# SYNCHROPHASORS AND SECURITY

North American SynchroPhasor Initiative
Presentation to NERC CIPC
June 9, 2011

NASPI North American
SynchroPhasor Initiative

# Phasors and security
Overview

1. Synchrophasor technology is another tool to improve reliability
2. Synchrophasor technology is maturing
3. Phasor deployments vary by company, purpose and design
4. Operations-supporting phasor system designs include security
5. Not all phasor systems are critical cyber assets, but all phasor systems will be CIP-compliant and cyber-secure.

# Synchrophasor uses

Synchrophasor systems are being used to protect and improve grid reliability

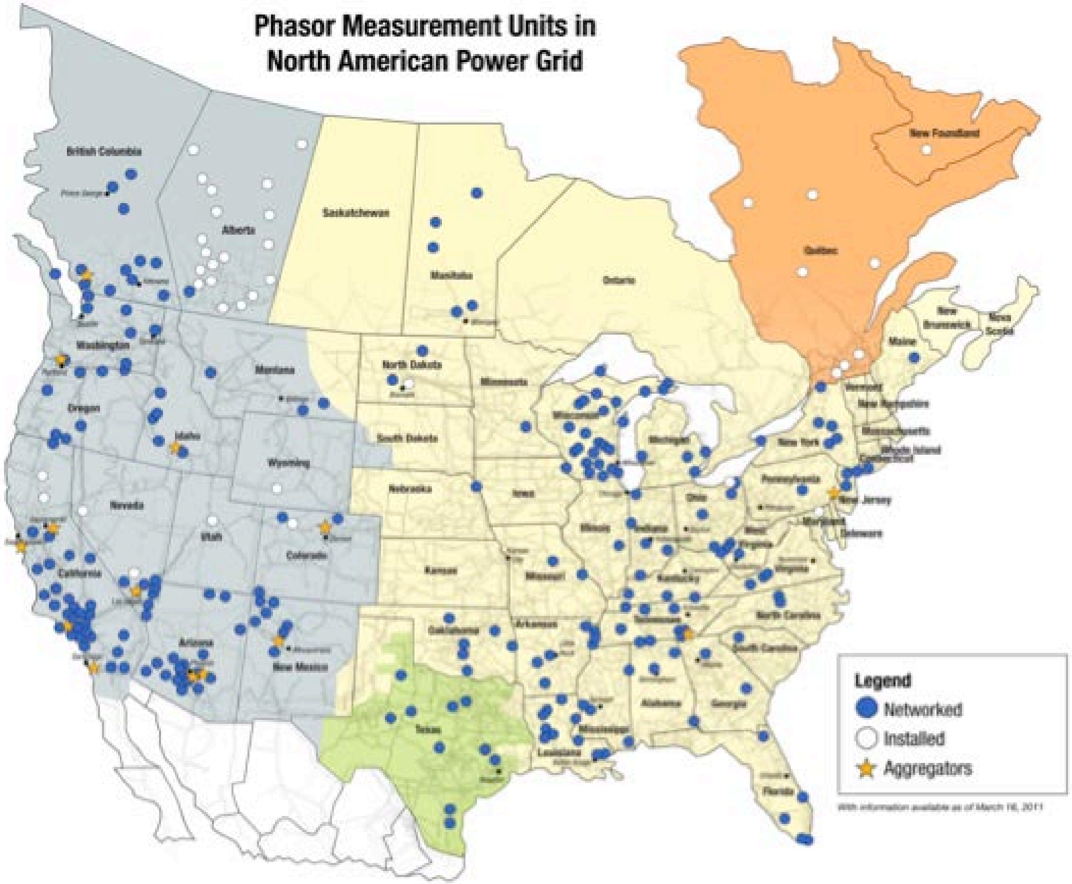
- Real-time applications
  - Wide-area situational awareness and visualization
  - Frequency monitoring and trending, island detection
  - Power oscillation monitoring
  - Voltage monitoring and trending
  - Alarming and setting operating limits
  - Event detection and avoidance
  - State estimation
  - Dynamic line loading and congestion management
  - Automated controls
  - Mode-damping estimates
- Planning and off-line applications
  - Baselining power system performance
  - Forensic analysis
  - Static and dynamic model calibration and validation
  - Power plant model validation
  - Special protection schemes and islanding

# Synchrophasor technology is maturing

- Most pre-2010 phasor systems are R&D-based with evolving applications, inconsistent maintenance by asset owners, diverse communications systems, and varying reliability of system performance.
- New systems funded by DOE ARRA grants are moving toward production-grade.
  - 13 DOE projects involving 57 RTOs, ISOs and utilities, funded by Smart Grid Investment Grants that will install over 850 new Phasor Measurement Units, high-speed dedicated communications systems, improved data applications, and user training.
  - High quality, commercially supported, volume production of standards-based PMUs
  - Rigorous design of phasor systems for reliability, functionality and security.
- By the end of the SGIG project period (2014), we'll be able to build upon the lessons learned about communications, applications, and security to fine-tune current systems to production-grade.

# PMU locations as of early 2011

Over 850 more networked PMUs and data concentrators will be added to the North American grid through 2013.



