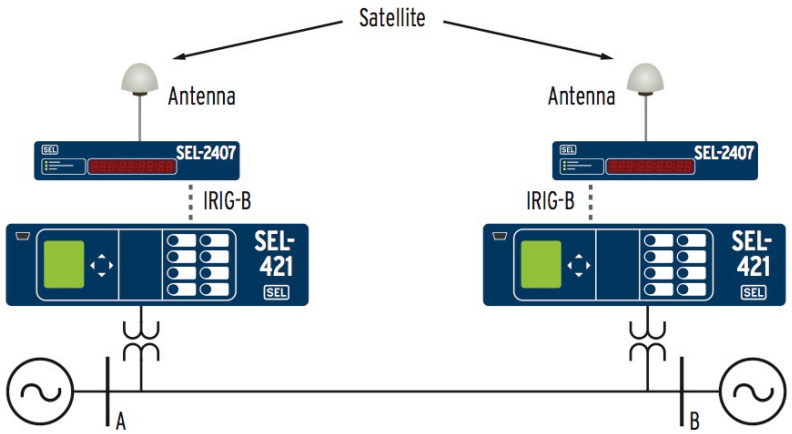
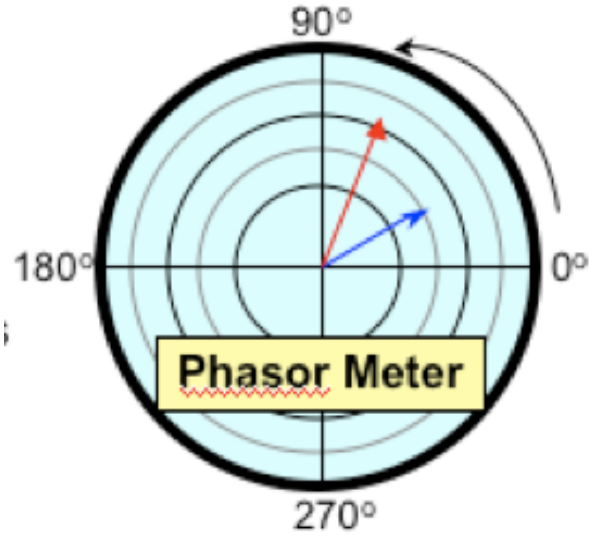
Secure Delivery of Time-Critical Data on NASPInet: Requirements and Challenges

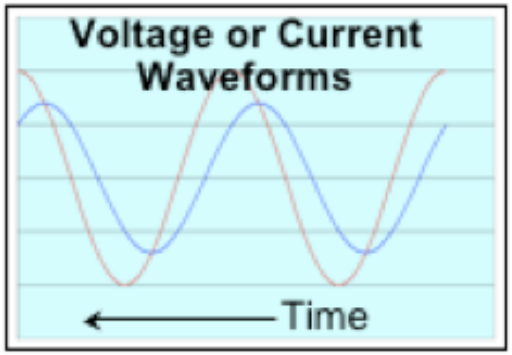
Rakesh Bobba

OMG Workshop on Real-Time, Embedded and Enterprise-Scale Time-Critical Systems
May 26, 2010

PMUs and Synchrophasors







- **Traditional SCADA data since the 1960's**
  - Voltage & Current Magnitudes
  - Frequency
  - Every 2-4 seconds
- **Data from Phasor Measurement Units (PMU's)**
  - Voltage & current phase angles
  - Rate of change of frequency
  - Time synchronized using GPS and 30 - 120 times per second

SynchroPhasor Applications

RESEARCHERS

- Automatic alarming of RAS
- Out of step protection
- Short/long-term stability control
- FACTS feedback ctrl

PLANNERS

- Post-mortem analysis
- Model validation
- Phasor network performance monitoring & data quality
- Email notifications
- Test new real-time applications

RELIABILITY COORDINATORS

- Situational awareness dashboard
- Real time compliance monitoring
- Frequency Instability Detection/Islanding

