Welcome

Enabling Wide Area Monitoring, Protection, and Control (WAMPAC) Systems with 61850 and the Importance of Time Synchronization

Ralph Mackiewicz

VP, Business Development
SISCO

Ralph@sisconet.com

SISCO provides communication and integration solutions to support model-driven integration of utility operations using IEC 61850 for power systems, wide area remedial action and measurement systems.

Debra Henderson

Director, Power Utility Markets
Symmetricom
dhenderson@symmetricom.com

Symmetricom helps power utilities mitigate large scale outages and operate the grid more efficiently by providing accurate, secure and reliable time synchronization solutions.

Agenda

- Overview of IEC 61850
- IEC 61850 for Wide Area Communications
- WAMPAC Applications
  - Wide Area Protection and Control via Centralized Remedial Action Systems (C-RAS) using GOOSE
  - Wide Area Measurement Systems (WAMS) using Sampled Values (SV)
- Time Impact on C-RAS & WAMS
- Why Have a Timing Strategy?
- Elements of a Timing Strategy
- Case Study for WAMS
- Key Takeaways
- Q&A

Definitions:

Interoperability and Integration

The ability of computer systems to exchange information with other systems and to cooperatively implement a useful process or function for the system owner/user.

Interoperability and Integration

- Easy to Achieve:

Nearly anything is possible with enough money and development effort

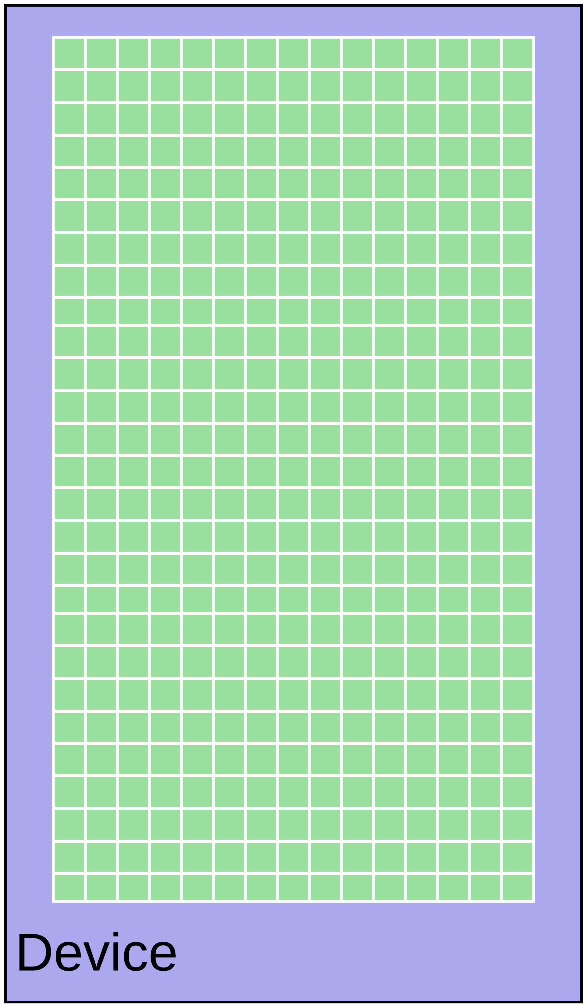
A Better Way

- Interoperability and Integration without having to program it all yourself

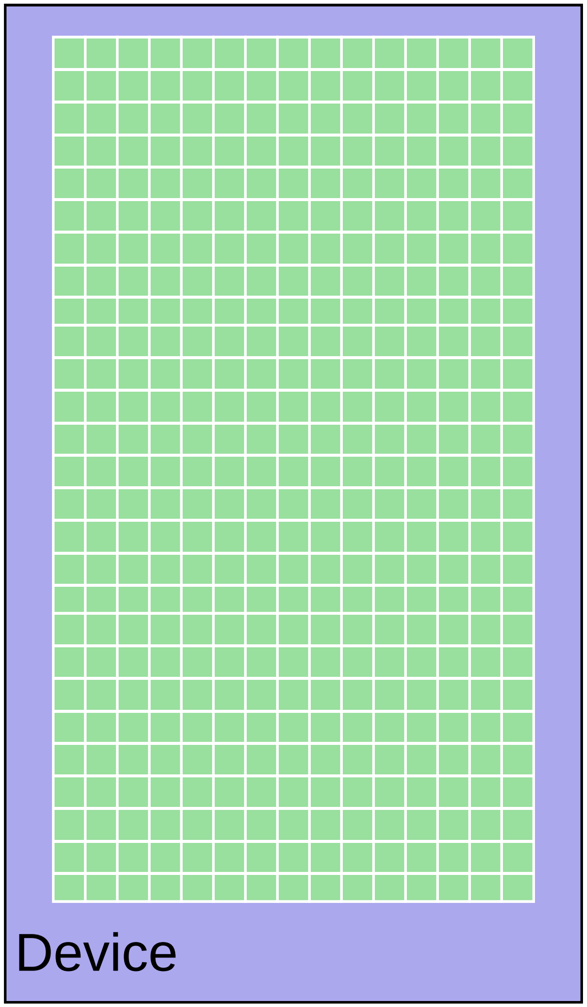
- Where applications and devices are inherently capable of interoperating with other systems and performing integrated application functions in a cooperative and distributed manner.

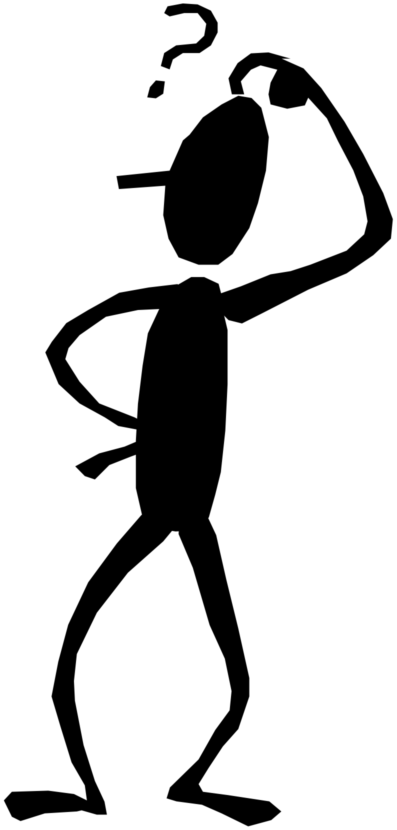
- This is only possible with standards.

Typical Legacy Protocol Data Model



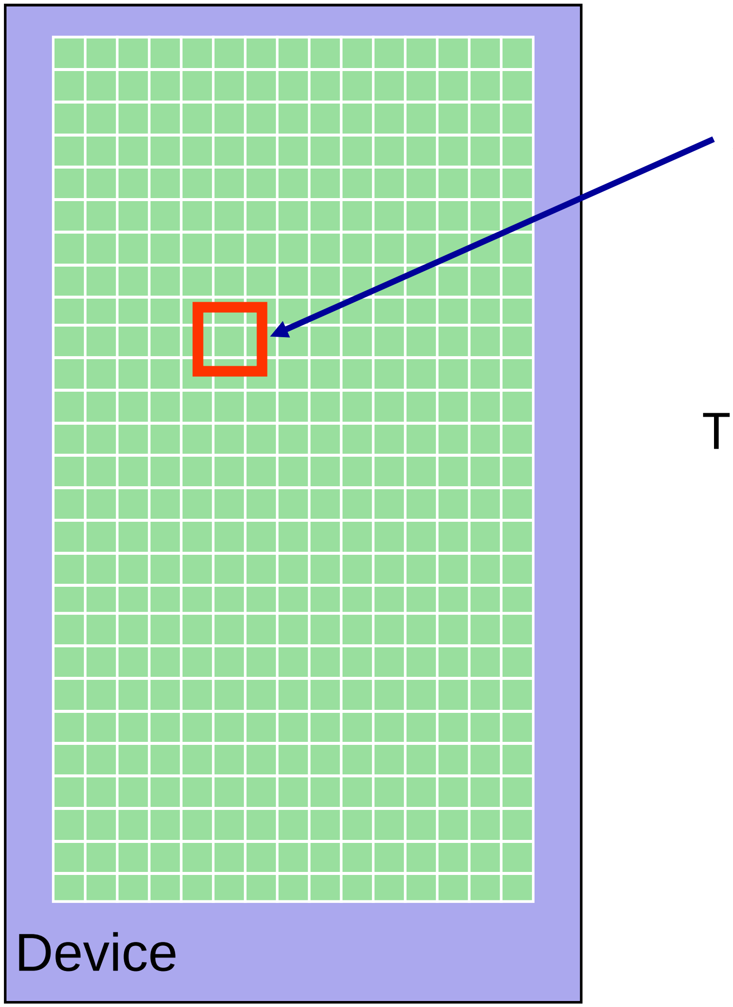
Typical Legacy Protocol Data Model





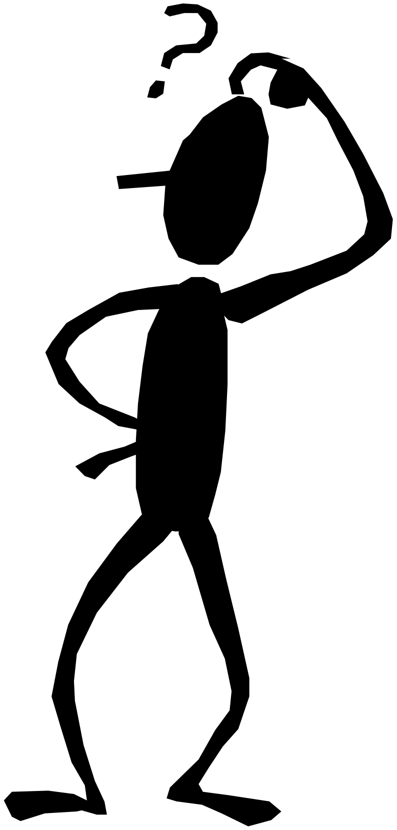
I need the Phase A voltage for the 345KV primary feeder

Typical Legacy Protocol Data Model



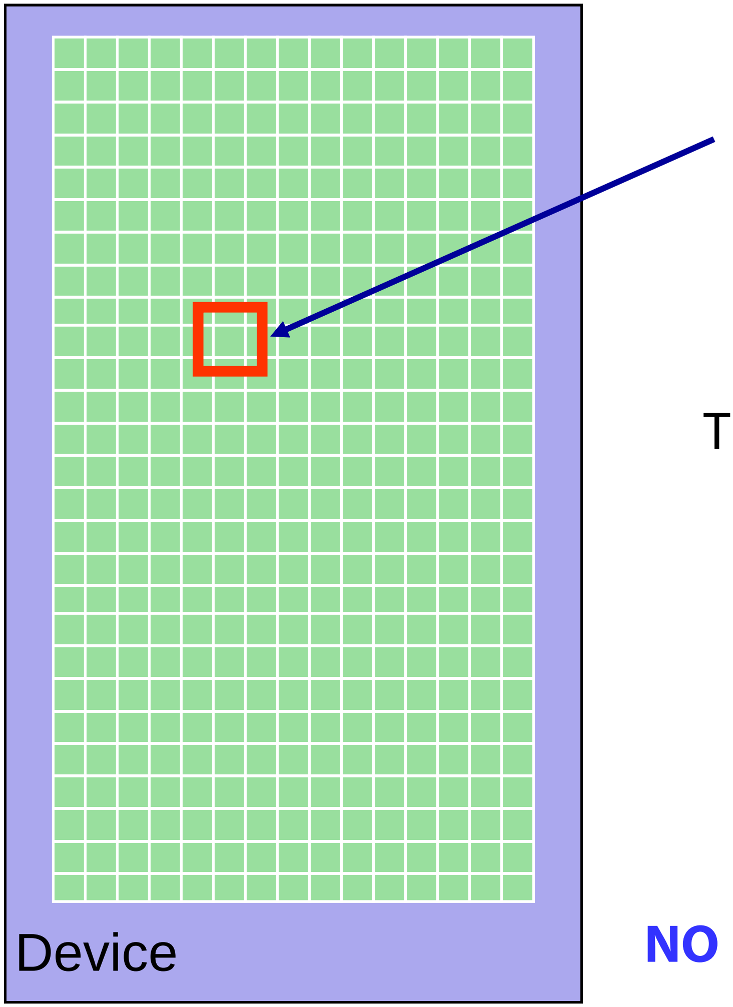
It is in:
Object #6,
Variation #2,
Index #27

That's intuitive?

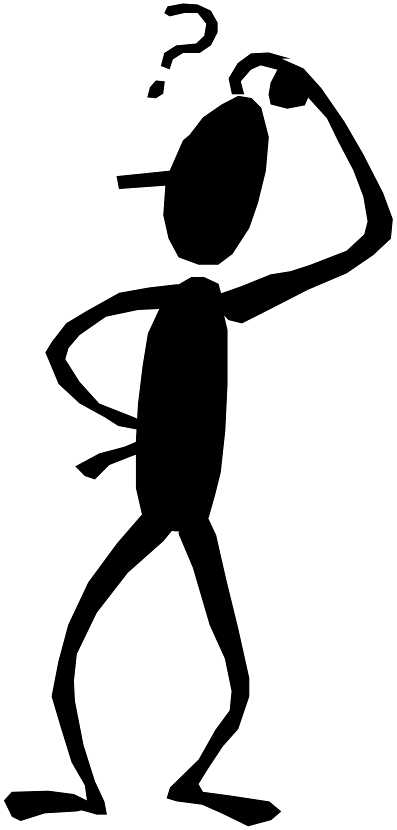


I need the Phase A voltage for the 345KV primary feeder

Typical Legacy Protocol Data Model



It is in:
Object #6,
Variation #2,
Index #27

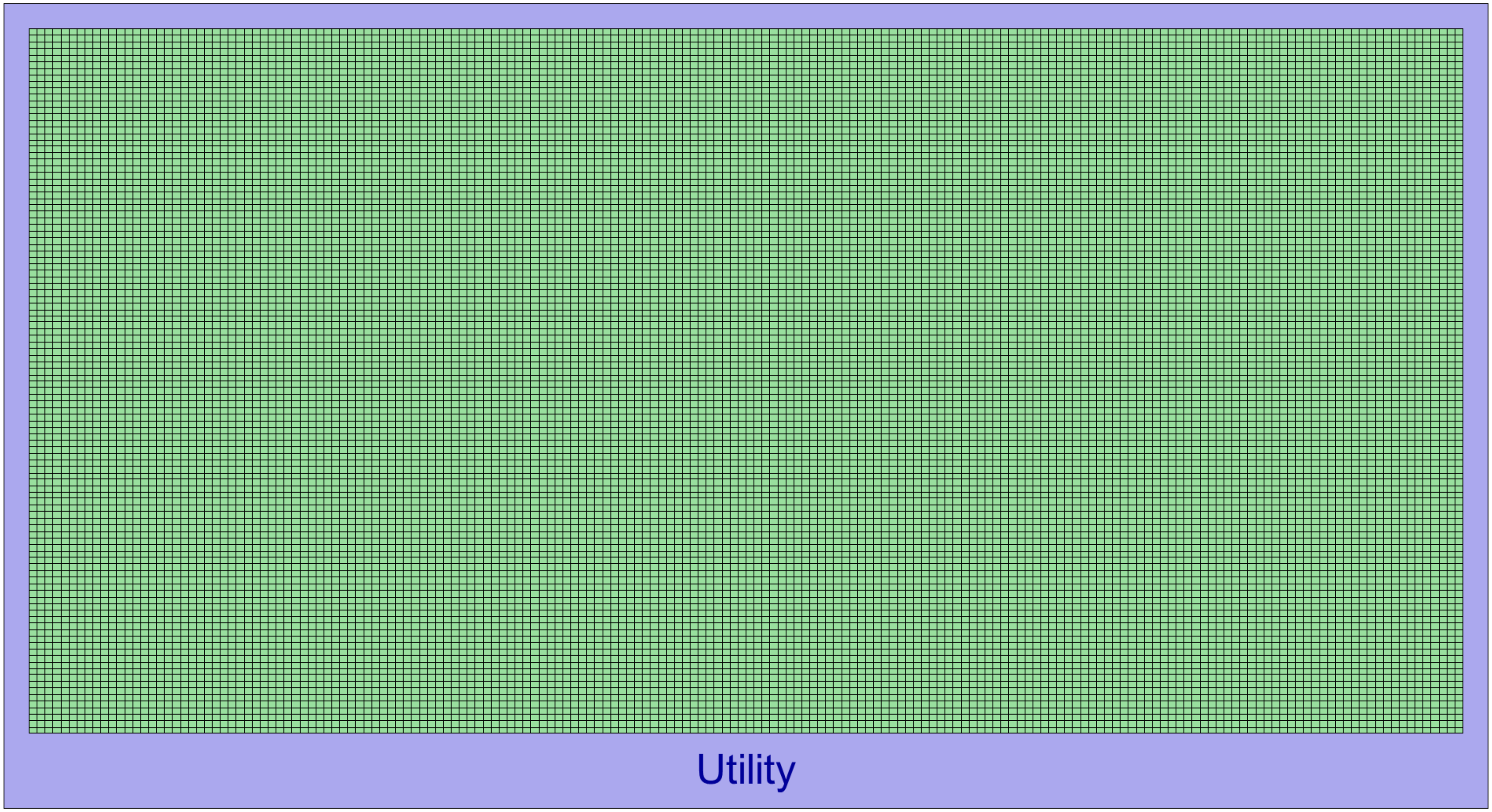


That's intuitive?