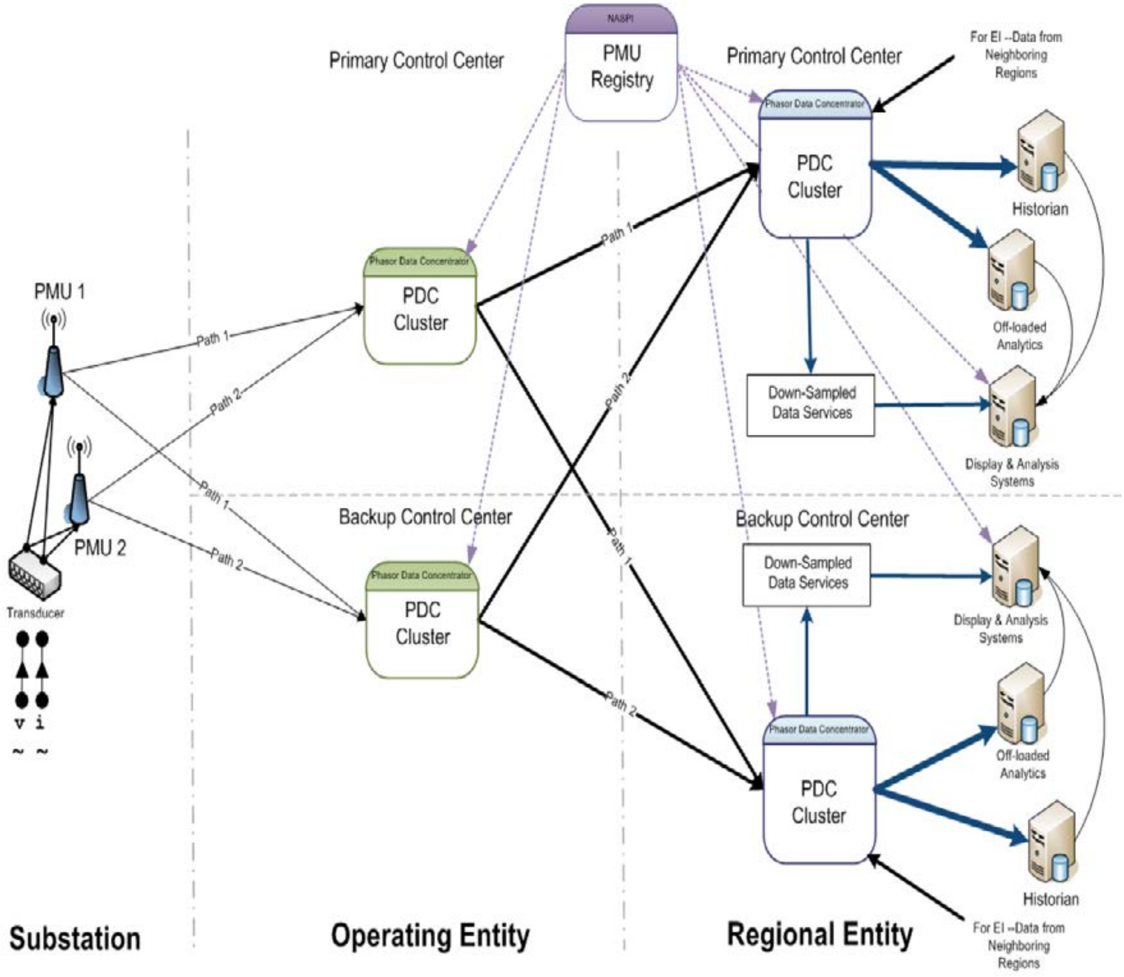
# Synchrophasor technology overview

- Phasor Measurement Units (PMUs) provide GPS time-stamped measurement and derivation of current and voltage phasors and frequency and frequency rate of change.
- Data from multiple PMUs are combined and time-aligned by a Phasor Data Concentrator (PDC) to provide a comprehensive set of data for a region or interconnection.
- PMUs typically provide measurements at 30 samples per second; some are sampling at 60 samples/sec with 120 samples/sec on the horizon.
- These high sample rates quickly create large volumes of historical phasor data that need to be analyzed and archived.
- Reliable, production-grade phasor systems are possible today due to advances in high-speed measurement, high-volume data storage capabilities and costs, high-speed communications, and high-speed analytics.