OPERATORS

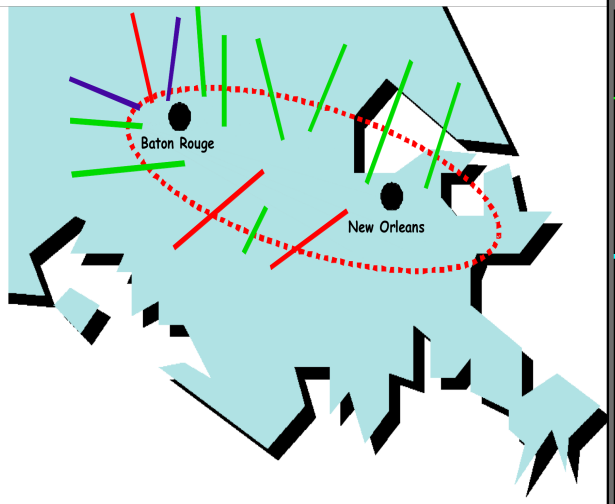
- Real time performance monitoring
- Real time alerts and alarms
- Event detection, disturbance location
- Suggest preventive action
- Interconnection state estimation
- Dynamic ratings

Credit: NASPI Operations Implementation Task Team (OITT)

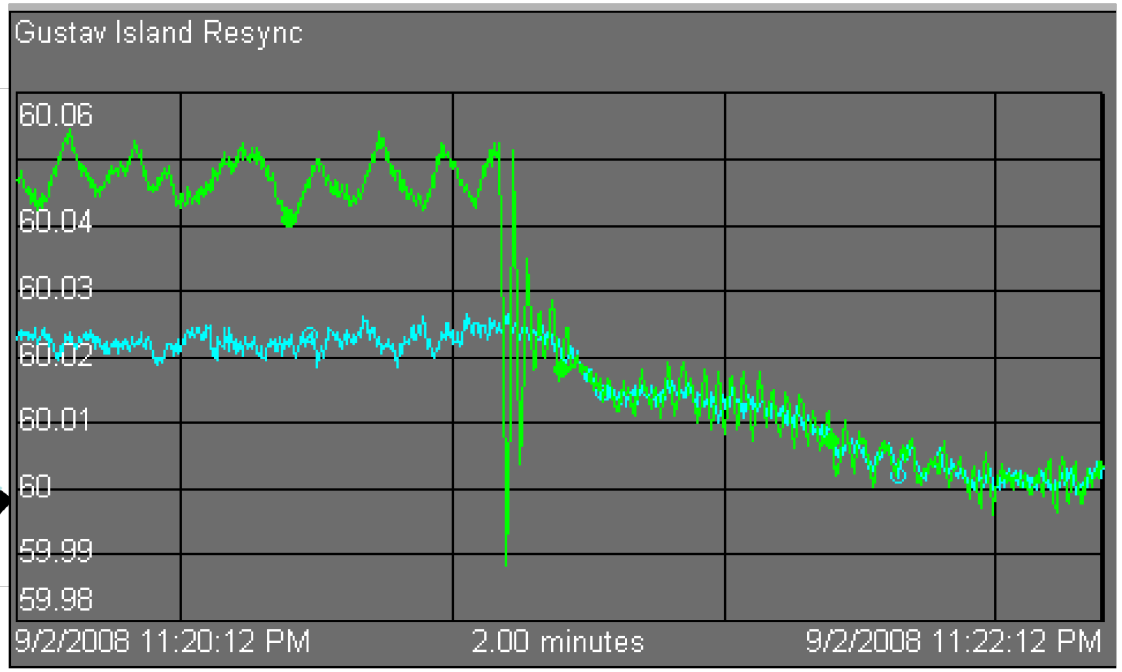
Real World Example

Entergy and Hurricane Gustav -- a separate electrical island formed on Sept 1, 2008, identified with phasor data