I need the Phase A voltage for the 345KV primary feeder

NO POWER SYSTEM CONTEXT

Device Tags Don’t Scale



Try to find a breaker position tag in this model

A New Approach Needed

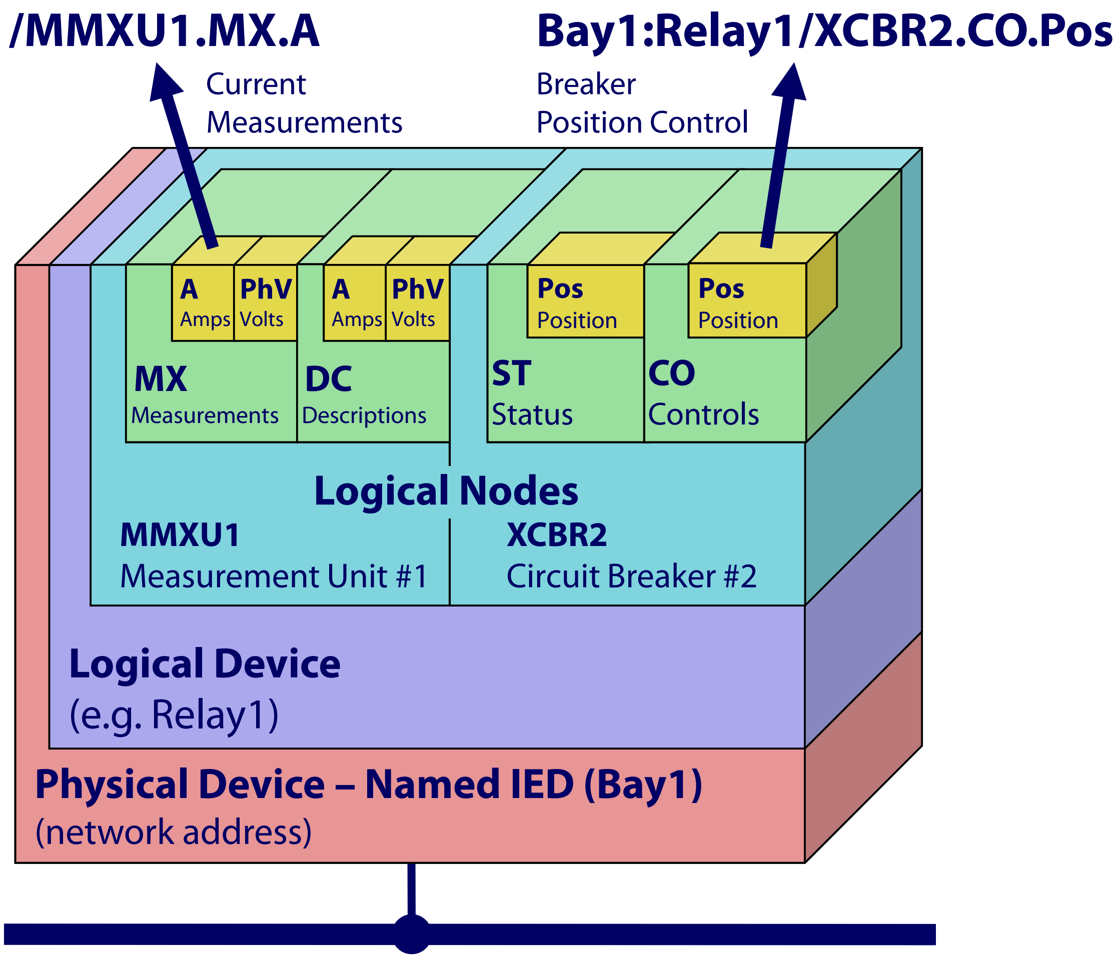
- For protocols to provide interoperability and integration at the system level they need to:
  - Specify the bytes/format (protocol) of the data on the wire
  - **Specify the meaning of data in power system context**
  - **Specify the behavior of the device serving the data**
  - **Specify how the devices and applications are configured**

IEC 61850 : An Innovative New Approach

- Not just protocols
- Standardized Data and Service/Behavior Modeling
- Standardized XML for System and Device Configuration
  - Substation Configuration Language (SCL)
- Standardized Communications Profiles for Specific Applications:
  - Station Level Monitoring and Control over TCP/IP
  - Protection and Control – Multicast **GOOSE** over Ethernet
  - Process I/O – Multicast **Sampled Values** over Ethernet
  - **Wide Area Measurement , Protection and Control**

IEC 61850 is Model Driven

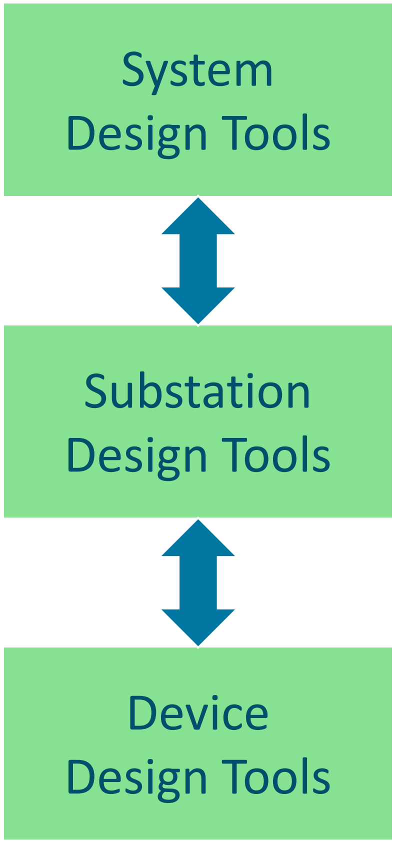
IEC 61850 Object Names Use Power System Context



IEC 61850 Substation Configuration Language (SCL)

- Enables devices and applications to exchange configuration data in a common XML format:
  - Power system connectivity
  - Relationship of devices to the power system used for naming
  - Device functions and settings
  - Network configuration of devices

- Increased Productivity
- Eliminate Integration Barriers



System Design Tools

Substation Design Tools

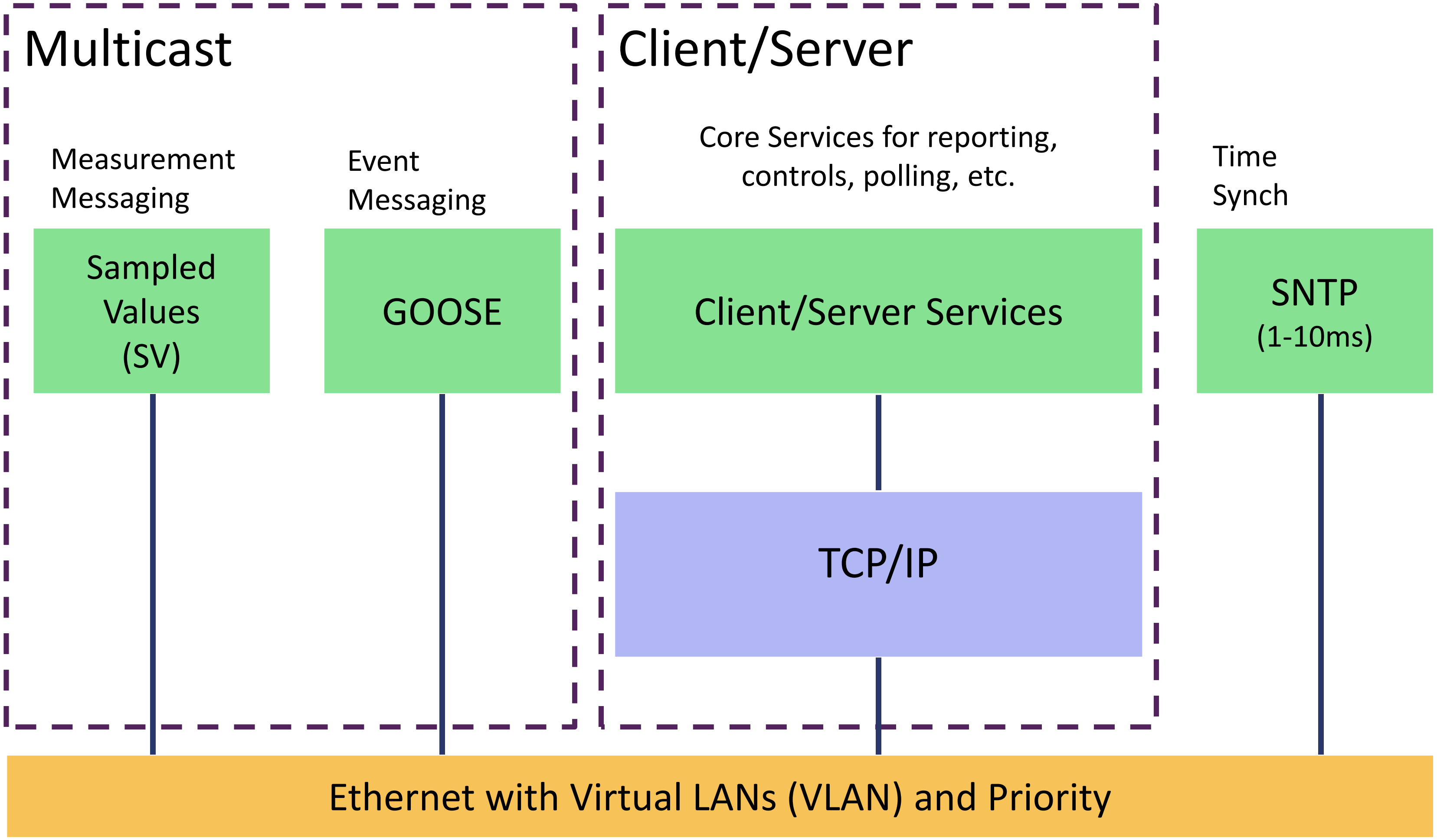
Device Design Tools

IEC 61850 Timestamps and Time Quality

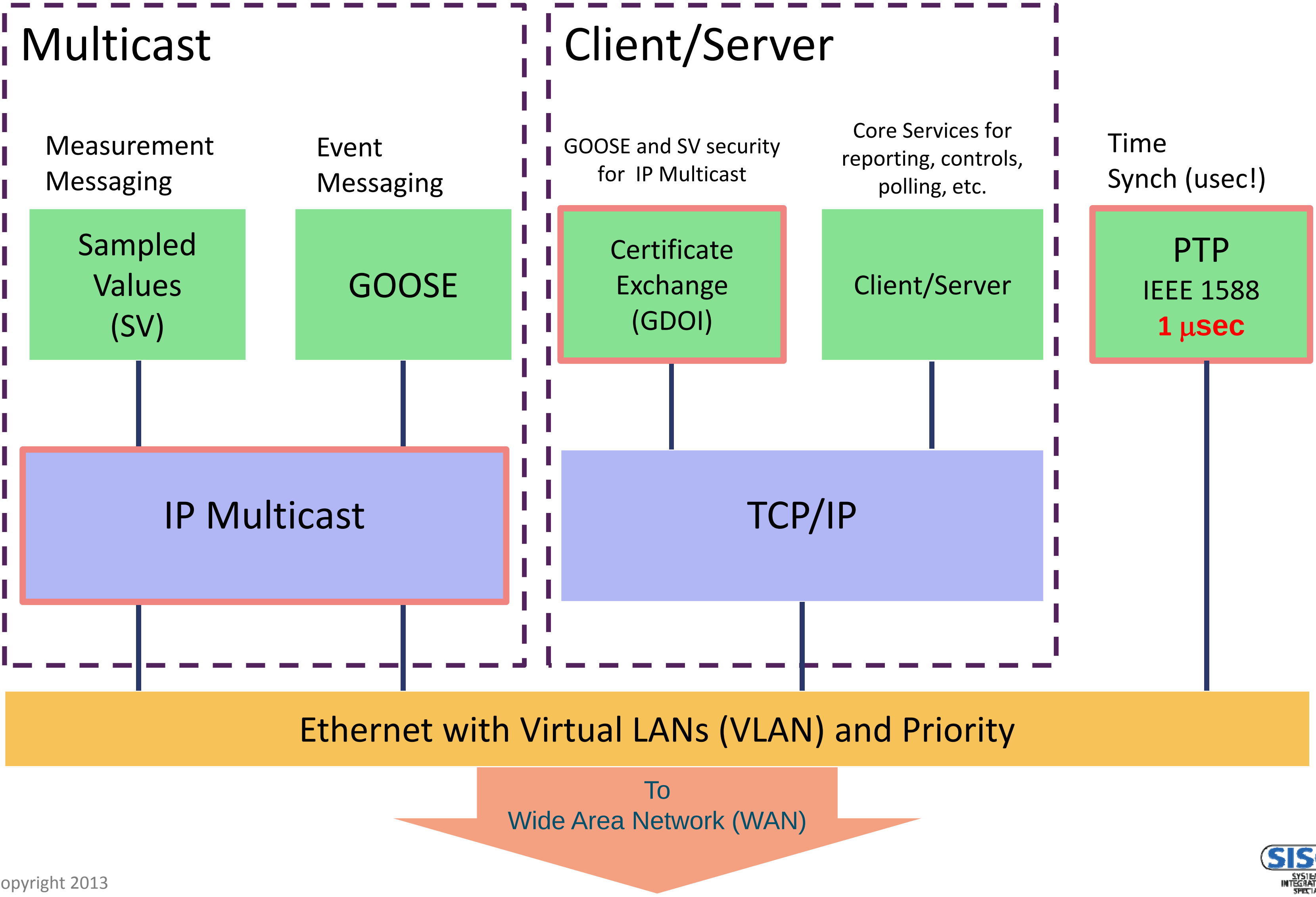
- All status and measurement objects in IEC 61850 have quality flags and timestamps.
- Data quality flags relate to the quality of the data.
- Every IEC 61850 timestamp conveys time quality information in the timestamp itself:
  - Leap Seconds Known
  - Clock Failure
  - Clock Not Synchronized
  - Timestamp accuracy from 10 msec to **1 µsec***