# Synchrophasor system elements

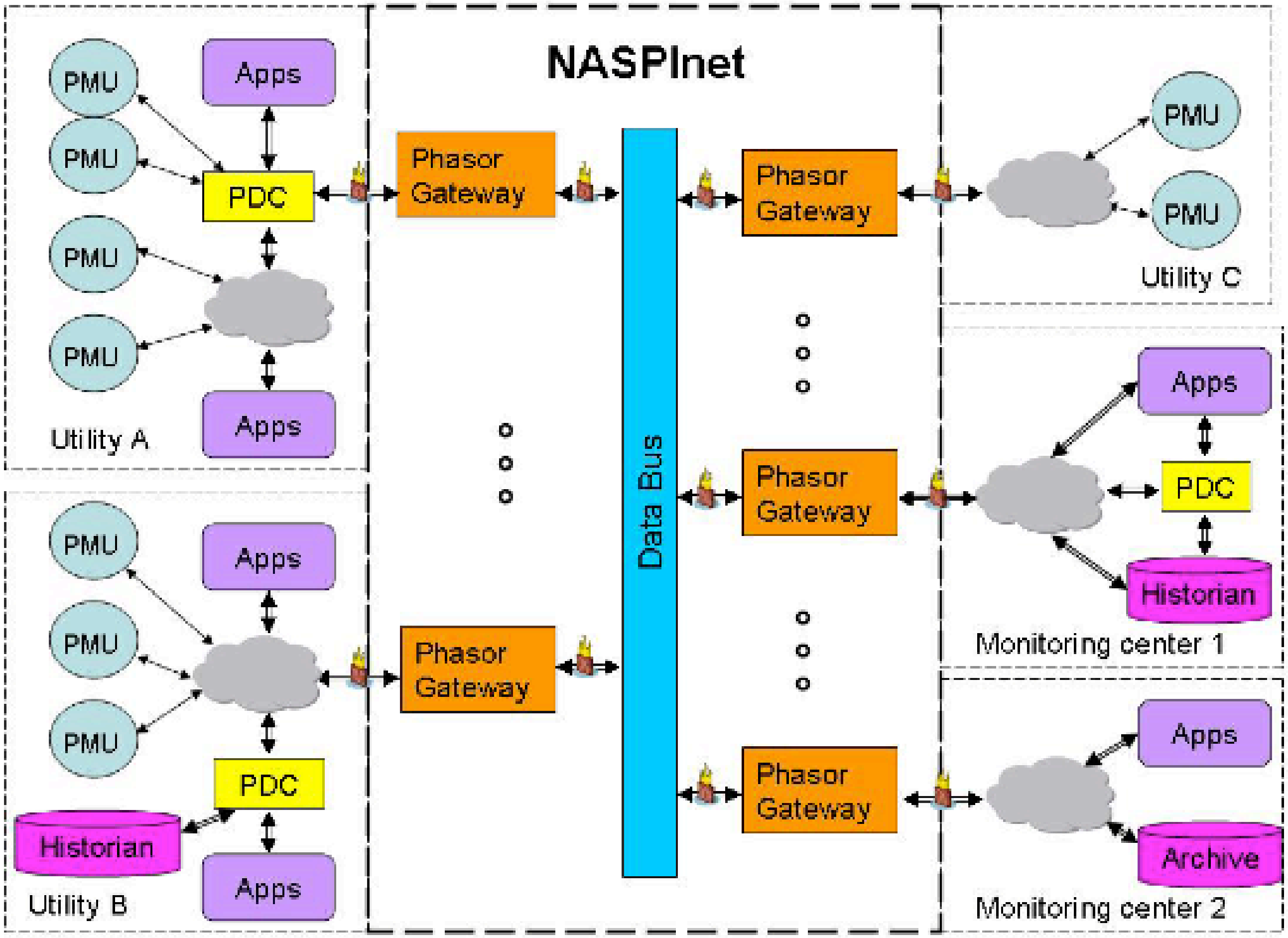
Key elements:

- PMUs
- Communications
- PDCs at local,
  asset owner,
  regional entity levels
- Applications



# Phasor communications network design

NASPInet -- Conceptual architecture for future phasor data networks; several SGIG projects will implement and test versions of NASPInet.



# Phasor Gateways are coming into service

- NERC-NASPI and DOE have been developing the technical requirements for a secure appliance to exchange phasor data since 2008 (like ICCP but with newer IT tools).
- Phasor Gateways:
  - Create a hardened security buffer between critical internal and external systems
  - Provide high-quality encryption to protect the confidentiality of reliability and market sensitive BES data
  - Facilitate and reduce the cost of phasor data exchange -- both the phasor data itself and the configuration information for this data
- Three SGIG projects will use PGs – Entergy, SCE and WECC.
- NERC is funding the development of a phasor gateway to accelerate the understanding and use of this technology. The alpha version of this gateway is now in service between TVA and Entergy.
- This gateway is open source and is available for download and test.

# Phasor systems and security

- Phasor systems are becoming part of the bulk electric system and will require physical and cyber-security – but phasor systems shouldn't be treated any differently than other forms of measurement and control telemetry.
- Phasor systems coexist with BES cyber infrastructure and will have similar dependencies on common communications and network elements. One common elements is likely to be transport (e.g., NERCnet).
- Phasor system designers and owners are learning from legacy EMS and cyber-security issues and leveraging emerging cyber-security standards and technologies.
- Phasor systems are being designed with both functionality and security in mind, using a risk-based approach.
- New phasor hardware and software components are being built with integral security measures and practices.
- Phasor Data Gateways and PDCs are important edge devices, much like ICCP nodes, to isolate and protect critical infrastructure.

# Security perspective

- Today almost all phasor systems and applications are NOT mission-critical.
- Phasor information is NOT yet the sole basis for operating decisions or control actions that support the reliable operation of the BES.
- Currently available phasor applications require further data analysis, software refinement and operational validation to be fully effective; many are in advanced development and testing and are not in full control room use.
- However, use of phasor data for control room decisions and/or automated control is now within a 5 year horizon.
- Many phasor applications need real-time data, so latency created by some cyber-security measures is a big concern.
- Cyber-security practices and technologies are still evolving (see, e.g., NISTIR 7628 and ASAP-SG WAMPAC draft) as well as iterations of NERC CIP.

