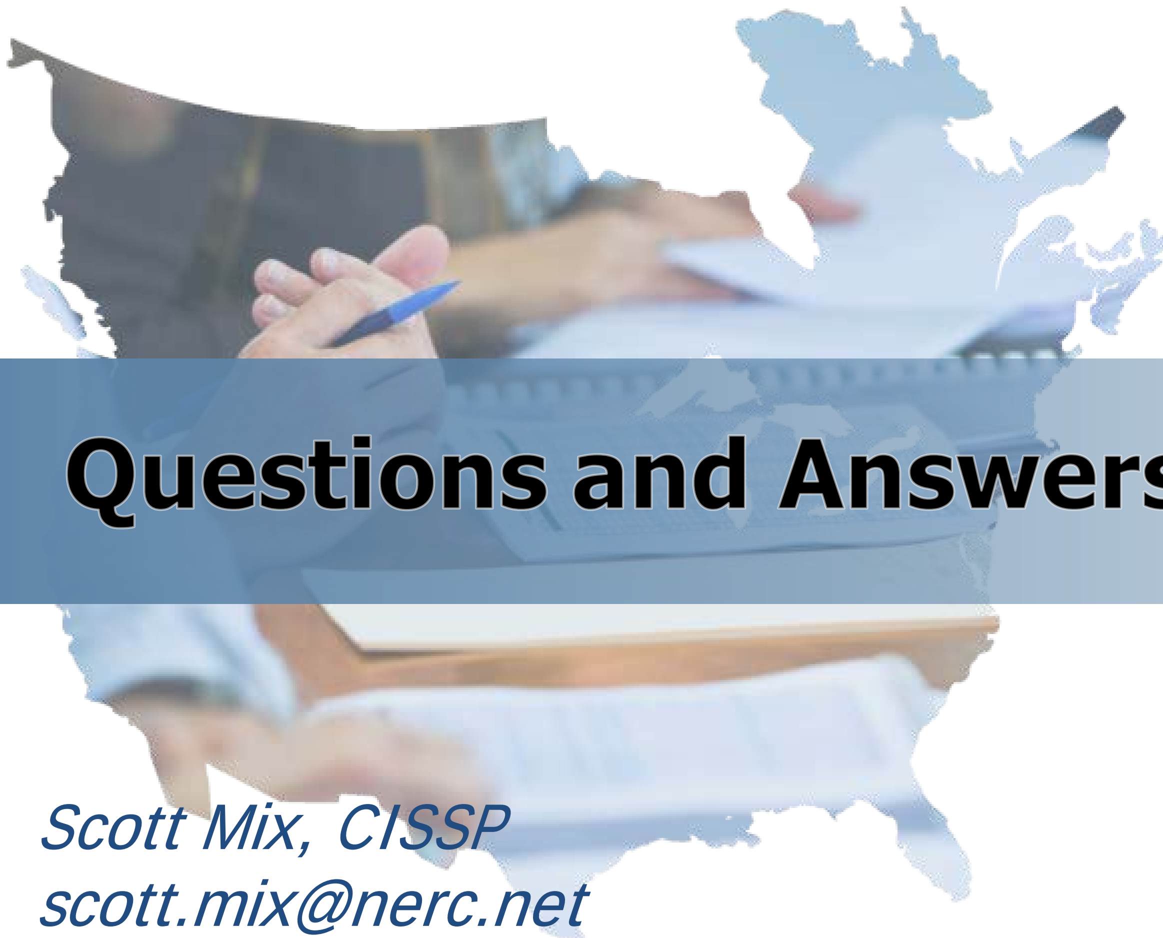
- What does this mean for low impact implementations?
  - There are no ESP requirements at low impact locations
    - However, there are requirements for controlling external routable access to low impact BES Cyber Systems
  - 61850 devices which communicate externally (i.e., to devices outside the station) 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 of there is no routable external access

Compliance Implications

- 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

Compliance Implications

- 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