* Common Requirement for WAMPAC

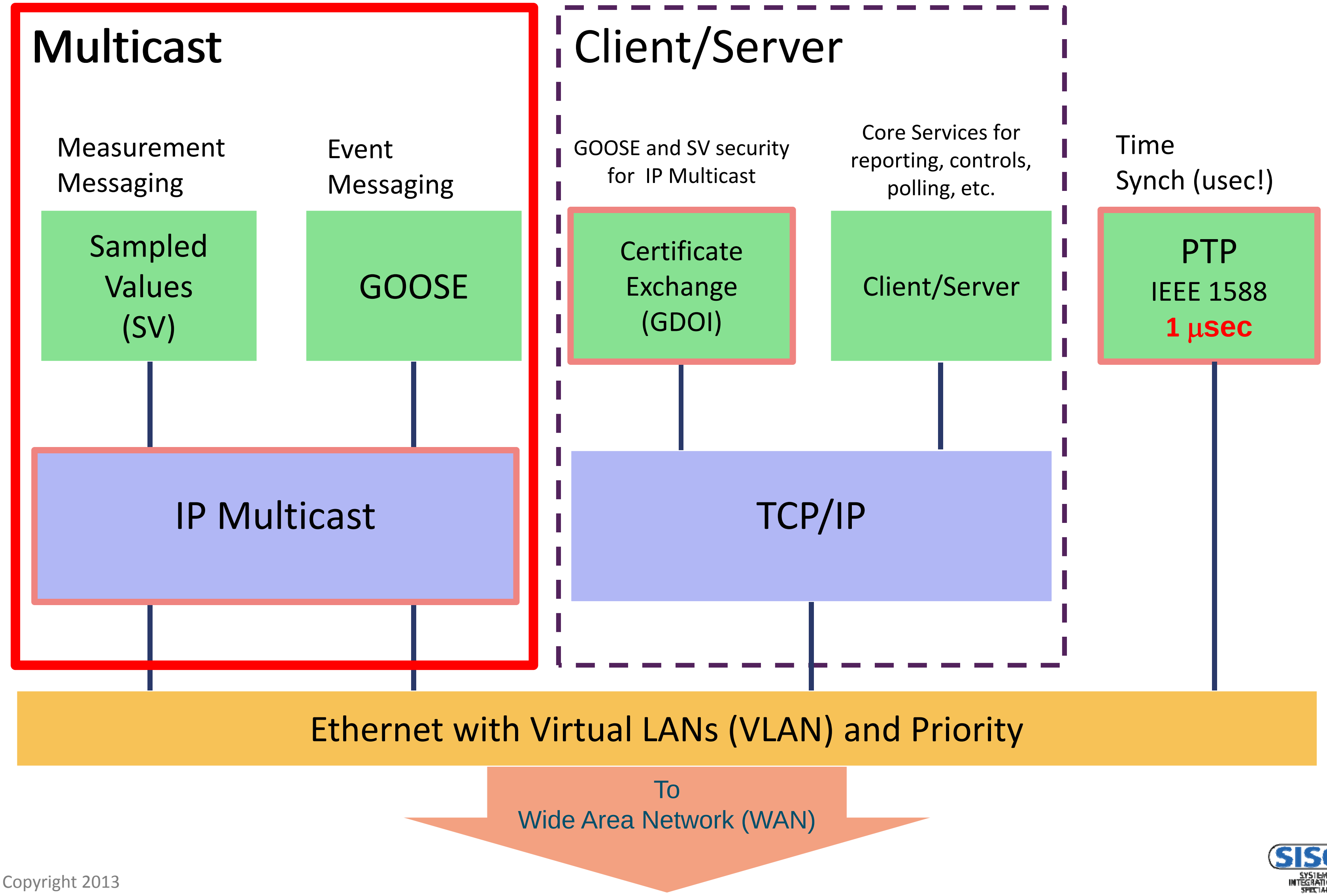
IEC 61850 Substation Profiles



IEC 61850 **Wide Area** Profiles



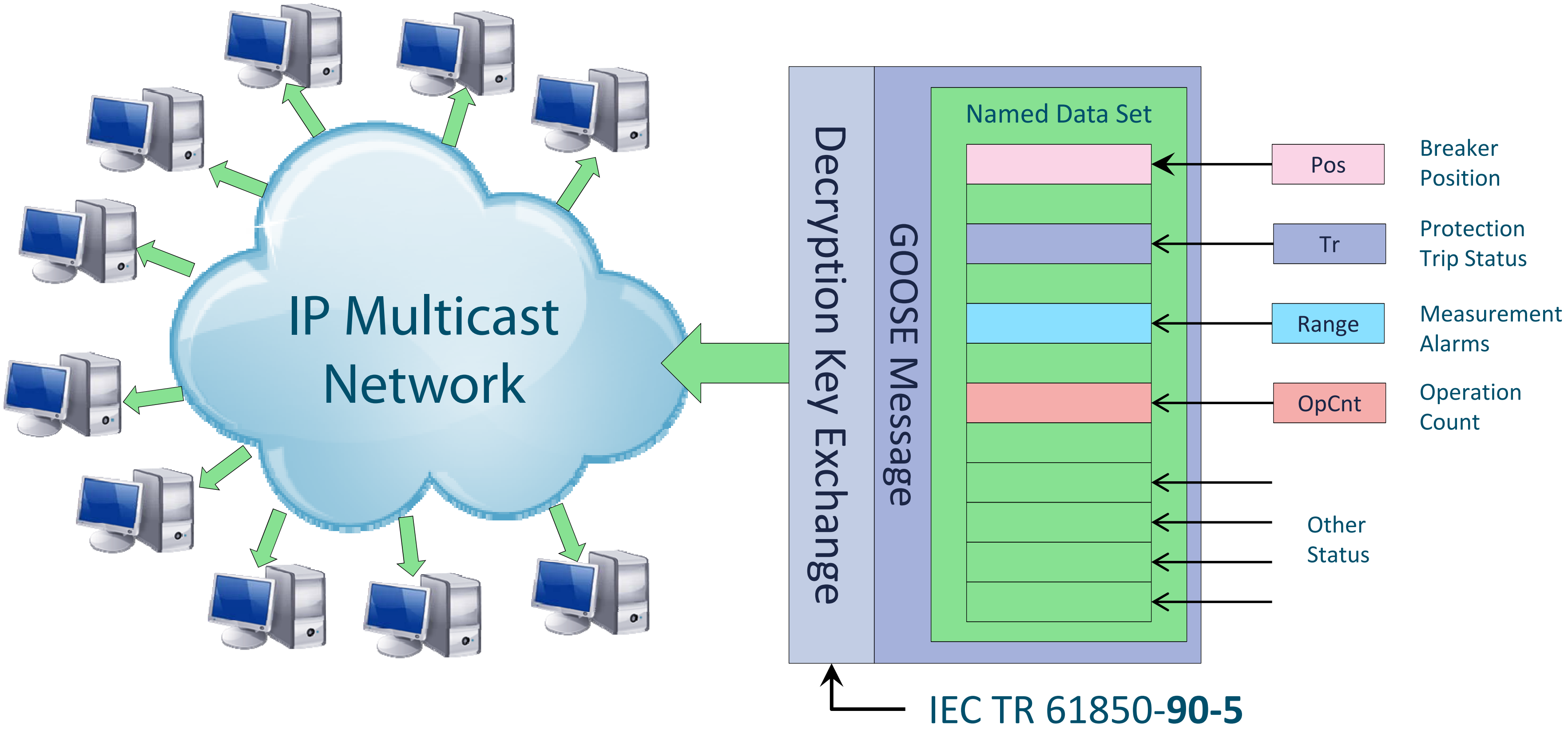
IEC 61850 **Wide Area** Profiles



Wide Area Applications

Protection and Control

GOOSE = Generic Object Oriented Substation Event – Event Messaging



- Any change in state of any element causes a repeating sequence of messages
- A message is sent periodically with no data change

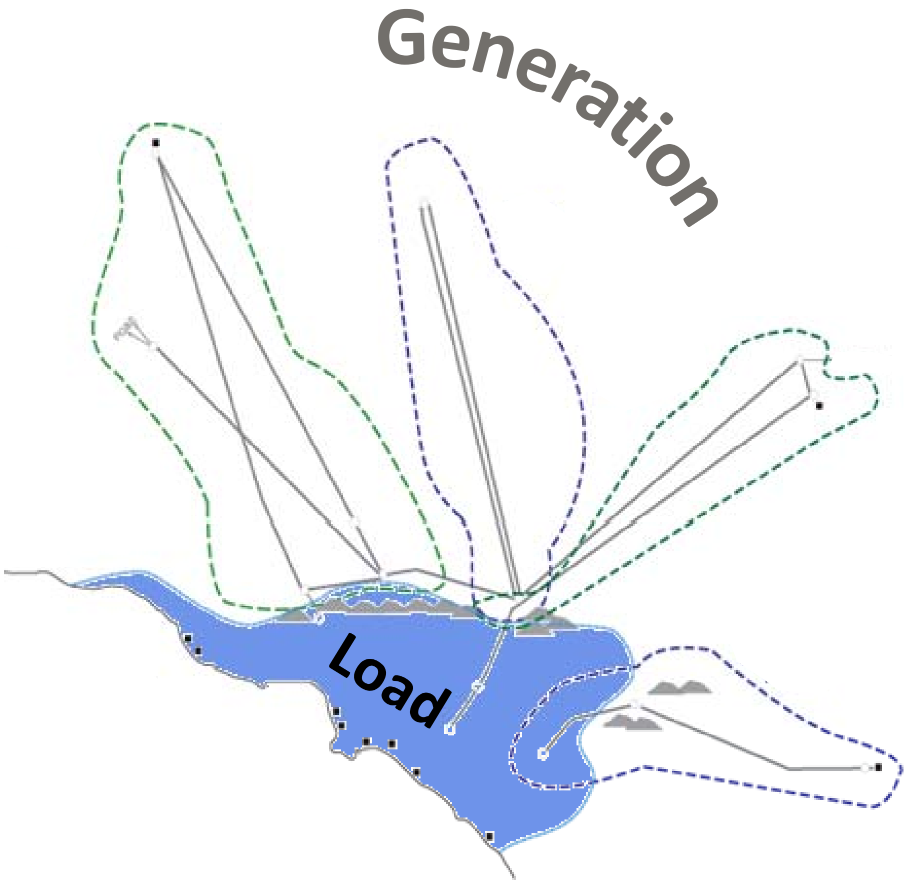
Wide Area Protection and Control

- Systems with long lines separating load and generation need protection to prevent damage from generation tripping.

- Increasing reserve margins to protect lines reduces available energy.

- Maintaining system stability during anomalous conditions challenges operators to respond quickly to prevent cascade failure

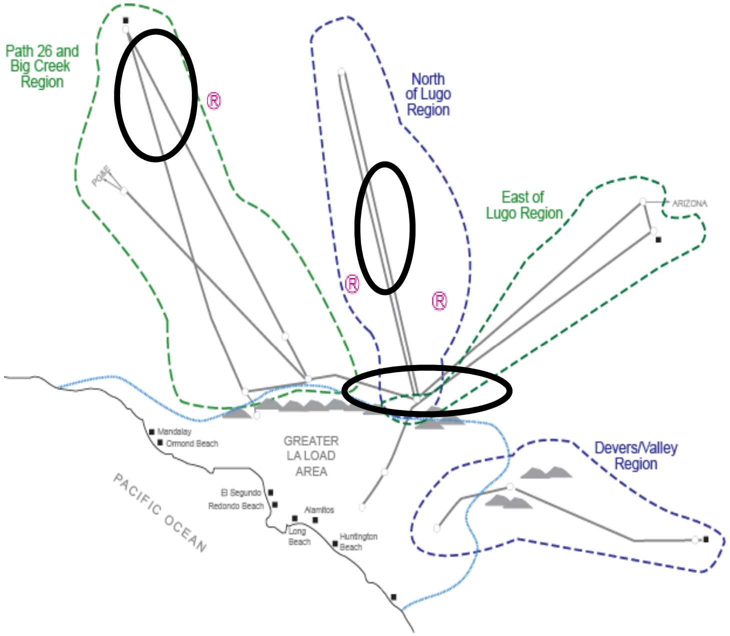
- More transmission capacity in the same corridor is subject to the same contingencies and only results in increasing reserve margins.



Individual Remedial Action Schemes and Special Protection Systems (RAS/SPS)

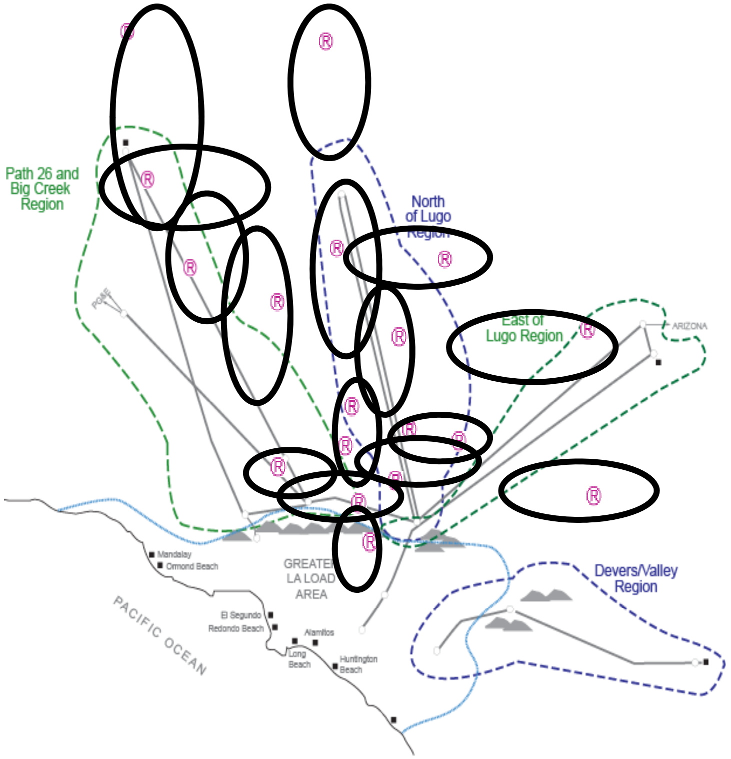
- Protects lines from damage during anomalous conditions.

- Individual RAS are available using traditional approaches involving hardwired devices within local areas.



Multiple Individual RAS

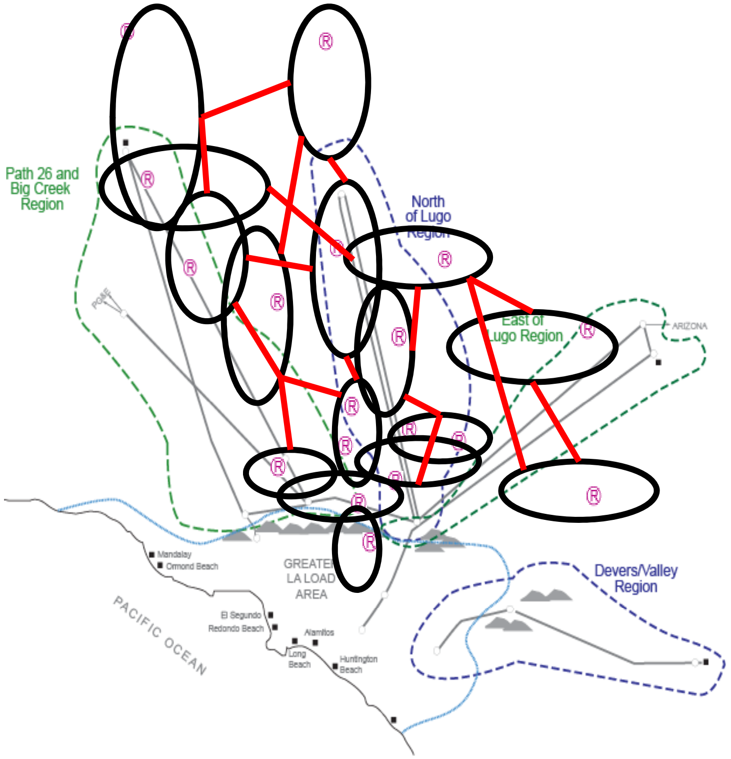
- Deploying multiple individual RAS does not significantly impact complexity and cost by itself because interactions are local to each individual RAS.