# Phasor projects and cyber-security

- Critical asset and critical cyber asset determinations are made by asset owners to reflect current role and future uses of phasor information (e.g., wide-area monitoring v. automated controls).
- Security designs reflect SGIG award winners' plans for near-term phasor data use as well as ease of integration within existing architectures. High consistency of approach within each multi-utility SGIG project.
- SGIG phasor projects have been designed using risk-based assessments to enable later security upgrades as system status and use become more critical.
- Phasor system hardware and software are deployed within physical environments with traditional power system control and protection (substations and control rooms).

# SGIG phasor project cyber-security plans

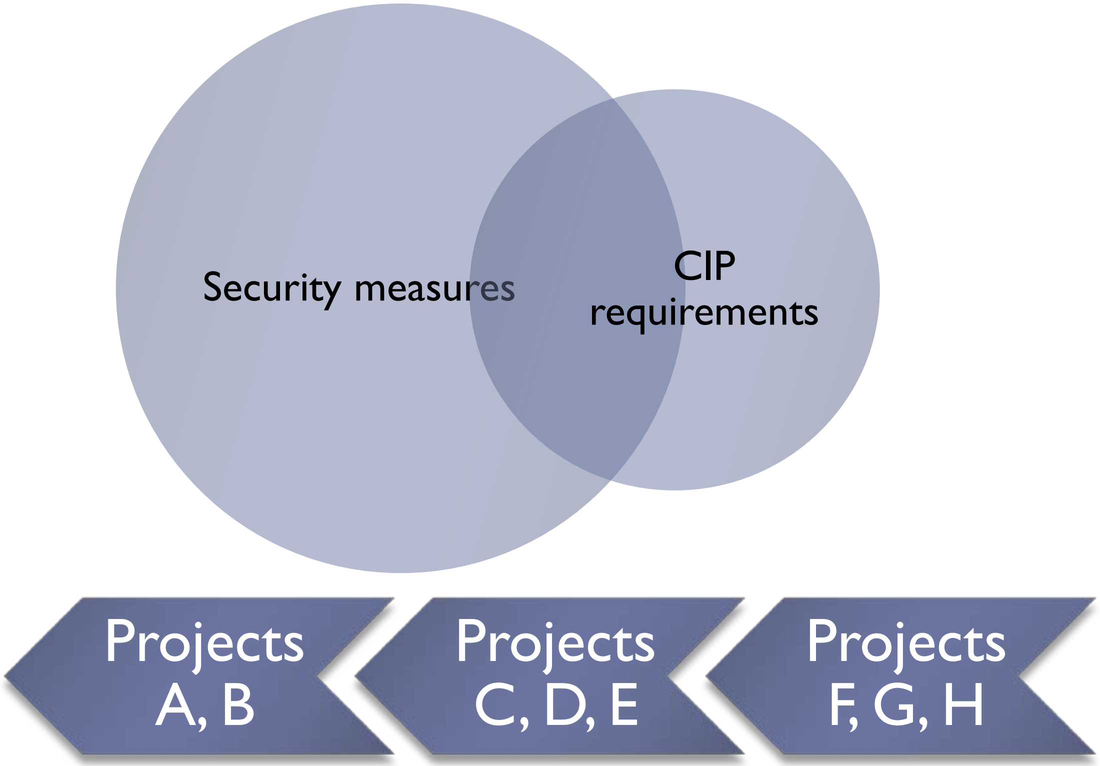
All ARRA SGIG projects committed to a technical approach to cyber-security that included:

- identification of cyber-security risks and how they will be mitigated at each stage of the lifecycle (focusing on vulnerabilities and impact),
- cyber-security criteria utilized for vendor and device selection,
- relevant cyber-security standards and/or best practices that will be followed, and
- plan for how the project will support emerging smart grid cyber-security standards.

DOE cyber-sec team reviewed all SGIG project designs to assure basic inter-operability and cyber-security measures consistent with each project's cyber-sec plans.

# SGIG phasor projects vary in their approach to security

The timing of security hardening for phasor data systems varies among the SGIG projects, but all are CIP-compliant.



