Exploring a Tiered Architecture for NASPInet

Rakesh Bobba, Erich Heine, Himanshu Khurana and Tim Yardley

IEEE PES Innovative Smart Grid Technologies Conference
January 20, 2010
• 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)
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
### Table 1. PMU deployment in different parts of the world.

<table>
<thead>
<tr>
<th>PMU Applications</th>
<th>North America</th>
<th>Europe</th>
<th>China</th>
<th>India</th>
<th>Brazil</th>
<th>Russia</th>
</tr>
</thead>
<tbody>
<tr>
<td>Post-disturbance analysis</td>
<td>v</td>
<td>v</td>
<td>v</td>
<td>P</td>
<td>T</td>
<td>v</td>
</tr>
<tr>
<td>Stability monitoring</td>
<td>v</td>
<td>v</td>
<td>v</td>
<td>P</td>
<td>P</td>
<td>v</td>
</tr>
<tr>
<td>Thermal overload monitoring</td>
<td>v</td>
<td>v</td>
<td>v</td>
<td>P</td>
<td>P</td>
<td>v</td>
</tr>
<tr>
<td>Power system restoration</td>
<td>v</td>
<td>v</td>
<td>v</td>
<td>P</td>
<td>P</td>
<td>P</td>
</tr>
<tr>
<td>Model validation</td>
<td>v</td>
<td>v</td>
<td>v</td>
<td>P</td>
<td>T</td>
<td>v</td>
</tr>
<tr>
<td>State estimation</td>
<td>P</td>
<td>P</td>
<td>P</td>
<td>P</td>
<td>P</td>
<td>P</td>
</tr>
<tr>
<td>Real-time control</td>
<td>T</td>
<td>T</td>
<td>T</td>
<td>P</td>
<td>P</td>
<td>P</td>
</tr>
<tr>
<td>Adaptive protection</td>
<td>P</td>
<td>P</td>
<td>P</td>
<td>P</td>
<td>P</td>
<td>P</td>
</tr>
<tr>
<td>Wide area stabilizer</td>
<td>T</td>
<td>T</td>
<td>T</td>
<td>P</td>
<td>P</td>
<td>P</td>
</tr>
</tbody>
</table>

T = Testing phase; P = Planning stage

Current PMU Deployment

Phasor Measurement Units in North American Power Grid

Legend
- Networked
- Installed
- Aggregators

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
  - NASPI\textsuperscript{net} - “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 (DNMTT) proposed a conceptual architecture
      - further refined in NASPI\textsuperscript{net} 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 Challenges: Data Bus (DB) Design

• Technical
  – large distributed network - continental scale
  – quality of service (QoS) - prioritization of traffic, latency management etc
  – securing PMU data – integrity, availability and confidentiality, key and trust management, network admission control, intrusion detection, response, recovery
  – network management – performance, configuration, accounting, fault management, security management

• Business/Organizational
  – who owns/manages/provides the network
  – high initial costs
Proposed Solution: Tiered Architecture

- Tiered Architecture
  - leverages data locality
  - leverages the existing hierarchy
    - power grid operators, monitors and regulators
    - allows for incremental growth/formation of NASPInet
    - simplifies trust and key management needed for securing PMU data
    - simplifies network management with localized providers
    - simplifies QoS management
    - provides distributed computing opportunities
Proposed Tiered Architecture

Backup Internet Overlay

Managed Secure Real-time Link

Reliability Coordinator acts as Hub

Storage Computation Content Router Services

Optional Direct Link

Managed Secure Real-time Network

DATA BUS

University of Illinois Urbana-Champaign
• Different network providers for different Hub Networks
  • local provider manages network
    • need some co-ordination between providers
  • Hubs can translate between the networks
- **PGWs in same Hub network**
  - managed real-time links between PGW and Hub
- **PGWs in different Hub networks**
  - managed real-time network between Hubs
  - point-to-point links possible
Cyber Security

- Network Admission Control, Key and Trust Mgmt.
  - by Hubs in their local networks
  - collectively by Hubs or central trusted entity (e.g., FERC)
- Intrusion Detection Response and Recovery
  - network service providers
• Distributed Storage Opportunity
  – Hubs can act as caches for data
    • improves availability and reliability
    • leverages COTS components
    • e.g., OpenPDC leverages Hadoop DFS (runs on COTS)