Integration of Multiple Individual RAS into a Distributed RAS

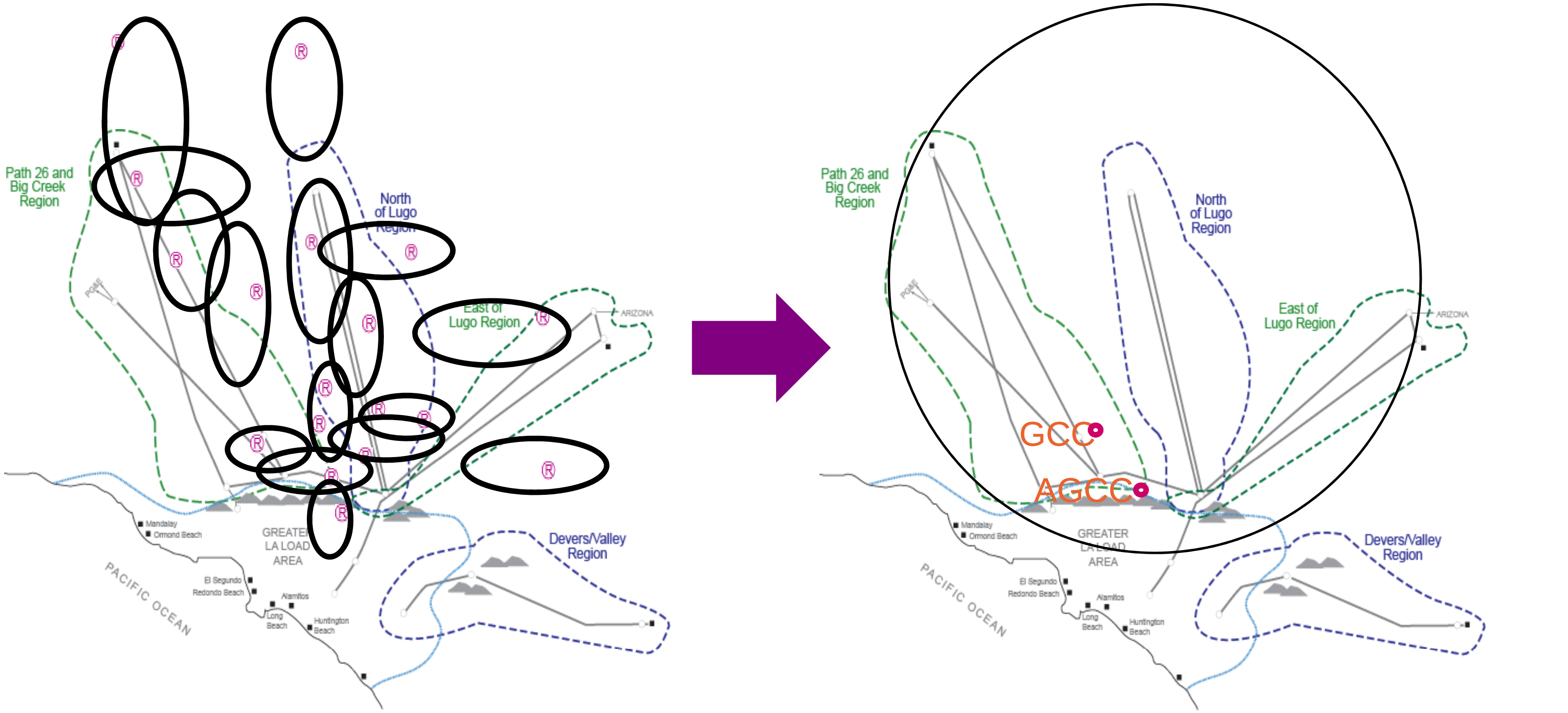
- Addressing system stability requires integration of WAS over a wide area.

- Information sharing and interactions between individual RAS using traditional techniques increases complexity and cost beyond what is practical.



Centralized Remedial Action Systems (C-RAS)

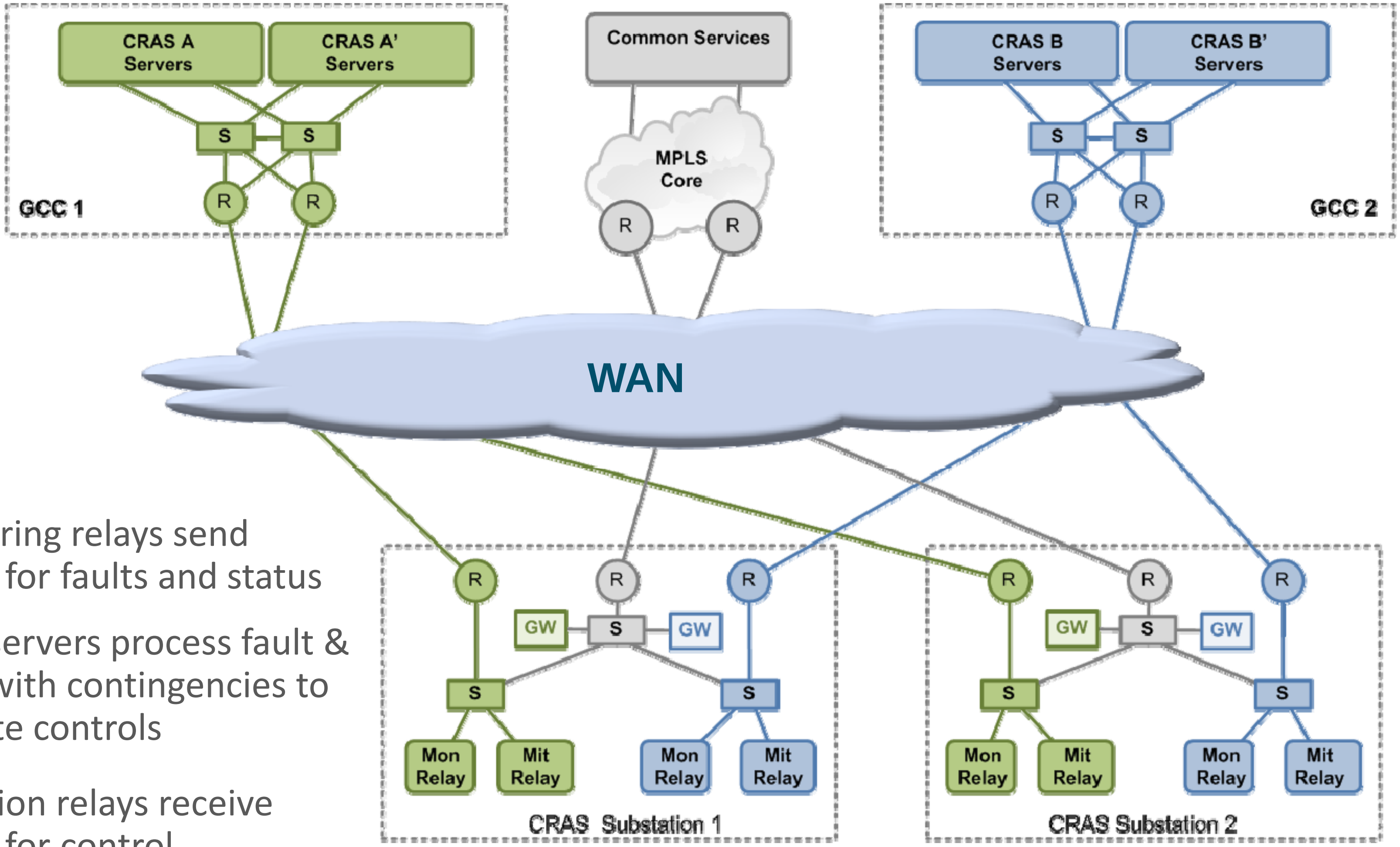
- Centralized control reduces complexity of information sharing making implementation feasible.
- Centralization of control requires a network architecture to support very reliable high speed communications of events and controls



Distributed

Centralized

C-RAS Needs Wide Area Networking



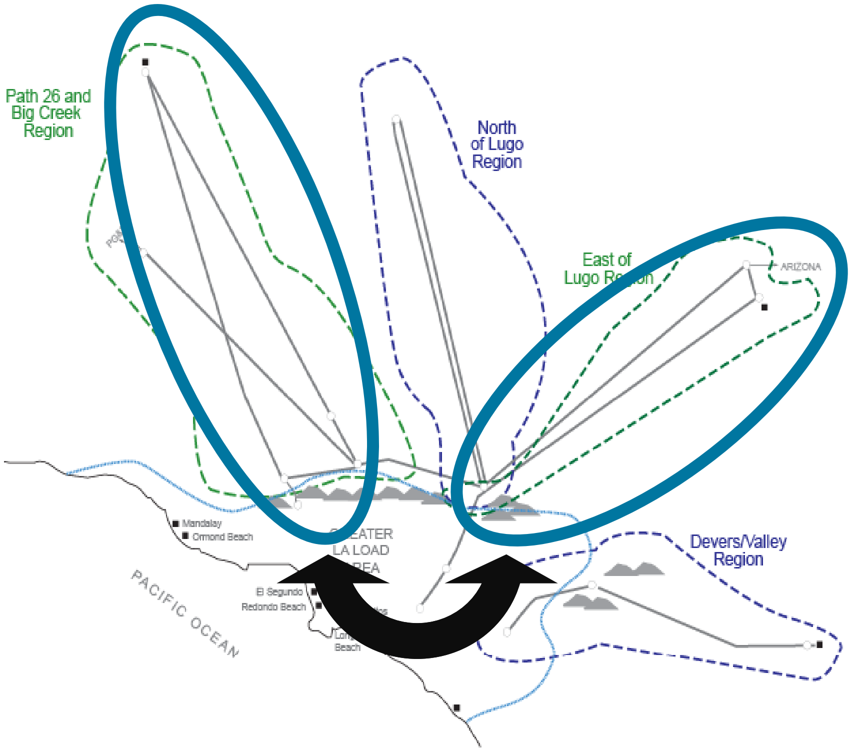
- Monitoring relays send GOOSE for faults and status
- C-RAS servers process fault & status with contingencies to generate controls
- Mitigation relays receive GOOSE for control

Why IEC 61850 for C-RAS?

- Relationship between status received and power system must be configurable and maintainable
  - IEC 61850 data is inherently in power system context
  - SCL enables sharing of device configuration and automated mapping
- Event data must be received simultaneously from all monitoring points
  - GOOSE multicast does not require interaction or session establishment with monitoring points by control center applications.
- Integrity of network must be established prior to control activity.
  - GOOSE periodic messaging constantly confirms network path.

Time Management is Critical

- 50 ms budget from fault detection to mitigation received at the control point must be monitored.
  - Precise time synchronization between control centers and substations required to measure performance.
- System stability RAS require comparison across lines over a wide area with 4ms processing time in RAS.
  - **Without time synchronized data control decisions would not be valid**.

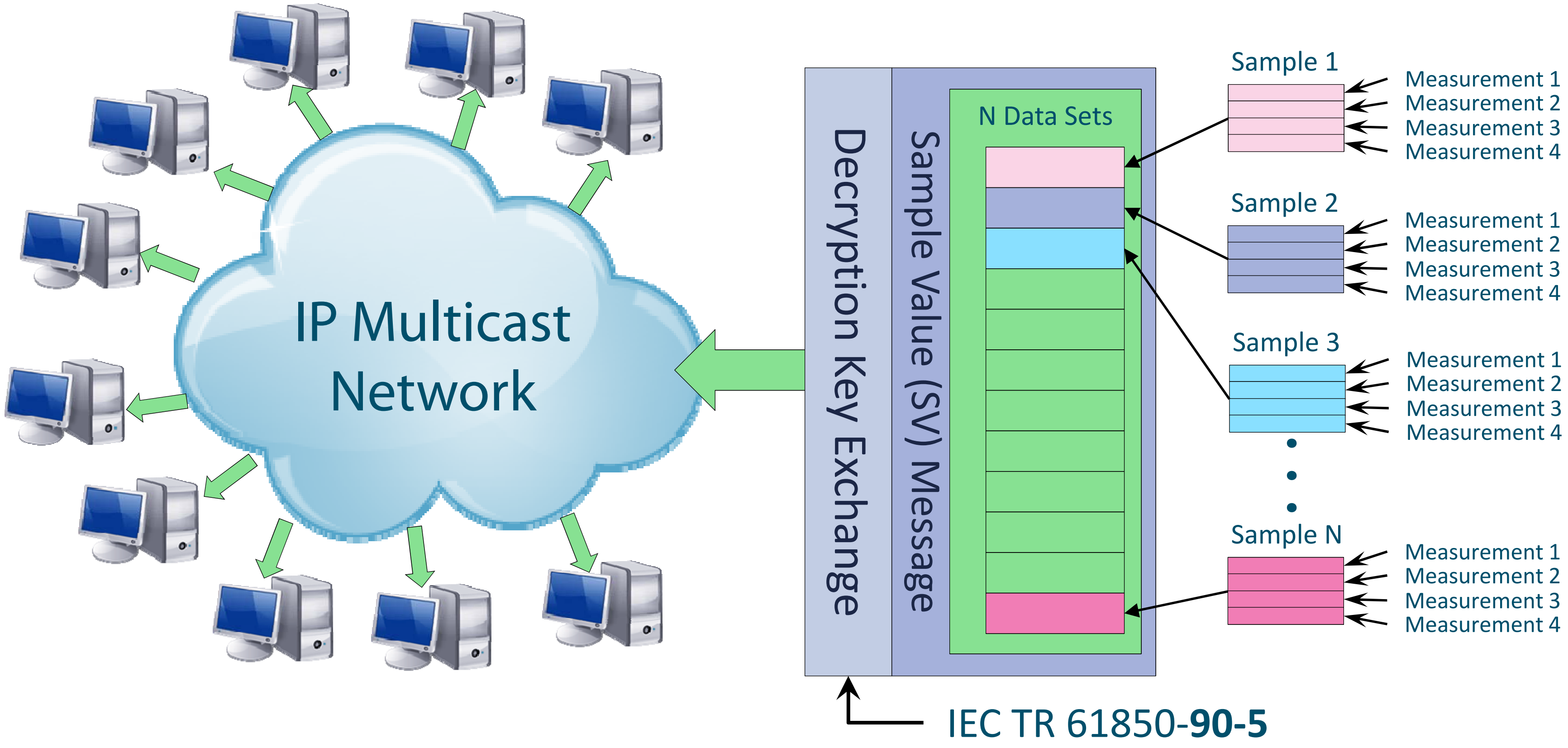


Wide Area Application of IEC 61850

Measurement Systems

SISCO
SYSTEMS
INTEGRATION
SPECIALISTS

IEC 61850 Sampled Values – Measurement Messaging



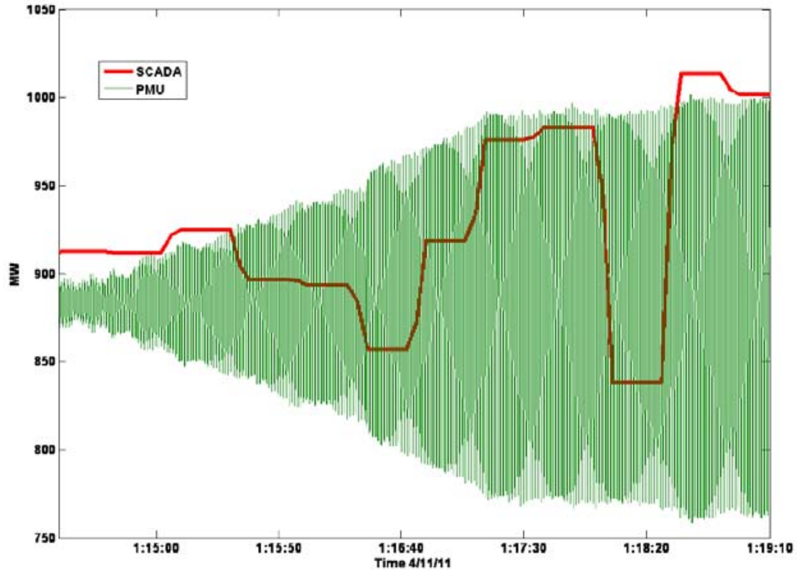
- Each data set contains one sample of a set of named measurements
- Messages containing multiple samples are sent periodically

Wide Area Measurement Systems (WAMS)

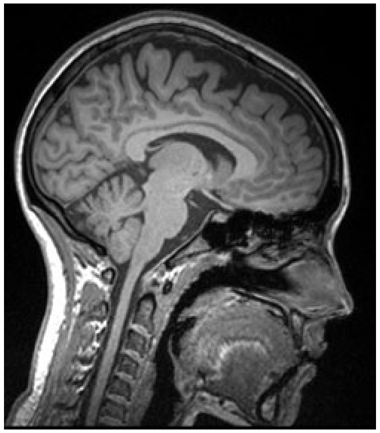
- Utilizes high-speed time-synchronized measurements of voltage, phase and frequency
  - From 30 to 120 samples per second of each measurement

- Enables comparison of system in “real” real-time over a wide area (e.g. State Measurement vs. State Estimation)

Why is WAMS Needed?