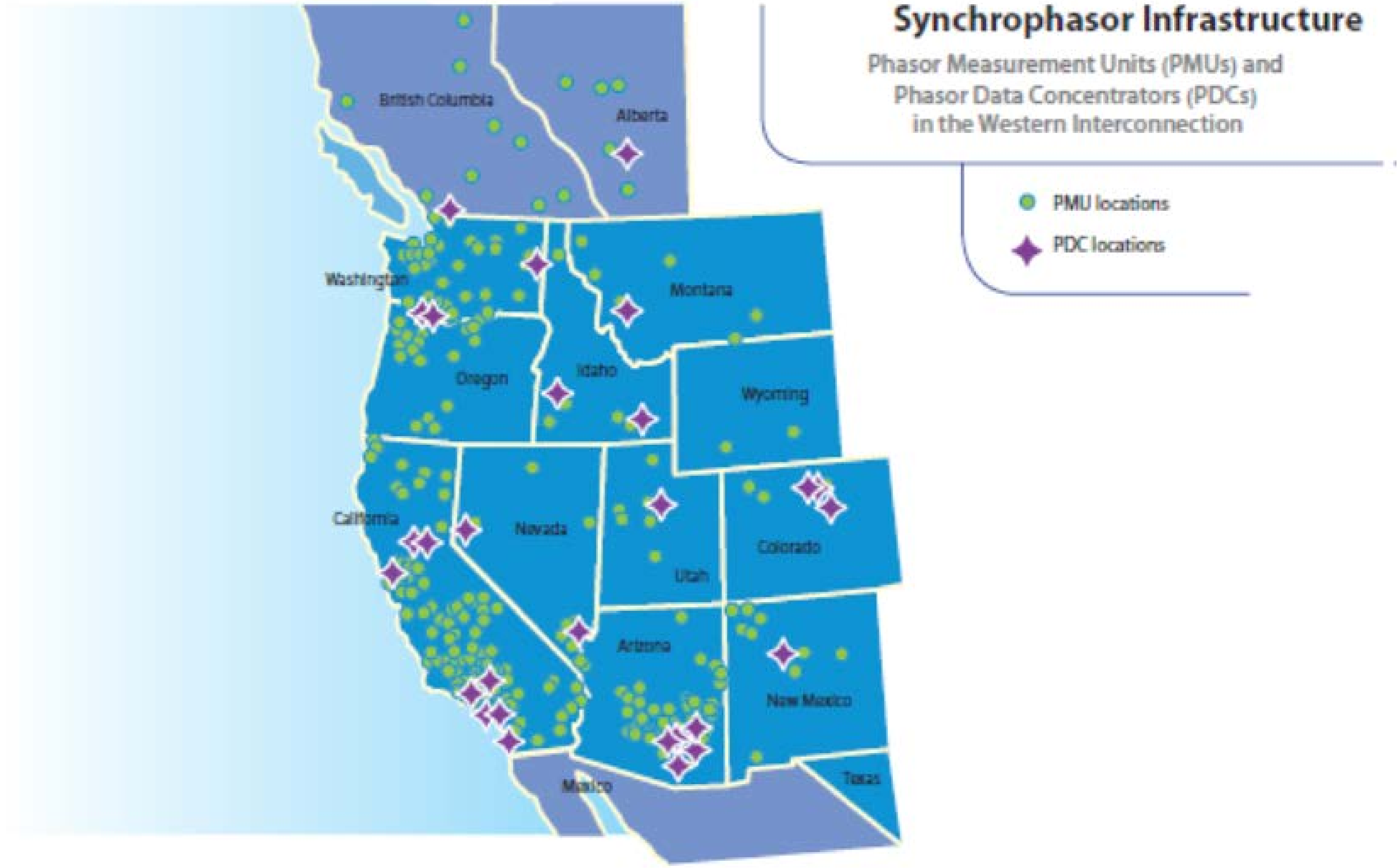
**Very** high security and CIP-compliant today

Secure and CIP-compliant today, more secure later

# Example 1 -- WISP

- Western Interconnection Synchrophasor Project (WISP) is an interconnection-wide synchrophasor program expected to enable smart grid functionality
- WISP will deploy:
  - Upgraded, replacement or new Phasor Measurement Units (PMUs) – 341 devices expected
  - Phasor Data Concentrators (PDCs) – 62 devices
  - Historical data archival systems at WECC RCs
  - Network architecture to connect measurement devices.
- Real-time and off-line applications for:
  - Situational awareness for operators and reliability coordinators
  - Event and system performance analysis for operations and planning engineers
  - Model validation and improvement
  - Real-time control and protection – including wide-area controls
  - System restoration.