Optional Direct Link
• Distributed Computing
  – leverages idle computing power at hubs
  – leverages in-network processing to minimize network transit
    • wide-area bandwidth is usually more expensive than computational power
    • e.g., distributed state estimation
• Tiered approach to NASPIInet makes many deployment challenges manageable
• Affords exciting opportunities for distributed services – storage and computing
• Lot more needs to be done
  – appropriate technologies – QoS, security
  – data formats
  – interoperability
• NASPI DNMTT is actively working on addressing the challenges
Questions?

rbobba@illinois.edu
Opportunities and Challenges

• **Opportunities**
  – Important applications emerging that require data sharing
    • Research into new applications needed
  – Smart Grid Investment Program to fund deployment of 800+ PMUs nation-wide

• **Challenges in data sharing**
  – Distributed network for data delivery
  – Tradeoffs between operational, regulatory and business aspects

• **Challenges in realizing NASPIinet**
  – Distributed wide-area network design
  – Network management
  – Quality of Service and real-time delivery
  – Cyber security
  – Progress on these topics made in recently released NASPIinet specification document (Quanta Technologies)
• 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
• A suggested approach: class-based QOS

<table>
<thead>
<tr>
<th>NASPInet Traffic Attribute</th>
<th>Real-time streaming data</th>
<th>Historical data</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>CLASS A Feedback Control</td>
<td>CLASS B Feed-forward Control</td>
</tr>
<tr>
<td>Low Latency</td>
<td>4</td>
<td>3</td>
</tr>
<tr>
<td>Availability</td>
<td>4</td>
<td>2</td>
</tr>
<tr>
<td>Accuracy</td>
<td>4</td>
<td>2</td>
</tr>
<tr>
<td>Time Alignment</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>High message rate</td>
<td>4</td>
<td>2</td>
</tr>
<tr>
<td>Path Redundancy</td>
<td>4</td>
<td>4</td>
</tr>
</tbody>
</table>

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

• **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

• **Confidentiality**
  – Needed to provide data privacy
  – *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

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

• NASPI - North American SynchroPhasor Initiative
  – 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

• SynchroPhasors
  – precise, time-synchronized measurements, >30 samples/second
  – provided by monitors called Phasor Measurement Units (PMUs)
  – MRI quality visibility of power system compared to x-ray quality visibility of SCADA
  – synchrophasors from different utilities can be combined together to provide a precise and comprehensive view of the entire interconnection
QoS Management

• QoS goals
  – data flow - are to minimize latency, jitter, loss, errors
  – overall - are avoiding and managing network congestion, shaping network traffic and managing priorities

• Between 2 PGWs in the same Hub network
  – need managed real-time links between PGW and Hub
    • leased lines may be able to provide QoS guarantees

• Between 2 PGWs in different Hub networks
  – need managed-real-time link between the two Hubs
    • managed real-time network between Hubs
      – easier to implement and manage
      » fewer hubs (~20)
• Distributed Storage Opportunity
  – Hubs can act as caches for data
    • improves availability and reliability
    • leverages COTS components
    • e.g., OpenPDC leverages Hadoop DFS (runs on COTS)

• Distributed Computing
  – leverages idle computing power at hubs
  – leverages in-network processing to minimize network transit
    • wide-area bandwidth is usually more expensive than computational power
    • e.g., distributed state estimation
• Wide-Area Monitoring and Visualization
  – visibility over a wide area
  – visibility of real-time dynamics
    • e.g., Phasor RTDMS
  – wide-area situational awareness (WASA) identified as priority – FERC, NIST

• Real-Time Operations
  – automatic control of SVC devices at Southern California Edison
  – island detection, maintenance and restoration at Entergy during hurricane Gustav
  – integration into State Estimation
SynchroPhasor Applications

- **Power System Planning**
  - calibrating and improving models
  - safe operating zones

- **Post Disturbance Analysis**
  - proved very useful in 2008 Florida event

- **Event Detection**
  - line outage detection
SynchroPhasor Applications

• Have varying latency and bandwidth requirements
  – E.g., Real-Time Operations – low latency is critical (< 100ms), no gaps in data
  – E.g., Monitoring and Visualization – relatively higher latencies (~seconds) are tolerable, small gaps in data tolerable
  – E.g., Post Disturbance Analysis – lax latency requirements (~ hour), no gaps in data
• **Network Admission Control**
  – administered by individual Hubs in their local networks
  – administered by service provider or collectively by Hubs on the managed real-time Hub network

• **Key and Trust Management**
  – mediated by Hub on their local networks
  – mediated by pair of Hubs between PGWs in different Hub networks
  – negotiated pair-wise between Hubs
    • can also be mediated by a trusted entity like NERC

• **Intrusion Detection, Response and Recovery**
  – service providers in respective networks