High-speed precision measurements provide information that EMS data cannot provide.

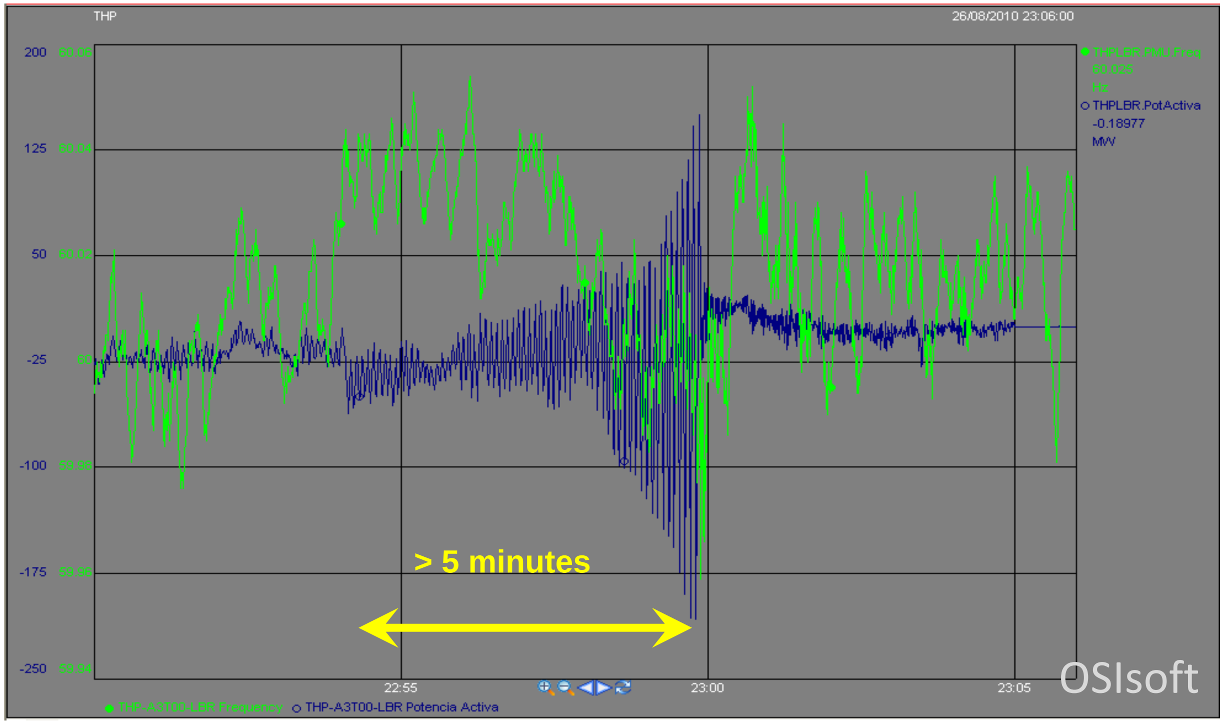


SCADA → Synchrophasor

↕

X-Ray → MRI

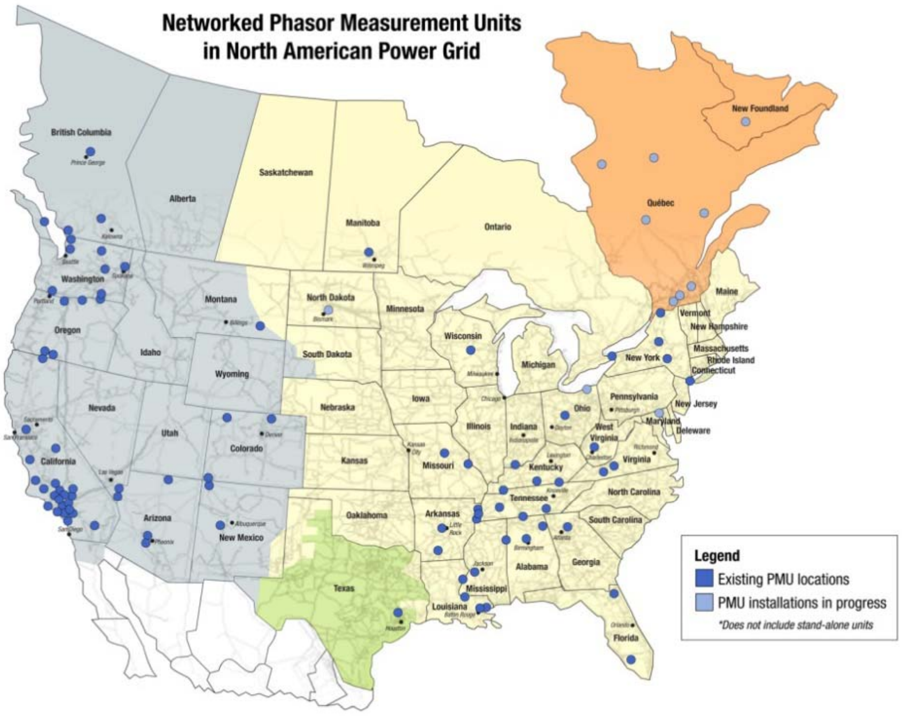
Example Tie Line Event in Mexico



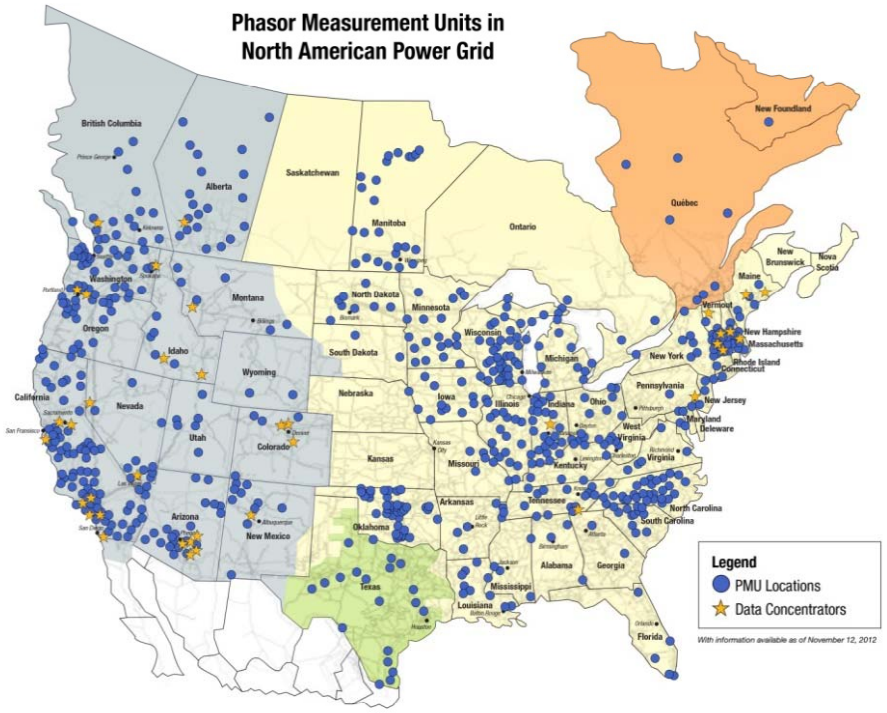
If the data can be transformed into information that enables operators to make faster more accurate decisions the benefits to reliability are tremendous.

Use of Wide Area Time Synchronized Measurements is Increasing…Why?

2007

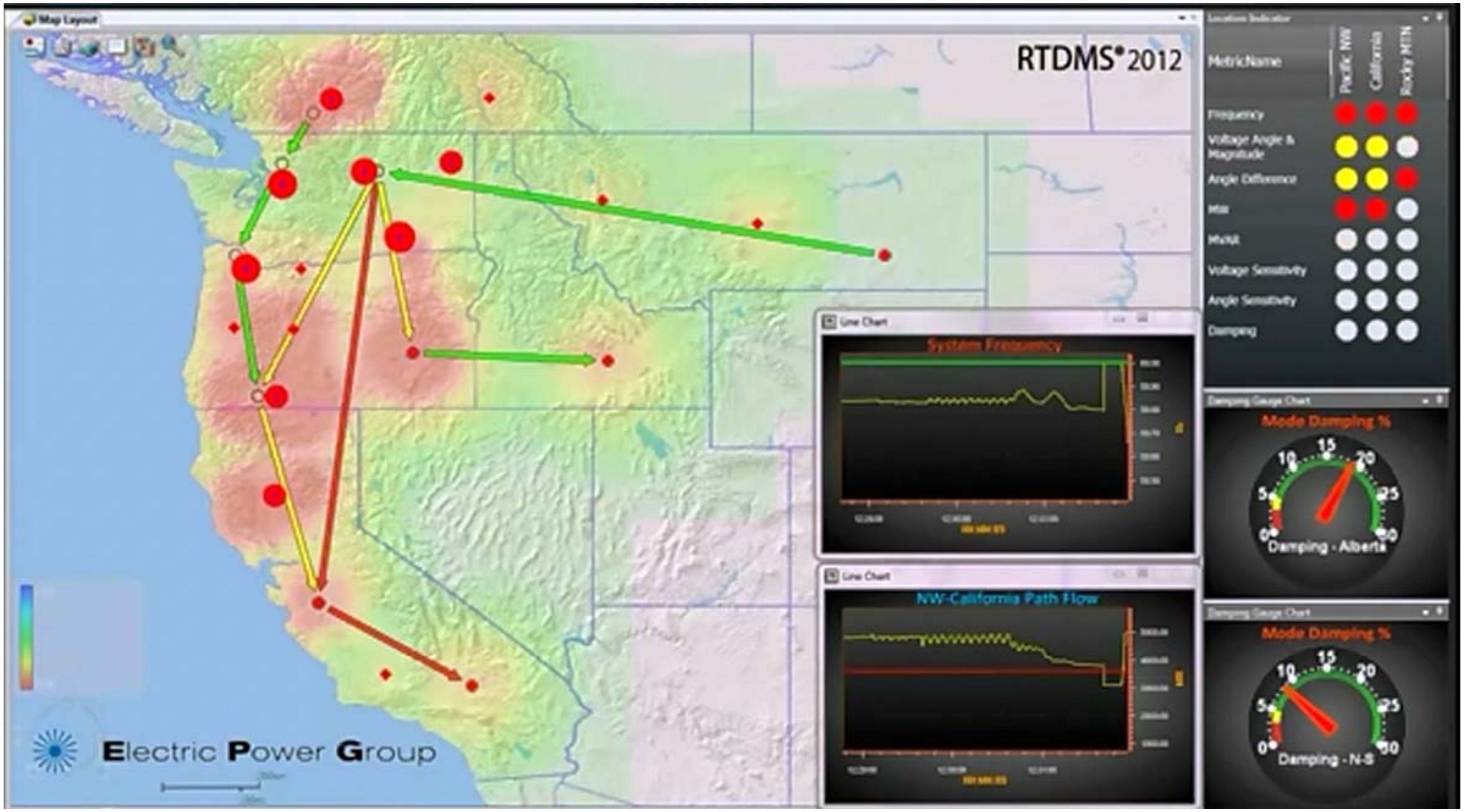

Networked Phasor Measurement Units in North American Power Grid

2012


Phasor Measurement Units in North American Power Grid

With information available as of November 12, 2012

Increased Situational Awareness



Map Layout

RTDMS® 2012

Electric Power Group

Line Chart

System Frequency

Line Chart

NW-California Path Flow

Location Indicator

MetricName	Pacific NW	California	Rocky MTN
Frequency	🔴	🔴	🔴
Voltage Angle & Magnitude	🟡	🟡	⚪
Angle Difference	🟡	🟡	🔴
MW	🔴	🔴	⚪
MVAR	⚪	⚪	⚪
Voltage Sensitivity	⚪	⚪	⚪
Angle Sensitivity	⚪	⚪	⚪
Damping	⚪	⚪	⚪

Damping Gauge Chart

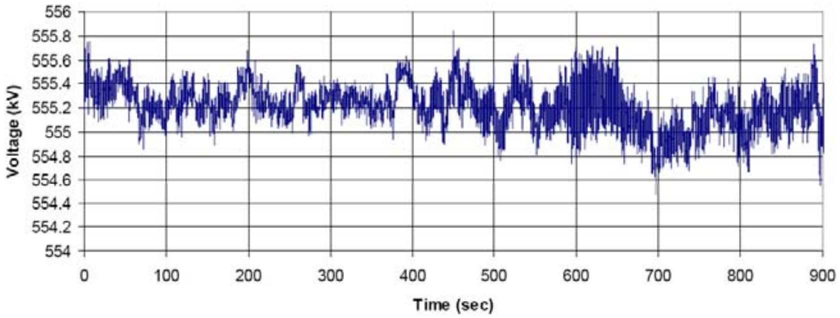
Mode Damping %

Damping Gauge Chart

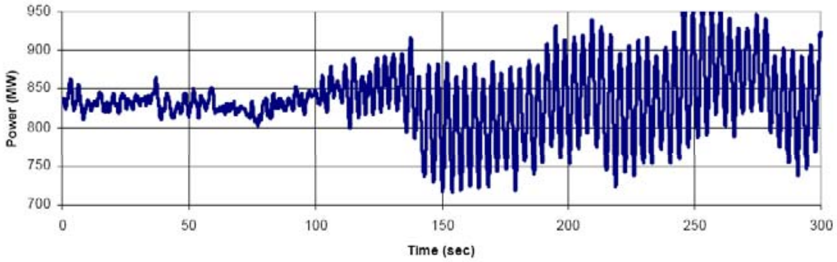
Mode Damping %

Oscillation Detection + Damping Factor Calculation

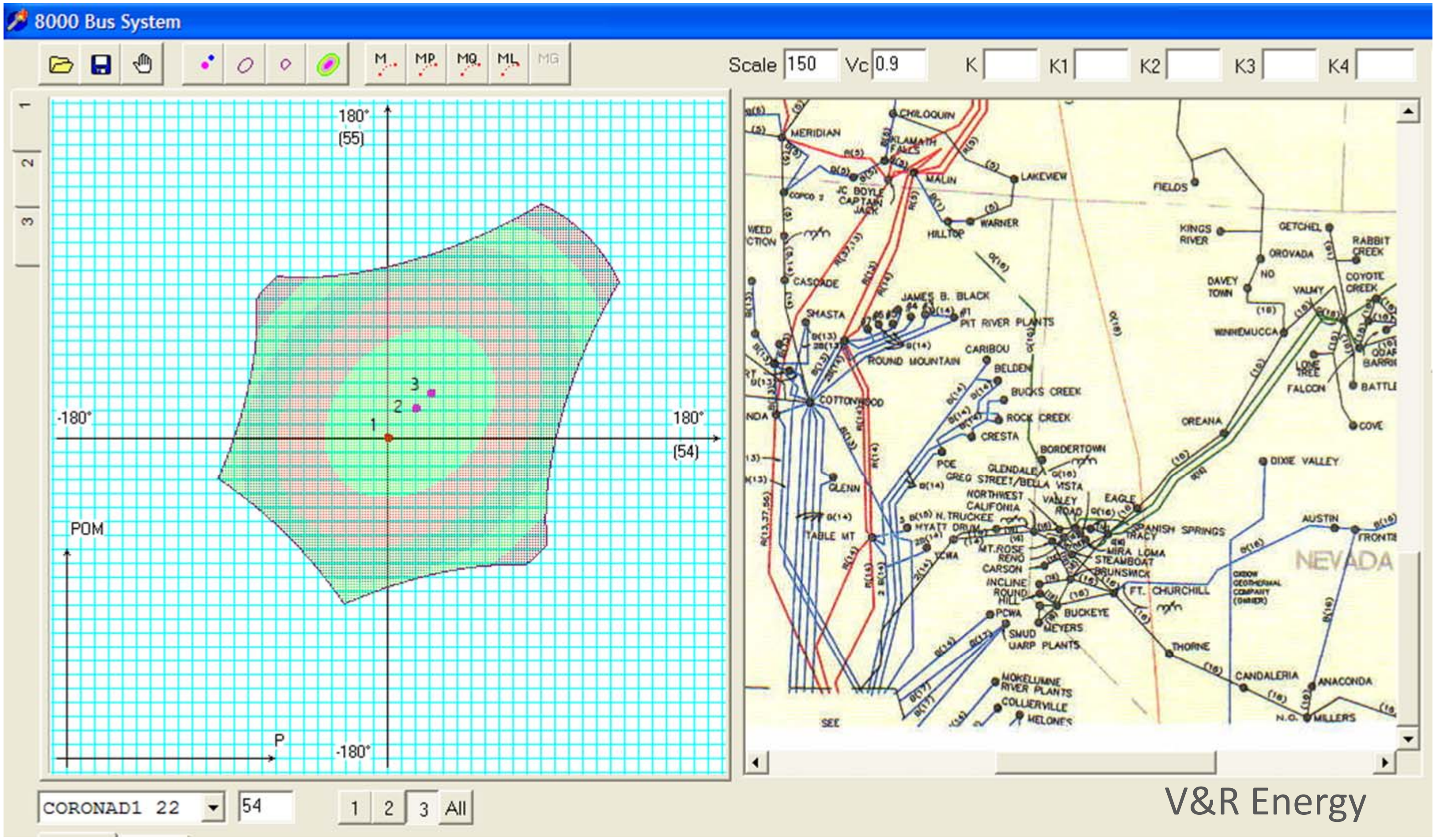
- No disturbance, but very low damping factor indicates potential instability



- Highly damped forced oscillations do not overly stress system but indicate problems that need to be addressed.