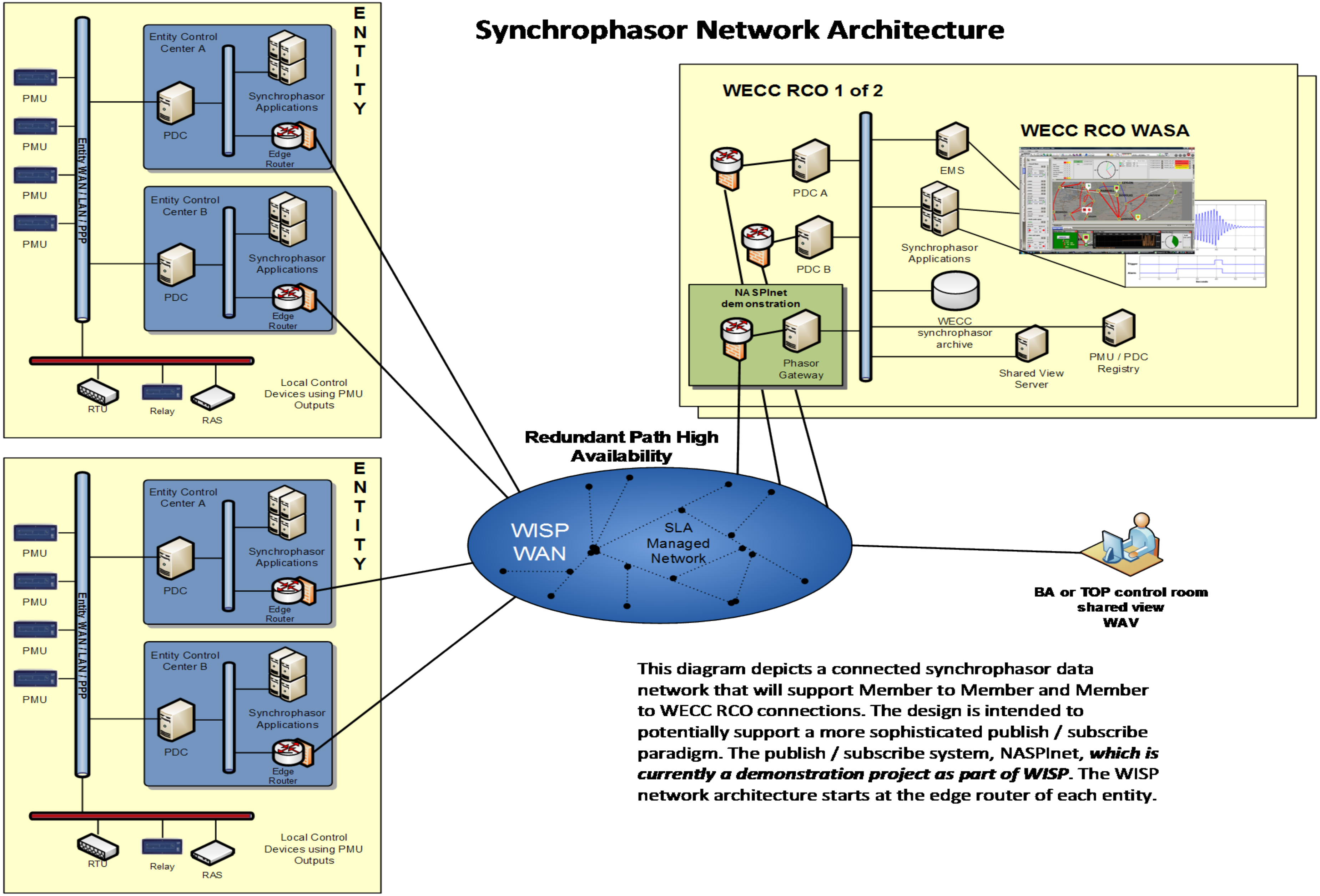
# WISP Overview



Synchrophasor Infrastructure

Phasor Measurement Units (PMUs) and Phasor Data Concentrators (PDCs) in the Western Interconnection

# Synchrophasor Network Architecture



This diagram depicts a connected synchrophasor data network that will support Member to Member and Member to WECC RCO connections. The design is intended to potentially support a more sophisticated publish / subscribe paradigm. The publish / subscribe system, NASPInet, ***which is currently a demonstration project as part of WISP***. The WISP network architecture starts at the edge router of each entity.

# Security for current and future compliance WISP

- WECC will be responsible for cyber-security of its Reliability Coordinator (RC) facilities and equipment, and at connection points to the newly planned synchrophasor wide area network (WAN).
- Participant entities are responsible for their cyber-security and relevant standards that allow an integrated end-to-end security of the entire system (PMU thru WECC RC systems).
- WECC WISP production systems are placed in an Electronic Security Perimeter (ESP) that includes CCAs:
  - WECC Risk Assessment, as merged with CIP 002, determined that its WISP systems are currently not a "Critical Asset" as prescribed.
  - WECC WISP systems are subject to CIP 005-R1.4, which makes them subject to CIP002-CIP009 if they reside within the ESP.
  - It is expected that all WECC WISP production systems will become Critical Assets once deployed and accepted by the WECC RC.

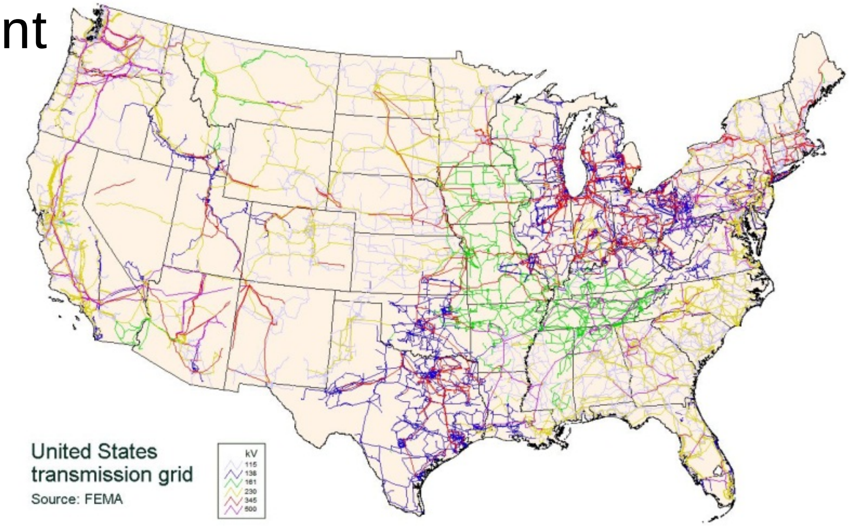
# Example 2

## Southern California Edison
## Common Cyber Security Services (CCS)

June, 2011

# Grid Modernization

- Strategic energy policy goals
- broad deployment of new technologies
- increased connectivity, automation and virtualization
- introduces vulnerabilities and risks to the electric grid from cyber security incidents
- Increasing hostile threat environment