Island kept intact and resynchronized 33 hours later



Source: Entergy



PMU Applications and Deployment

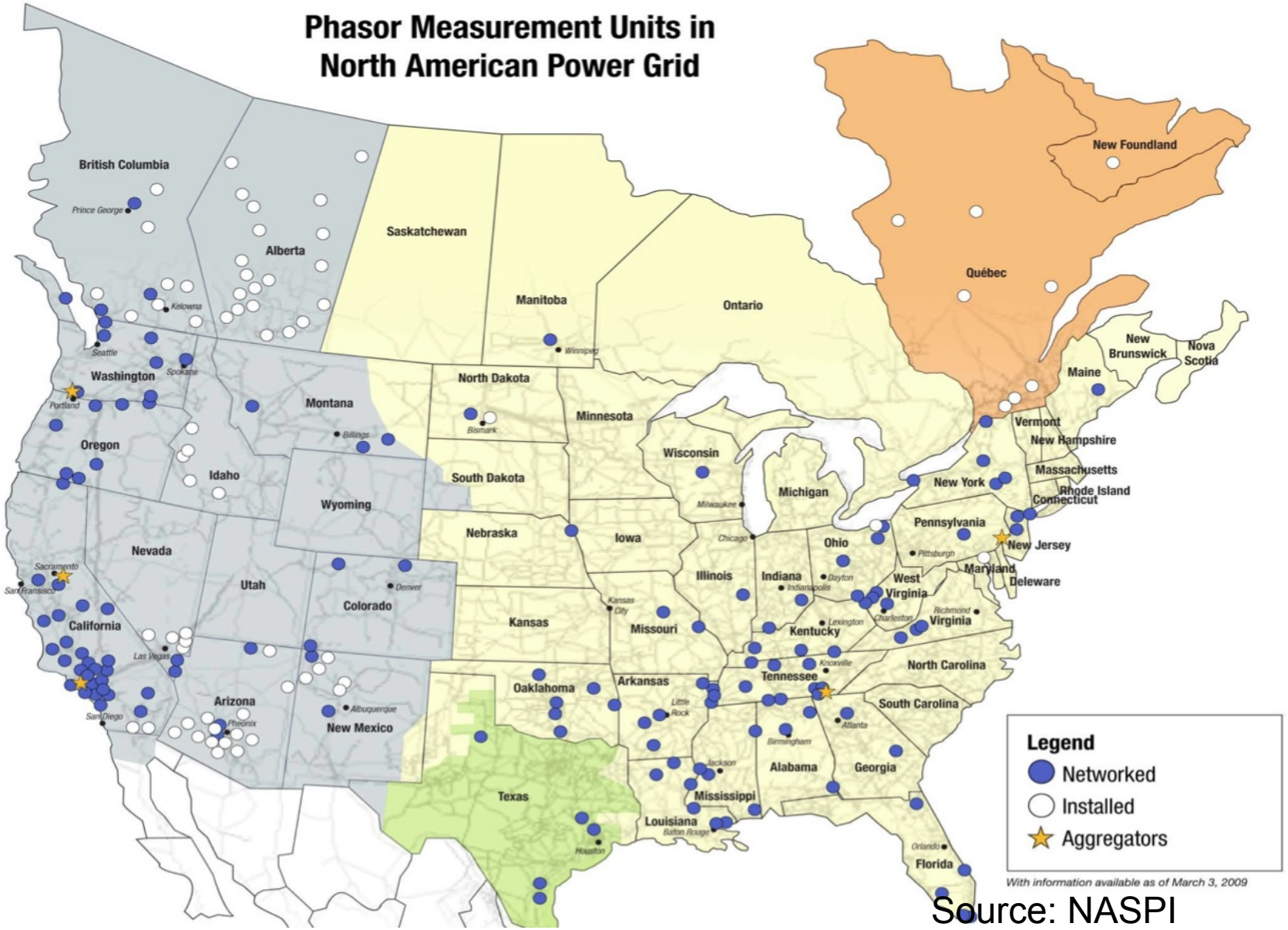
table 1. PMU deployment in different parts of the world.

PMU Applications	North America	Europe	China	India	Brazil	Russia
Post-disturbance analysis	√	√	√	P	T	√
Stability monitoring	√	√	√	P	P	√
Thermal overload monitoring	√	√	√	P	P	√
Power system restoration	√	√	√	P	P	P
Model validation	√	√	√	P	T	√
State estimation	P	P	P	P	P	P
Real-time control	T	T	T	P	P	P
Adaptive protection	P	P	P	P	P	P
Wide area stabilizer	T	T	T	P	P	P