Voltage Stability Prediction



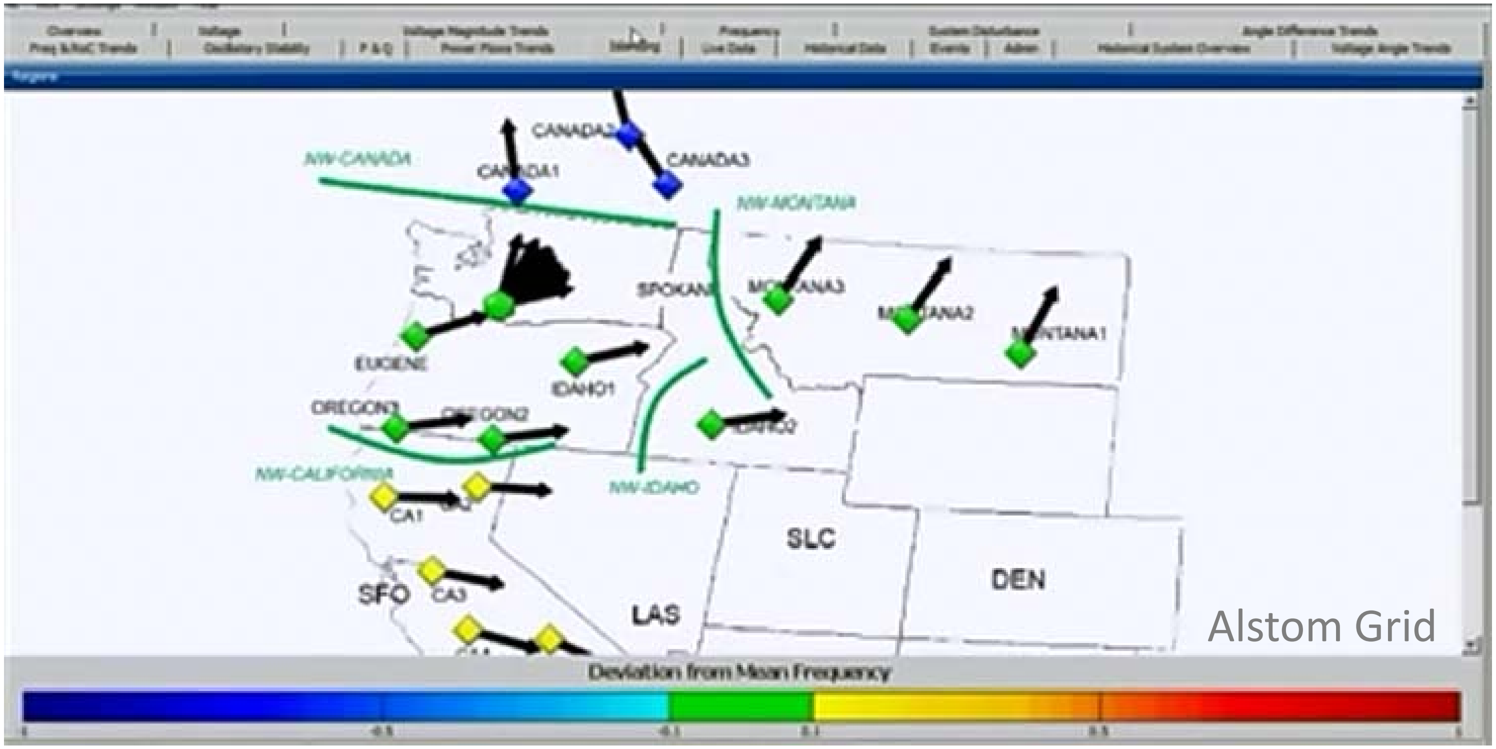
8000 Bus System

Scale 150 Vc 0.9 K K1 K2 K3 K4

CORONAD1 22 54

V&R Energy

Islanding Detection



Alstom Grid

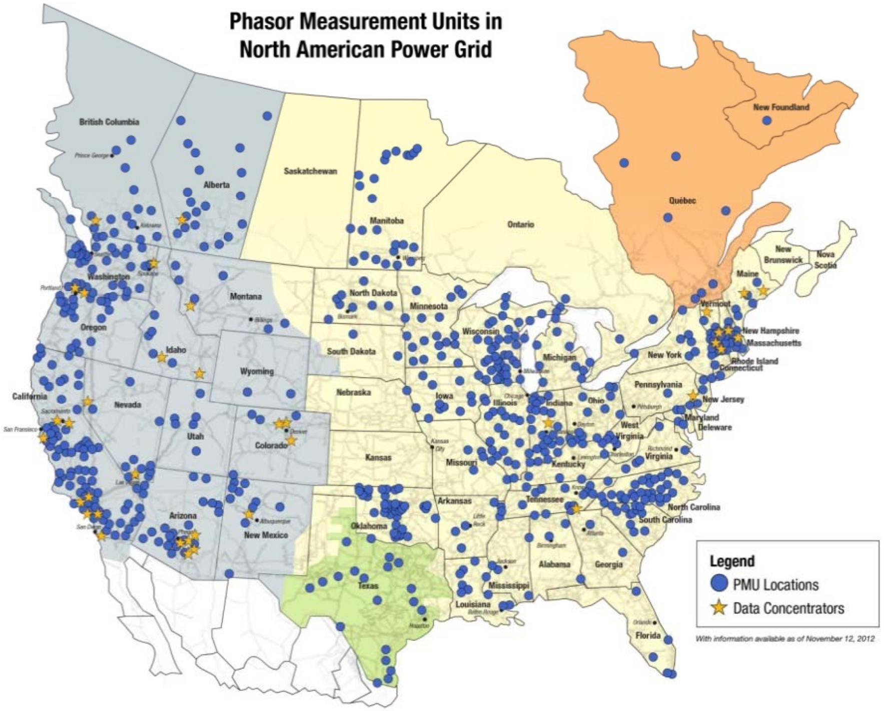
Why IEC 61850 for WAMS?

- Existing systems use C37.118 for synchrophasor communications.
  - 16 character signal names
  - No security options
  - Protocol limitations require use of phasor data concentrators (PDC) adding latency

- IEC TR 61850-90-5 (WAMPAC Profile)
  - Power System Context Naming of all Signals
  - Secured with authenticated key exchange (and endorsed by NERC)
  - Use of IP Multicast enables flatter architectures with fewer PDCs.

Why IEC 61850 Naming is Important

- Each dot represents a PMU with 12 or more measurements
- PMU data from neighboring utilities is needed
- IEC 61850 models can integrate with EMS models using CIM
- Enables signal registries using existing power system models to find and subscribe to signals



Phasor Measurement Units in North American Power Grid

Legend
● PMU Locations
☆ Data Concentrators

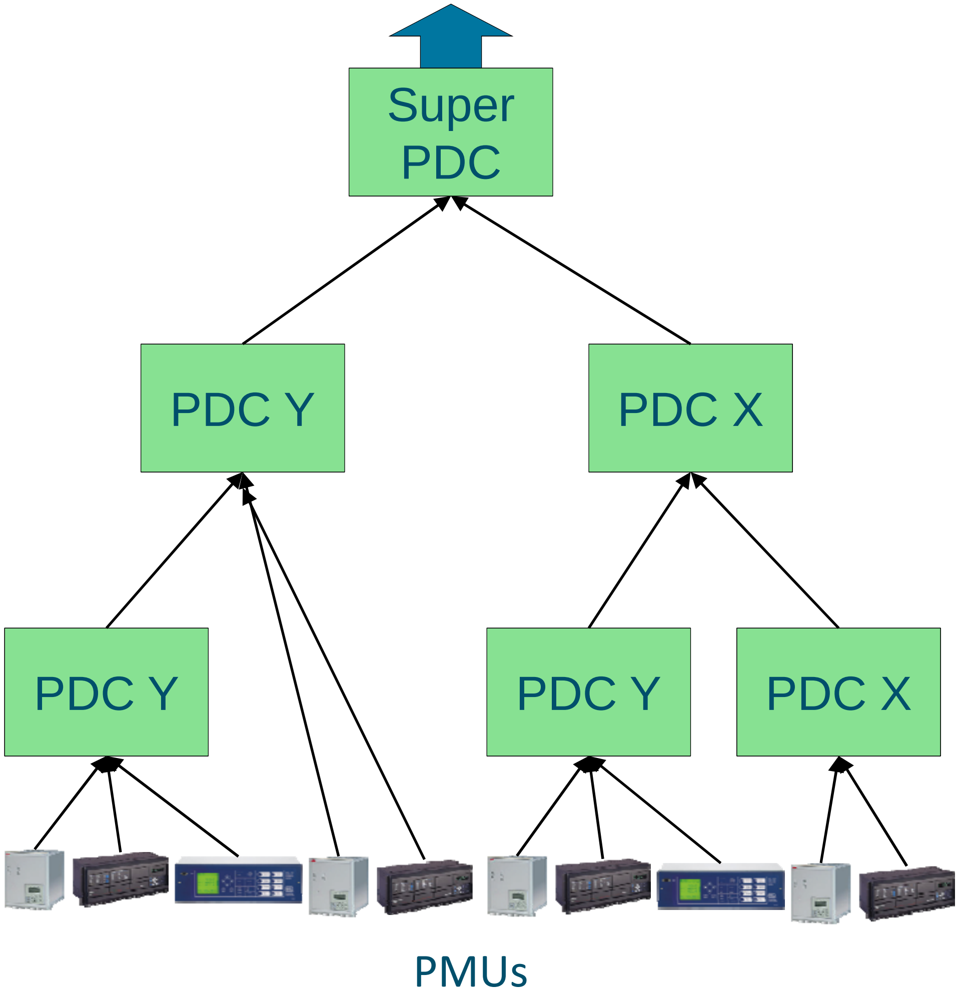
With information available as of November 12, 2012

16 Character Signal Names are not enough!

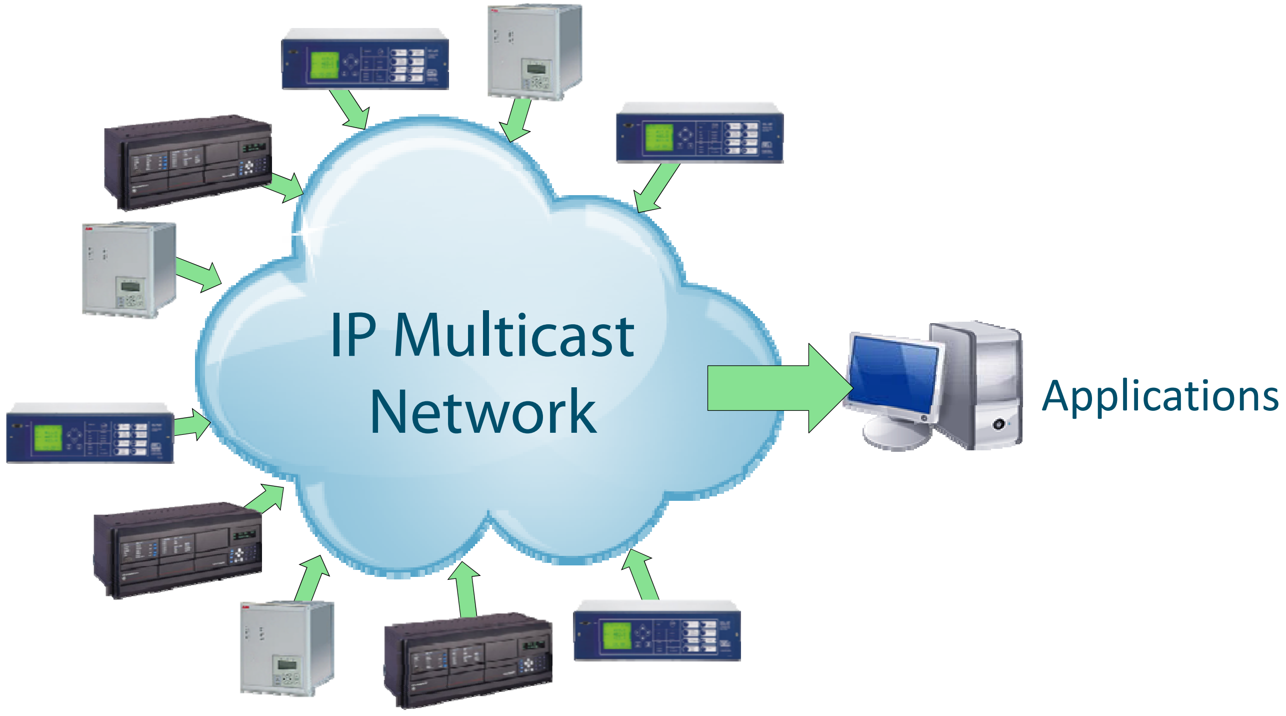
© Copyright 2013

PDC Latency Issues

- In practice: multiple levels of PDCs from multiple different vendors
- Result is large discrepancy in latencies between measurements taken at the same time.
- PDCs won't forward late arriving data
- Difficult to align data for comparison and calculations with large latency and missing packets



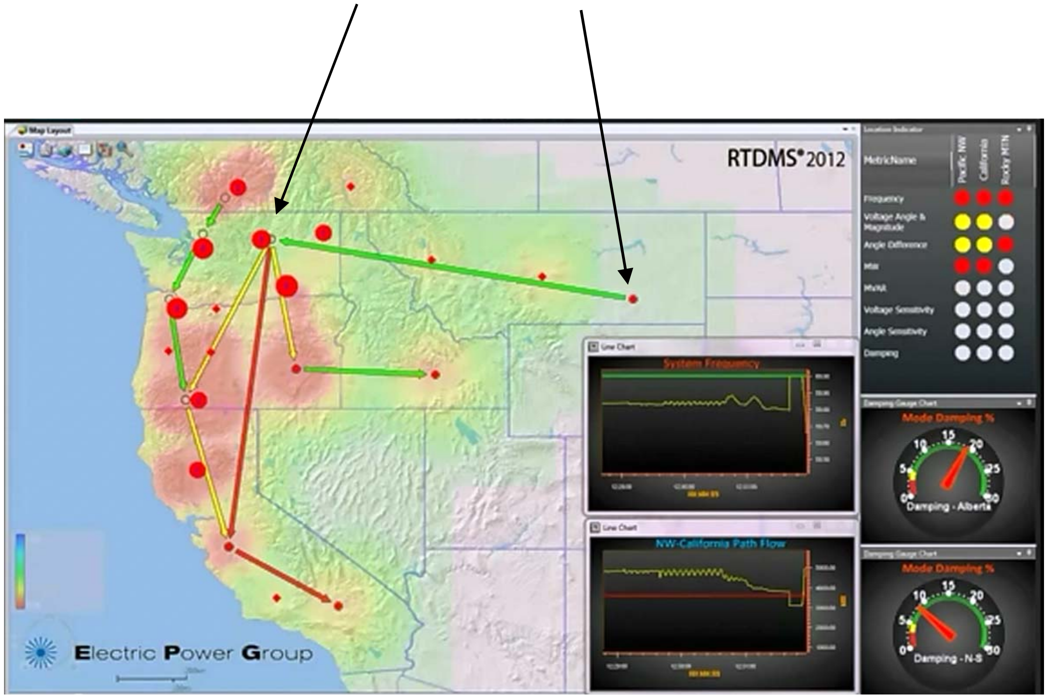
IEC TR 61850-90-5 Supports a Flatter Network Architecture



- Fewer PDCs reduces latency differences from arriving signals and eliminates dropped packets.