United States transmission grid

Source: FEMA

# Grid Modernization Security Challenges

- Most Stakeholders recognize Smart Grid security challenges
- An evolving landscape creates new organizational challenges
- Rapid pace of adoption creates a new set of technical challenges

# Meeting cyber security challenges

- Design security into Smart Grid Architectures from the beginning
- Use a common services architecture
- Use gateways coupled with physical security to allow legacy devices to participate
- Use standards-based security solutions to ensure interoperability across multi-vendor solutions
- Ensure people, processes as well as new security technologies are designed and implemented together to ensure secure operations
- Ensure the security implementation does not introduce single points of failure in the Smart Grid Architecture
- Use military-grade security from the beginning to protect against constant, rip and replace and re-documentation as security standards evolve
- Security solutions should be end-to-end across the electric grid, regardless of asset classification (i.e. transmission vs. distribution)

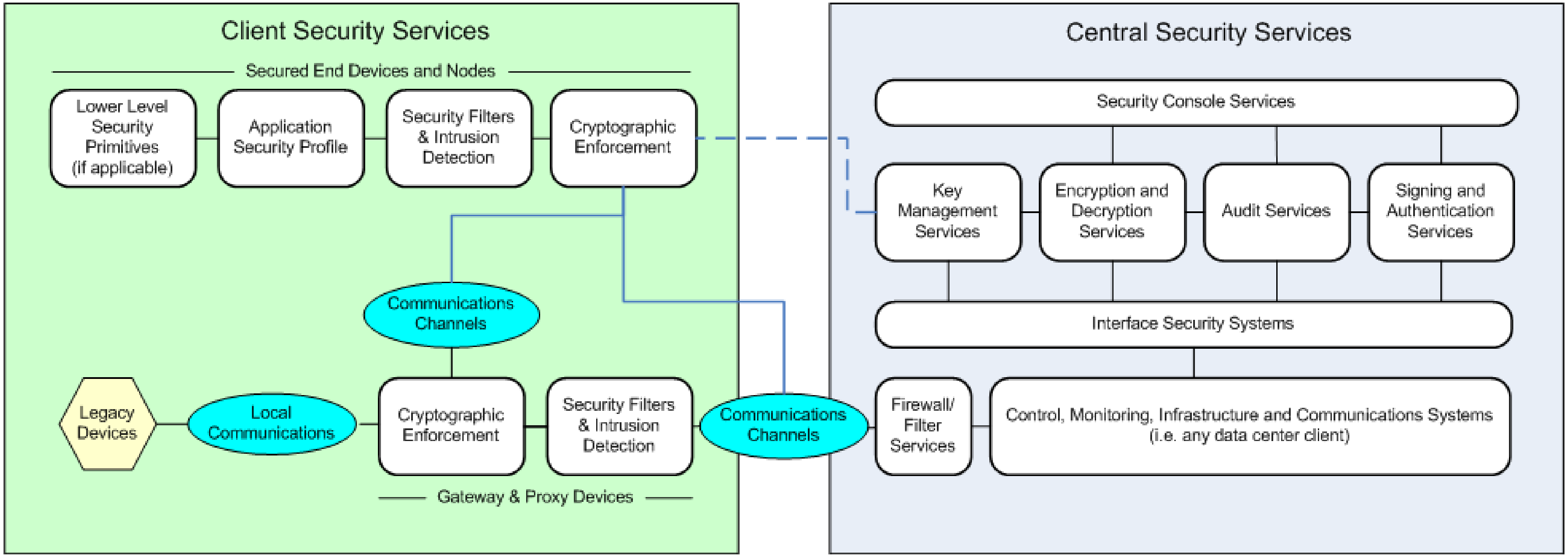
# Common Cyber-Security Services Goals

- A common cyber-security services approach is required to address the impacts and requirements across Smart Grid related projects
- As such, SCE’s NERC-CIP program shall develop Common Cyber-security Services (CCS).
- Provides set of Information Assurance and Cyber Security functions essential for secure and reliable operation of Edison’s Smart Grid infrastructure and assets.