T = Testing phase; P = Planning stage

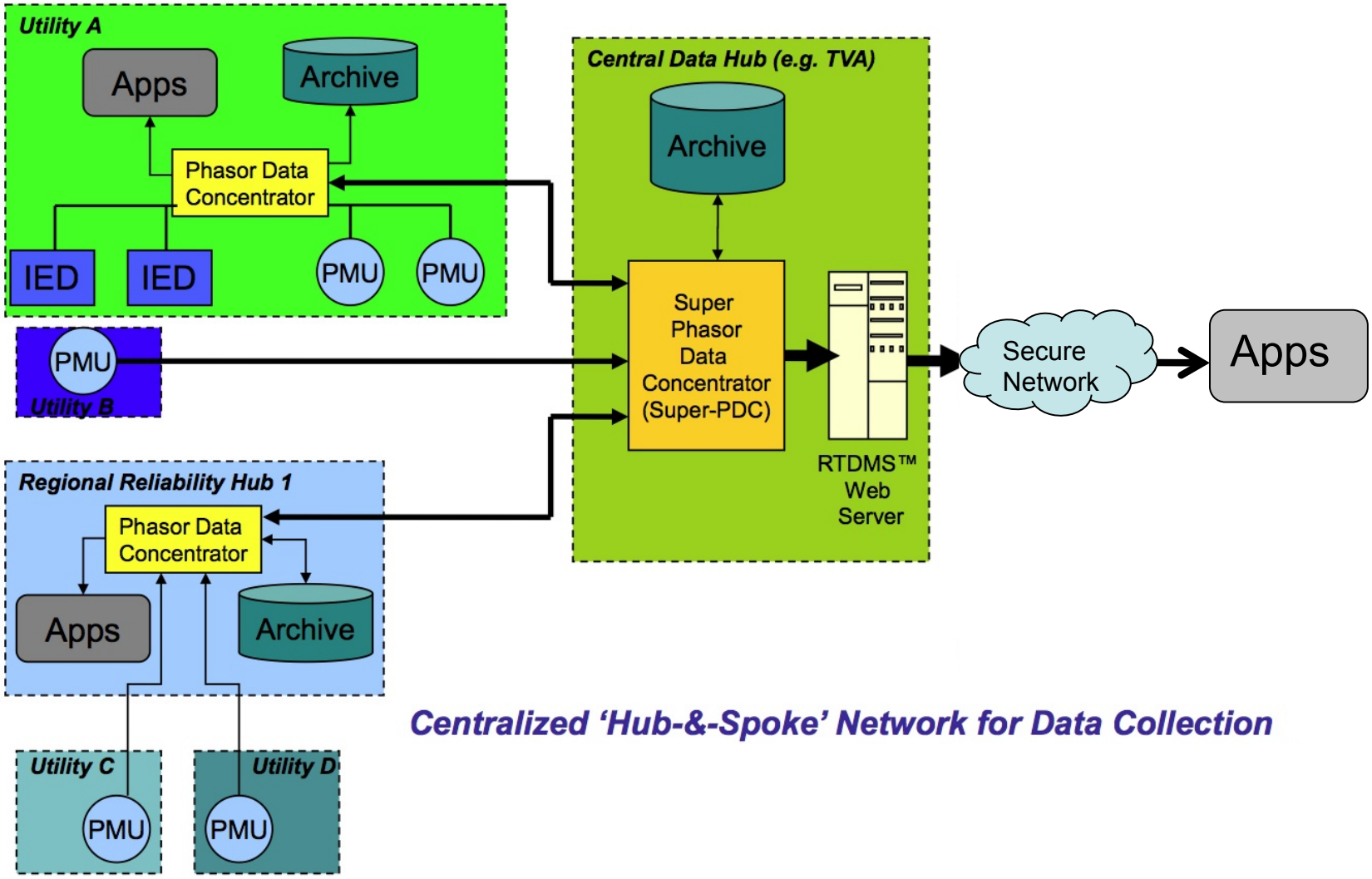
Source – Chakrabarti, Kyriakides, Bi, Cai and Terzija, “Measurements Get Together,” IEEE Power & Energy, January-February 2009