Importance of Time Synchronization

- If Signal A and Signal B are not time synchronized the result of any calculation or application using those signals becomes noise.


Signal A

Signal B

Synchrophasor data is pretty much useless without time synchronization

Summary So Far

- IEC 61850 has unique features that enable wide area applications for measurement protection and control
  - Configuration, naming and modeling that manages the complexity of large scale systems.
  - Protocols and profiles that support WAMPAC requirements.

- Time synchronization is a fundamental requirement for wide area applications.
  - Control decisions are not valid without accurate and consistent event time stamps
  - Measurement data is not useful without time synchronization over the wide area of interest

Symmetricom®

Leading the world in precise time solutions.

Timing Strategy for WAMPAC

Debra Henderson, Director – Power Utility Markets

June 5, 2013

Do you have a timing strategy?

If not, you may have issues and not know it.

GPS antenna farms are created from multiple point solution implementations. Some of the issues that can impact your timing reference:

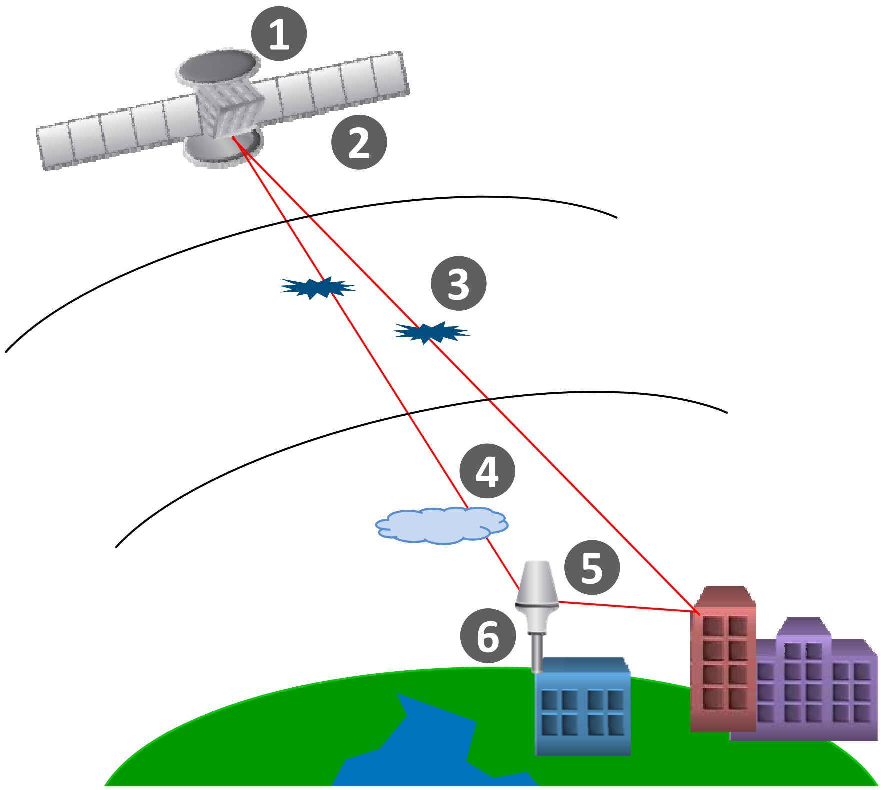
- Improper antenna installations
- Damaged antennas causing interference

- Environmental conditions

- Intentional and unintentional sabotage such as jamming and spoofing

Normal GPS Operations Can Induce Errors

Symmetricom



1. Orbit error
2. Satellite clock error
3. Ionospheric delay
4. Tropospheric delay
5. Multipath
6. Receiver noise

High quality receivers can adjust for most of these errors. Multipath impacts time more than the other sources

Threats to Substation Security

Symmetricom

Jammers and Spoofing — Real

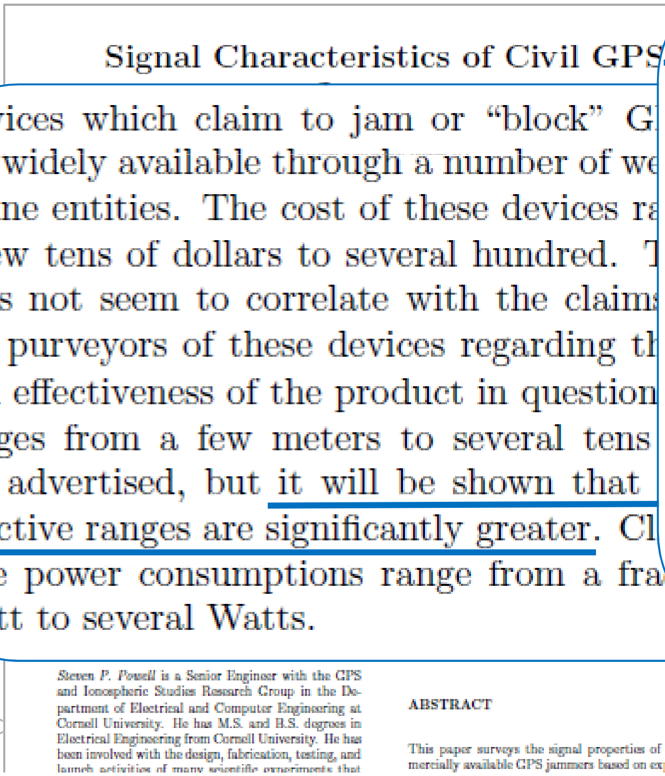
Jammers

$55 Ebay

$83 GPS&GSM

Spoofing

Cheap jammers to sophisticated spoofin



Signal Characteristics of Civil GPS

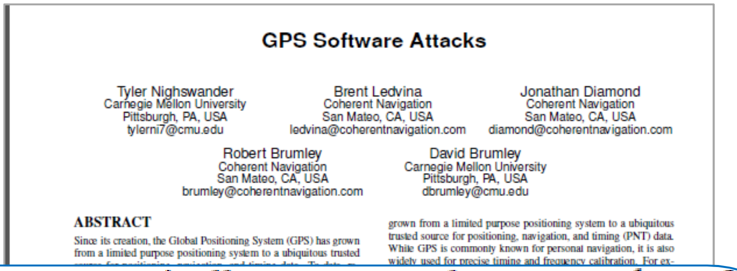
Devices which claim to jam or "block" G
are widely available through a number of we
online entities. The cost of these devices ra
a few tens of dollars to several hundred. T
does not seem to correlate with the claims
the purveyors of these devices regarding th
and effectiveness of the product in question
ranges from a few meters to several tens
are advertised, but it will be shown that
effective ranges are significantly greater. Cl
true power consumptions range from a fra
Watt to several Watts.

Steven P. Powell is a Senior Engineer with the GPS and Ionospheric Studies Research Group in the Department of Electrical and Computer Engineering at Cornell University. He has M.S. and B.S. degrees in Electrical Engineering from Cornell University. He has been involved with the design, fabrication, testing, and launch activities of many scientific experiments that

ABSTRACT

This paper surveys the signal properties of 18 commercially available GPS jammers based on experimen-

Software attacks — Possible



GPS Software Attacks

Tyler Nighswander
Carnegie Mellon University
Pittsburgh, PA, USA
tylerni7@cmu.edu

Brent Ledvina
Coherent Navigation
San Mateo, CA, USA
ledvina@coherentnavigation.com

Jonathan Diamond
Coherent Navigation
San Mateo, CA, USA
diamond@coherentnavigation.com

Robert Brumley
Coherent Navigation
San Mateo, CA, USA
brumley@coherentnavigation.com

David Brumley
Carnegie Mellon University
Pittsburgh, PA, USA
dbrumley@cmu.edu

ABSTRACT

Since its creation, the Global Positioning System (GPS) has grown from a limited purpose positioning system to a ubiquitous trusted

grown from a limited purpose positioning system to a ubiquitous trusted source for positioning, navigation, and timing (PNT) data. While GPS is commonly known for personal navigation, it is also widely used for precise timing and frequency calibration. For ex-

In this work, we systematically map out a larger attack surface by viewing GPS as a computer system. Our surface includes higher level GPS protocol messages than previous work, as well as the GPS OS and downstream dependent systems. We develop a new hardware platform for GPS attacks, and develop novel attacks against GPS infrastructure. Our experiments on consumer and professional-grade receivers show that GPS and GPS-dependent systems are significantly more vulnerable than previously thought. For example, we show that remote attacks via malicious GPS broadcasts are capable of bringing down up to 30% and 20% of the global CORS navigation and NTRIP networks, respectively, using hardware that costs about the same as a laptop. In order to improve security, we propose systems-level defenses and principles that can be deployed to secure critical GPS and dependent systems.

Elements of a timing strategy

*The benefit of having a timing strategy is to ensure that you have a single **secure, accurate and reliable time reference** within and across your substations.*

Your timing architecture should consider the following elements:

1. Redundant hardware and primary reference
2. Backup time references
3. Holdover
4. Management

GPS or WAN
Primary Reference

#1

Substation Master Clocks

#2

IEEE 1588 PTP
WAN synchronization

IEEE 1588 Telecom
Profile Grandmaster

#3

Rubidium
Holdover

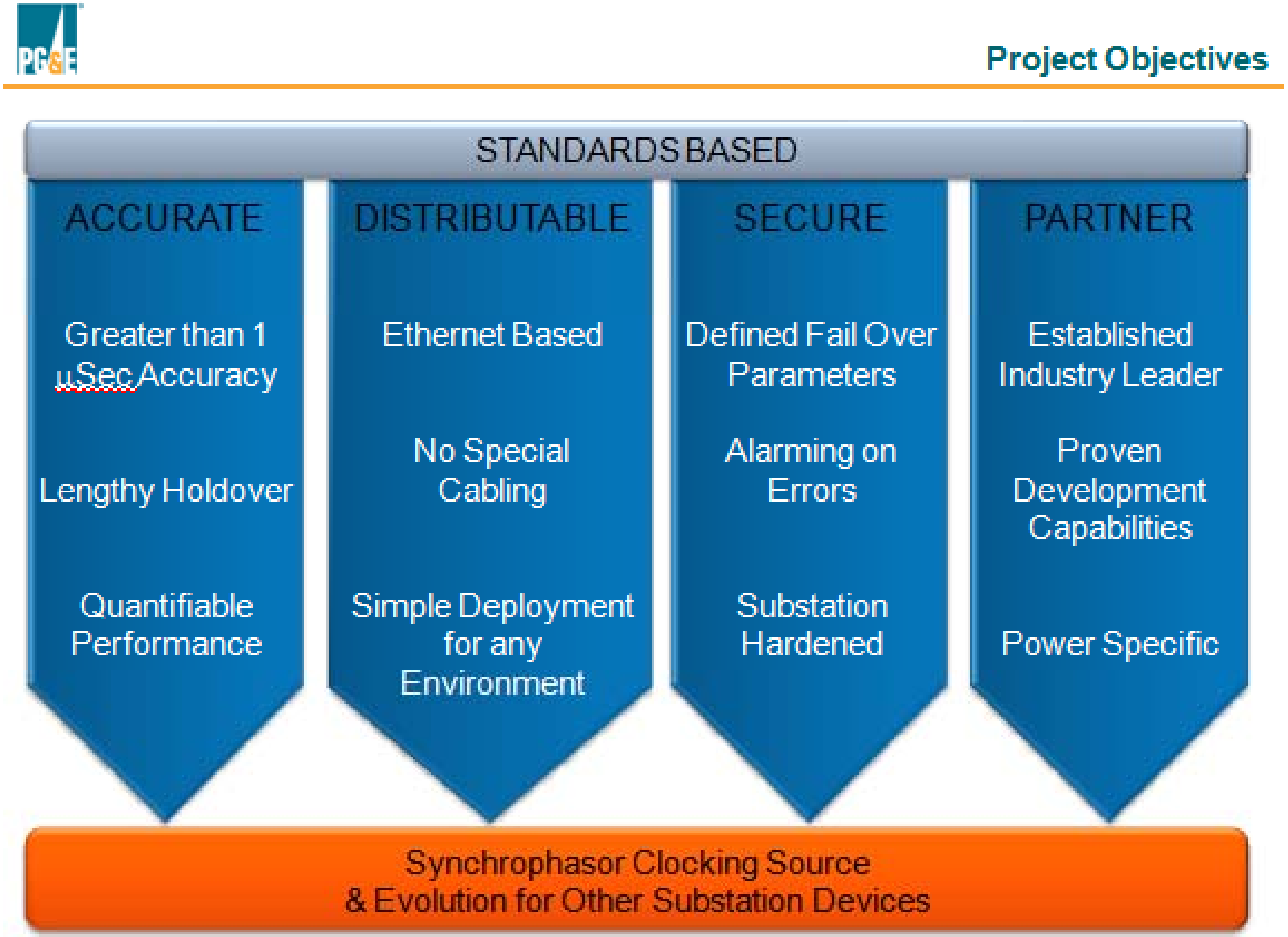
#4

Remote Management

Alarm Status
SNMP Monitoring

PG&E Timing Objectives for the Synchrophasor Project

Symmetricom



PG&E

Project Objectives

STANDARDS BASED

ACCURATE

Greater than 1 uSec Accuracy

Lengthy Holdover

Quantifiable Performance

DISTRIBUTABLE

Ethernet Based

No Special Cabling

Simple Deployment for any Environment

SECURE

Defined Fail Over Parameters

Alarming on Errors

Substation Hardened

PARTNER

Established Industry Leader

Proven Development Capabilities

Power Specific

Synchrophasor Clocking Source
& Evolution for Other Substation Devices

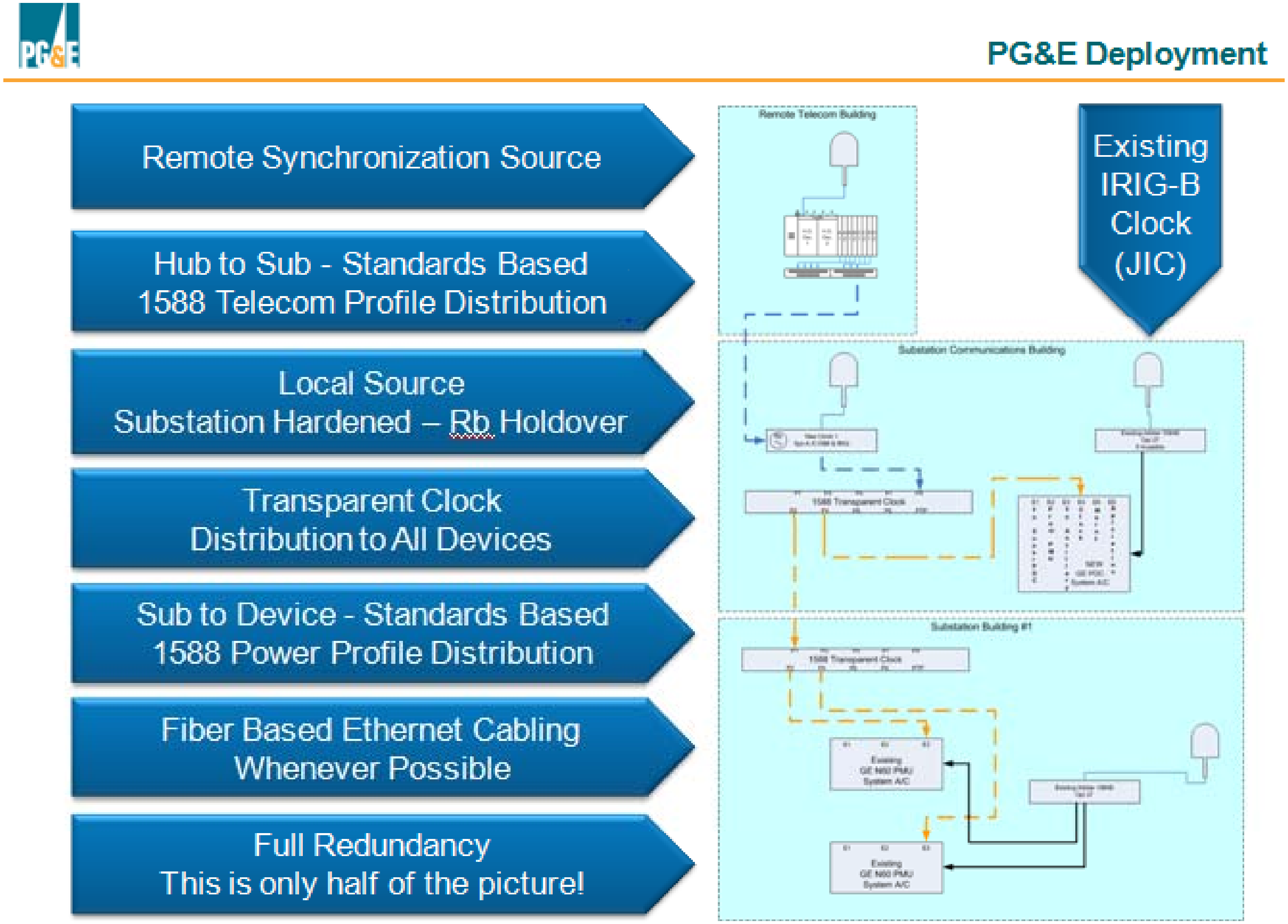
Source : i-PCGRID
March 2013

Time Transfer Technologies

Symmetricom

	IRIG-B	(S)NTP	PTP
Accuracy (typical)	1-10μs	1ms – 10 ms	100ns-1μs
Transport media	Dedicated cables	Ethernet cables	Ethernet cables
Protocol style	Master-slave	Client-server	Master-slave
Built in latency correction	No	Yes	Yes
Set-up	Configured	Configured	Self-organizing, or configured
Update intervals	1 second	Minutes	1 second
Specialized hardware	Required	No	Required
Redundant masters for N-1 contingency	No	Yes	Yes