# SCE's Common Cyber Security Solution

## Solution Highlights

- Designed to meet current and expected future NERC and NIST standards
- Transfers security technology from military and intelligence industry
- Allows legacy devices to participate in a secure Smart Grid Architecture
- Provides a path to evolve the architecture over time
- Designed to scale and communicate across diverse communication protocols
- Designed to integrate with multiple vendor solutions and technologies


Client Security Services
Secured End Devices and Nodes
Lower Level Security Primitives (if applicable)
Application Security Profile
Security Filters & Intrusion Detection
Cryptographic Enforcement
Communications Channels
Legacy Devices
Local Communications
Cryptographic Enforcement
Security Filters & Intrusion Detection
Communications Channels
Gateway & Proxy Devices
Central Security Services
Security Console Services
Key Management Services
Encryption and Decryption Services
Audit Services
Signing and Authentication Services
Interface Security Systems
Firewall/ Filter Services
Control, Monitoring, Infrastructure and Communications Systems (i.e. any data center client)

# Sustainable Smart Grid Security

***A Smart Grid Security Lifecycle is needed to ensure system security evolves as capabilities and threats evolve***

- Objectives:
  - Increase reliability through security
  - Extend reach and capabilities of operational technologies
  - Accelerate security technology and standards
  - Encourage competition through interoperability and certification
  - Help foster a sustainable market
- Education and outreach
  - Security concerns while challenging are manageable
  - Industry and regulations needs to adapt next generation principles
  - Infuse technology lifecycle with security engineering (research, commercialization, acquisition, operations)
- Specification Adoption
  - Develop detailed build to specification based on standards and make them broadly available to vendors, utilities and other stakeholders
  - Use requirements and specifications to motivate vendors and Standards Development Organizations (SDOs)
  - Develop certification processes against the standards and informed by successful implementations

# Centralized Capabilities

- **SmartGrid PKI** – a set of certificate based services for managing equipment in the field for authentication and system integrity
- **SmartGrid Policy Manager** – Authorization service for creating and managing SmartGrid asset rights
- **Boundary Enforcement Manager** – Manages policy rules associated with filtering and deep content inspection
- **Group Key Manager** – The industry's first cryptographic service which allows for the dynamic creation of groups and communities of interest
- **Trust Manager** – A service which allows data to be processed according to trustworthiness thorough the use of rules and data tagging
- **Audit Manager** – A service which captures and analyzes audit data includes alarming, pattern matching and other next generation audit functions

# Requirements for Securing Edge Devices

- Device Hardening Requirements: prevent local tampering and reverse engineering
- Device Security Performance Requirements: Transport protocol, QoS algorithm support
- Device Attestation Requirements: device ability to self-test and report security health
- Device Cryptographic Requirements: cypher-suites, cryptographic algorithms and security interoperability
- Device Audit requirements: Monitoring, Reporting and Alarm handling

# Where are we right now?

- SCE Interim security solutions case-by-case analyses with Planned Migration to Full automated common security solution across SCE domains
- Many vendor providing technology in security area supports this model
- Gap exists in product maturity for full security automation, but manageable with interim point solutions
- Allows for complete end-to-end security analyses of routed protocols between IED's and data collection points per NERC-CIP-002

# Synchrophasor systems are NOT automatically critical cyber assets

- CIP standards state the function and linkages of an asset determine its criticality.
- The presence of a PMU in a substation does not make a previously non-critical substation a critical asset, nor does it make the PMU a critical cyber asset.
- The location of phasor hardware within a critical substation or control room does not in itself make the phasor hardware critical (although it benefits from location inside a secure perimeter).
- If a communications network carries phasor data, the network does not automatically become a critical cyber asset; but if phasor hardware is on a network with other CCAs, it must be treated as a CCA (even if its role is not critical).
- Operators make control decisions using inputs from many sources – relays, SCADA, news reports, weather forecasts, lightning detection systems – but that use does not solely justify labeling a control input source as a critical asset.
- Critical cyber asset status for phasor systems must be determined by the asset owner within the deployment context and use, not determined by CIPC or FERC based on generalities and assumptions.

Many phasor systems will be highly cyber-secure without being critical cyber assets.

# Conclusions

- Phasor data will become an important or critical element of BES planning and operation.
- The timing from a NERC perspective is soon – but no earlier than the completion of the SGIG projects (late 2013)
- Phasor technology can be expected to undergo rapid change and refinement over the next decade.
- Security for phasor data will be as important, but likely no more so, than other critical cyber infrastructure
- Due to nature of phasor information – continuous, high-volume data flows – new systems will be required to collect, process and protect phasor information.

# References and sources

- NASPI report for NERC, Real-time Application of Synchrophasors for Improving Reliability, 10/10 -- http://www.naspi.org/resources/resources.stm
- WISP – http://www.wecc.biz/awareness/Pages/WISP.aspx
- DOE ARRA resource – www.ARRASmartGridCyber.net
- NASPInet framework -- http://www.naspi.org/naspinet.stm
- openPG – http://openpg.codeplex.com/
- NISTIR 7628, 10/10, at http://csrc.nist.gov/publications/PubsNISTIRs.html#NIST-IR-7628
- UCA ASAP-SG  WAMPAC draft -- http://www.smartgridipedia.org/images/5/5e/WAMPAC_Security_Profile_-_v0_08.pdf

# NASPI presenters and contributors

- Jeff Dagle (PNNL) -- jeff.dagle@pnl.gov
- Dan Brancaccio (Bridge Energy Group for WISP) -- dbrancaccio@bridgeenergygroup.com
- Tony Johnson (SCE) -- anthony.johnson@sce.com
- Alison Silverstein (NASPI) – alisonsilverstein@mac.com
- Russell Robertson (Grid Protection Alliance) -- rrobertson@gridprotectionalliance.org
- Terry Bilke (MISO)
- Scott Mix (NERC)
- Larry Bugh (ReliabilityFirst)