Current PMU Deployment



Source: NASPI

Current Architecture for PMU Data Sharing



Centralized 'Hub-&-Spoke' Network for Data Collection

Source: NASPI

Towards a Distributed PMU Data Network

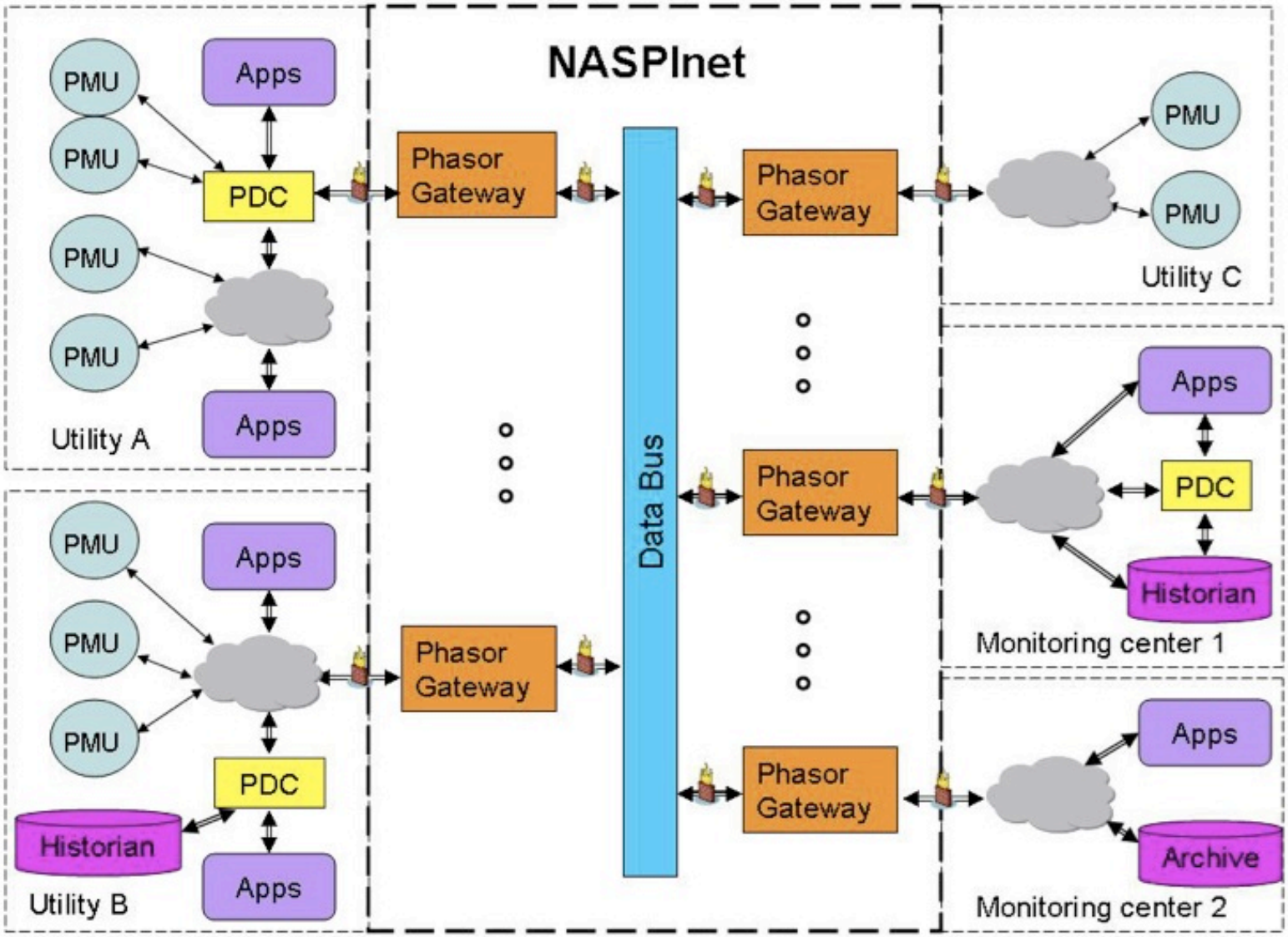
- Centralized Network
  - not scalable
- Need a de-centralized network
  - NASPInet - “industrial grade”, secure, standardized, distributed, and expandable data communications infrastructure to support synchrophasor applications
  - NASPI - North American SynchroPhasor Initiative, a collaborative effort between U.S. DOE, NERC, electric utilities, vendors, consultants, federal and private researchers and academics
    - Mission: to improve power system reliability and visibility through wide area measurement and control
  - NASPI (D&NMTT) proposed a conceptual architecture
  - further refined in NASPInet specifications

Why NASPInet?