PG&E Deployment

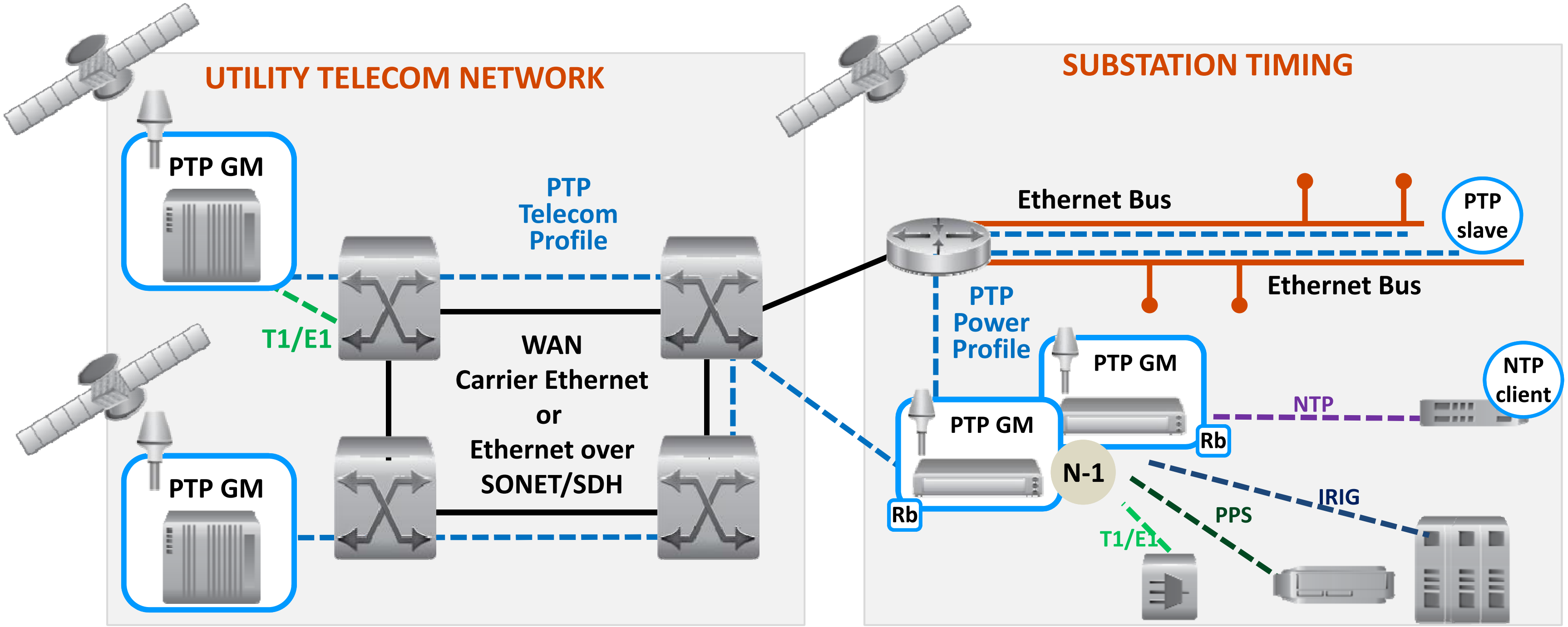

PG&E Deployment

- Remote Synchronization Source
- Hub to Sub - Standards Based 1588 Telecom Profile Distribution
- Local Source Substation Hardened – Rb Holdover
- Transparent Clock Distribution to All Devices
- Sub to Device - Standards Based 1588 Power Profile Distribution
- Fiber Based Ethernet Cabling Whenever Possible
- Full Redundancy This is only half of the picture!

Existing IRIG-B Clock (JIC)

Source : i-PCGRID
March 2013

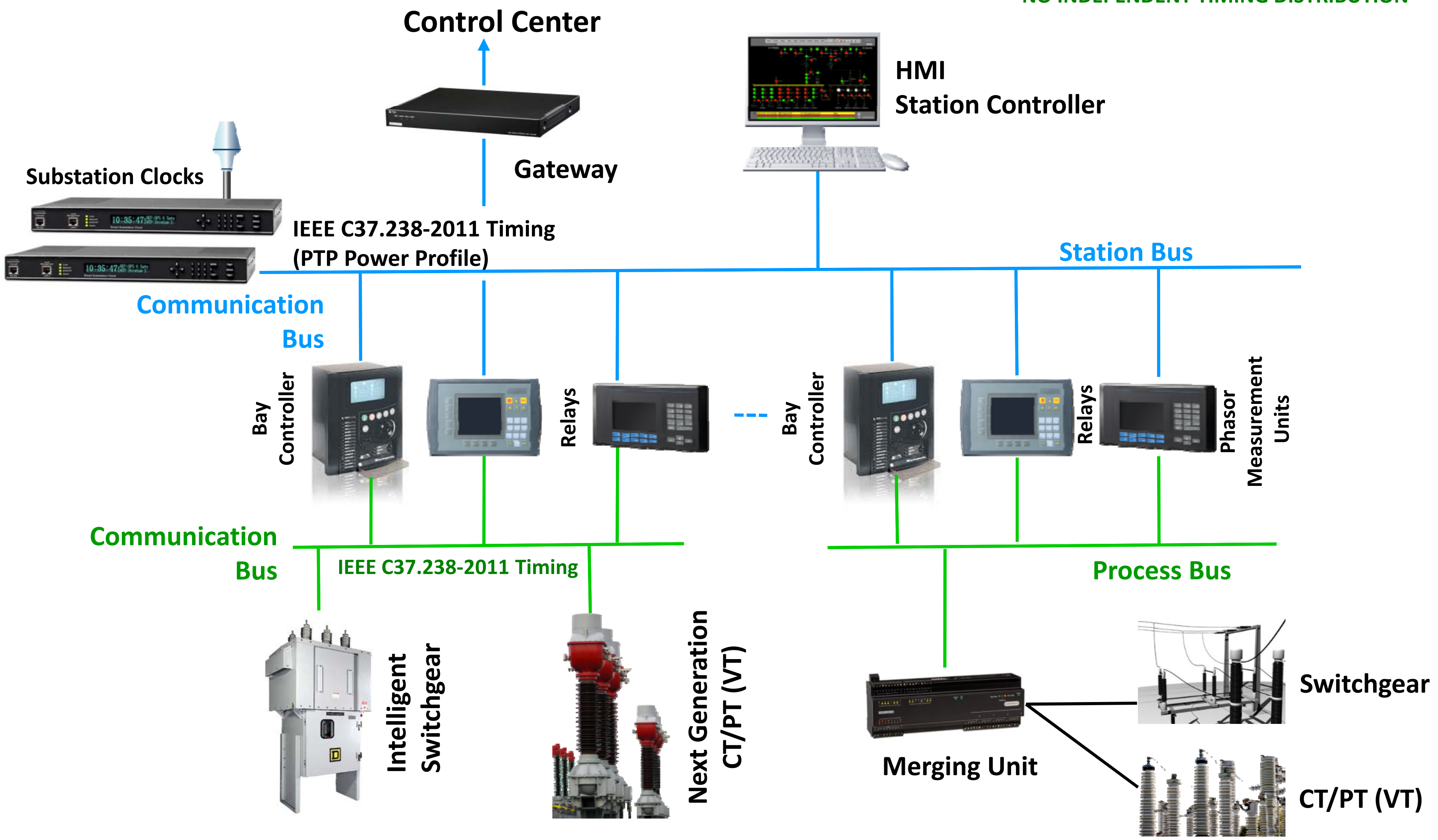
Network Distributed Timing for Substations



- Grandmaster in the substation, PTP microsecond accuracy for PMU and Sampled Values, IRIG-B, PPS and NTP for legacy IED
- Redundant deployment for N-1 protection
- Eliminate “GPS antenna farms”
- Rubidium for extended holdover
- Backup or primary reference with PTP over the telecom network

IEC 61850 Smart Substation: Industrial Ethernet Infrastructure With PTP

NO INDEPENDENT TIMING DISTRIBUTION



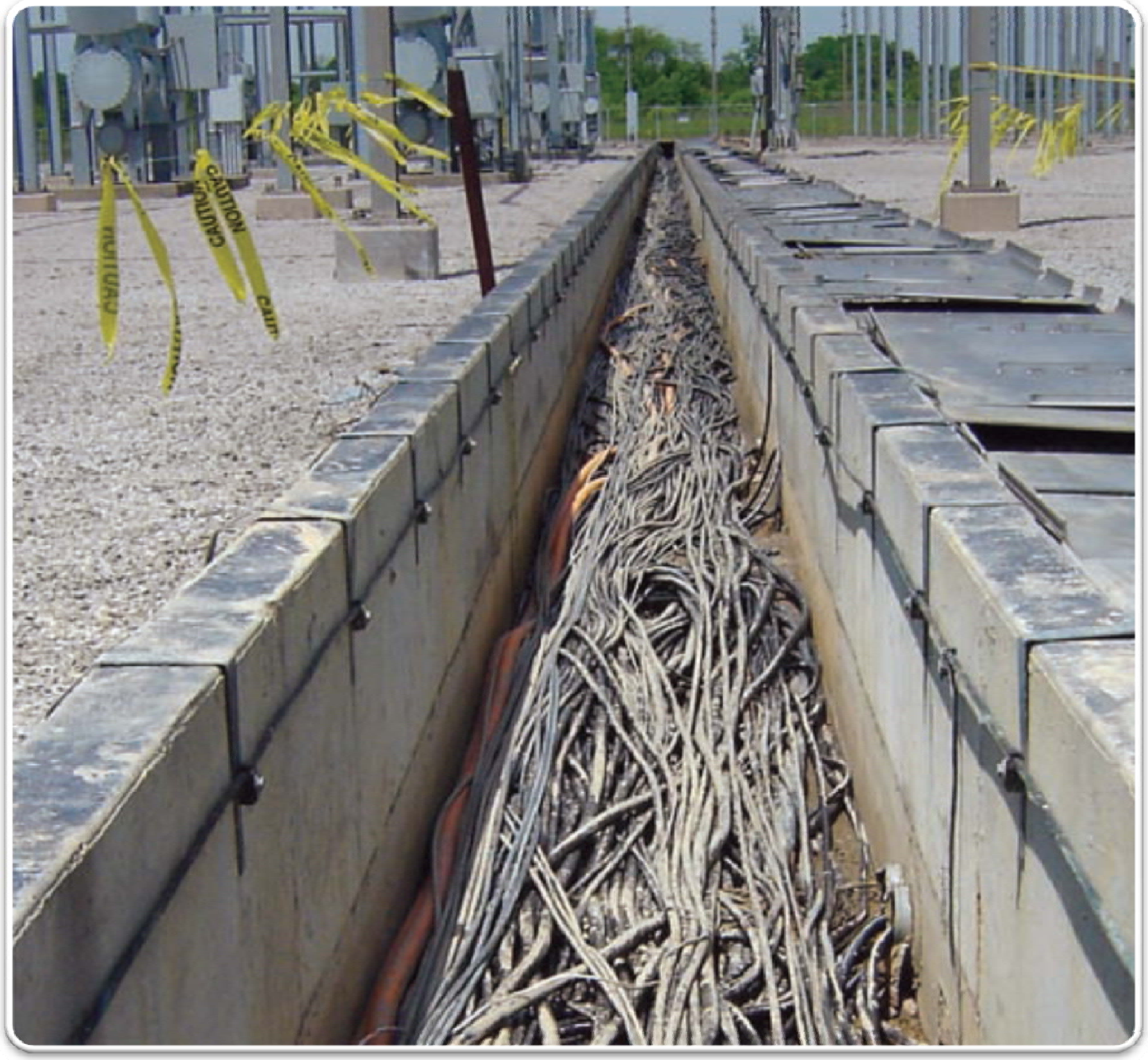
IEC 61850 Smart Substations: Process Bus To The Switchyard

Current practice

- Parallel copper cabling between switch yard & control building:
- Analog samples to protection equipment
- Coaxial cables for IRIG timing

Future systems

- Fiber optic network IEC 61850 Process Bus
- Digitized sampled values to protection equipment
- Timing on data network
- Increases reliability & control
- Provides isolation
- Lowers cost



Source
GE Protection & Control Journal
October 2008

Summary

- Using PTP for time distribution in substations is most accurate with lowest TCO.
- GPS vulnerability is real and needs to be mitigated.
- Point solutions will not scale and will become impossible to manage.
- Don’t limit your options. Have a strategy to transition from a traditional substation to a smart substation.
- Time sync will continue to increase in importance. Quality and expertise matter.

Q&A

Ralph Mackiewicz

VP, Business Development
SISCO

Ralph@sisconet.com

Debra Henderson

Director, Power Utility Markets
Symmetricom
dhenderson@symmetricom.com

Key Takeaways

- IEC 61850 provides the tools to manage the complexity of WAMPAC systems.
- WAMPAC systems require absolute time synchronization within the area.
- A timing strategy is essential to ensure that you have a secure, accurate and reliable time reference.

IEC 61850 and IEEE 1588 standards are designed to ensure WAMPAC system performance and lower TCO.

Thank You

SGC-1500 Smart Grid Clock

- Multiple GigE ports
- GPS timing receiver
- PTP Power Profile GM
- PTP Telecom Profile slave*
- Secure management
- NERC CIP compliance

- IRIG-B, DCF-77, pulse rates, 10MPPS output timing ports
- T1/E1, Fiber optic, Open collector outputs
- Rubidium oscillator option
- IEC 61850-3, IEEE 1613 hardened

**Additional information on the PTP Telecom Profile is available on the Symmetricom website (recorded webinar and white paper.)*

SISCO Products & Services for Utilities

- IEC 61850 for Power System Automation & Control
  - Portable Source Code for Embedded Systems
  - Off-the-Shelf IEC 61850 Interfaces using OPC
- Unified Analytic Platform for real-time analytics:
  - Wide Area Protection using GOOSE for C-RAS
  - Synchrophasor processing for WAMS
- CIM based Integration for Smart Grid applications
- CIM Adapter for PI: Enabling OSIsoft PI with power system models

www.sisconet.com