- Ad-hoc approaches
  - do not scale
    - e.g., point-to-point links -> $O(n^2)$ for full connectivity
  - not efficient
    - e.g., same signal has to be sent over many links
  - do not interoperate

- Need to be ready for an explosion of PMU applications
  - e.g., iPhone and its apps caused 5000% increase in data traffic for AT&T Wireless

De-Centralized NASPInet: Conceptual Architecture



Source: NASPInet Spec.

NASPInet Requirements and Challenges

- Large distributed network - continental scale, peer-to-peer?
- Quality of Service (QoS) - prioritization of traffic, latency management etc
- Security of PMU data – integrity, availability and confidentiality, key and trust management, network admission control, intrusion detection, response, recovery
- Network management and security – performance, configuration, accounting, fault management, security management

NASPInet Challenges - Large Distributed Network

- Continental scale
  - Owner
    - single – who owns it?
    - multiple collaborating owners - interoperability
  - Monolithic or organic?
    - high initial cost if monolithic

- Network management and security
  - performance, configuration, accounting
  - fault and security management

NASPInet Challenges – Quality of Service (QoS) over WAN

- QoS goals per data flow are to minimize latency, delay, jitter, loss, error
- Overall QoS goals are to support dedicated bandwidth, resource provisioning and allocation, avoiding and managing network congestion, shaping network traffic and managing priorities
- Interoperable QoS enforcement potentially across multiple heterogeneous network domains

NASPInet Challenges - Quality of Service (QoS) over WAN

NASPInet Traffic Attribute	Real-time streaming data			Historical data	
	CLASS A Feedback Control	CLASS B Feed-forward Control	CLASS C Visualization	CLASS D Post Event	CLASS E Research
Low Latency	4	3	2	1	1
Availability	4	2	1	3	1
Accuracy	4	2	1	4	1
Time Alignment	4	4	2	1	1
High message rate	4	2	2	4	1
Path Redundancy	4	4	2	1	1

Table key:
4 – Critically important, 3 – Important, 2 – Somewhat important, 1 – Not very important

- Examples:
  - Real-Time Operations – low latency is critical (< 100ms), no gaps in data
  - Monitoring and Visualization – relatively higher latencies (~seconds) are tolerable, small gaps in data tolerable
  - Post Disturbance Analysis – lax latency requirements (~ hour), no gaps in data

NASPInet Challenges - Security of PMU Data

- Authentication and Integrity
  - Essential to ensure reliable and trustworthy decisions
  - Tools: cryptographic protocols leveraging digital signatures, HMACs, etc.
  - Challenges: efficiency, supporting one-to-many data exchanges, e.g, publish/subscribe and multicast

- Availability
  - Essential due to the critical nature of underlying power system
  - Specific requirements may vary by application classes
  - Tools: redundancy, security monitoring, attack detection and response, fail-safe design
  - Challenges: scalability and cost-effective design

NASPInet Challenges - Security of PMU Data

- Confidentiality
  - Needed to prevent unauthorized access to data
  - Tools: encryption protocols, access control
  - Challenges: efficiency for streaming data, supporting one-to-many data exchanges

- Key Management
  - Distribution and management of key material and credentials
  - Revocation
  - Tools: Public Key Infrastructure, on-line credential distribution/verification services
  - Challenges: scalability, trust establishment

NASPInet Challenges - Security of PMU Data

- Monitoring and compliance
  - Intrusion detection and response services
  - Future regulations may apply; e.g., NERC CIP
  - Tools: IDS, firewalls, etc.
  - Challenges: multi-organization coordination

Conclusion

- NASPInet enables many exciting and useful PMU data based applications
- Design and deployment of NAPSInet poses many challenges both from networking and security perspectives
- NASPI Data and Network Management Task Team (D&NMTT) is actively working on addressing these challenges

Questions?

rbobba@illinois.edu