Application-driven Design for Secure and Timely Electric Grid Systems

Himanshu Khurana

Information Trust Institute, University of Illinois at Urbana-Champaign

DIMACS Smart Grid Workshop. October 26, 2010.

TCIPG

tcipg.org

TCIPG: Trustworthy Cyber Infrastructure for Power Grid

- **Objective: Develop technologies that collectively provide resilience in the power grid cyber infrastructure**
- **Five-year effort: 2009 – 2014 ($18.8m); build on TCIP (2005 – 2010; $7.5m)**
- **Multi-University Research Team**
  - *UIUC, Dartmouth, WSU and UC-Davis*
  - *25 faculty and scientist, 30 students, 10 developers and engineers*
  - *Expertise in power systems, cyber security, communication systems, computing technologies*
- **Public-private Partnership**
  - *Extensive industry partnerships include operators, utilities, vendors and providers*
  - *DoE National Labs and the National SCADA Test Bed Program*
- **Research focus: Resilient and Secure Grid Systems**
  - *Secure and real-time communication substrate*
  - *Automated attack response systems*
  - *Risk and security assessment*
  - *Experimental Evaluation using an extensive testbed*

University of Illinois • Dartmouth College • University of California - Davis • Washington State University

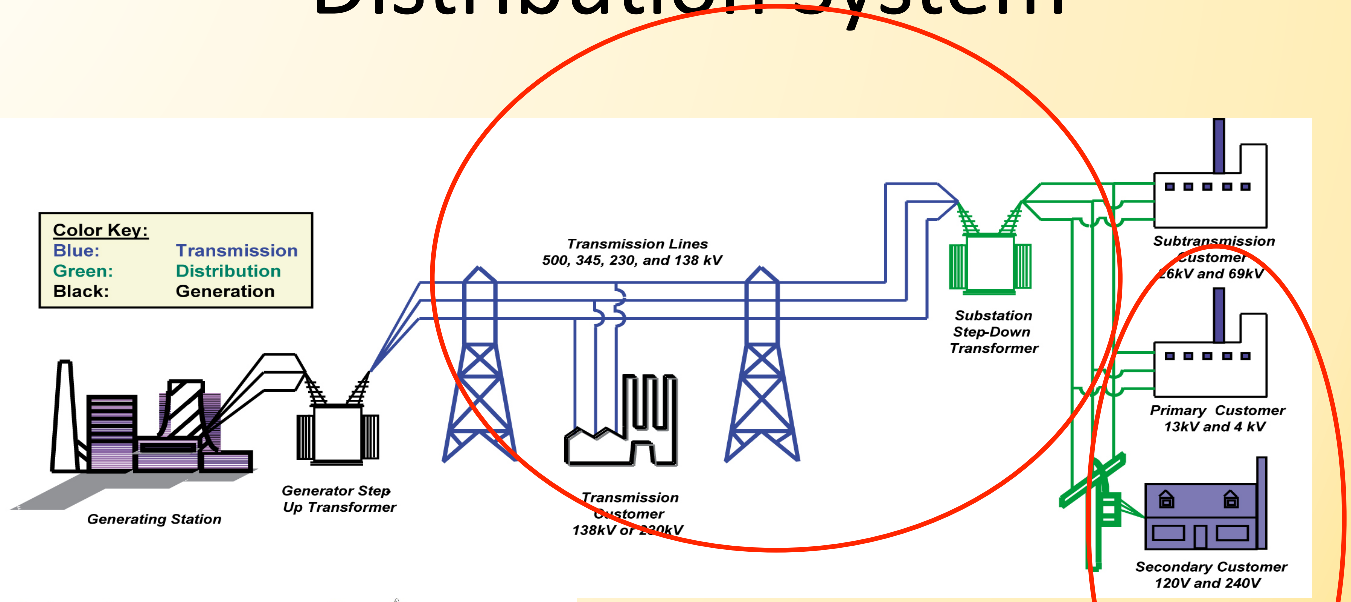
U.S. DEPARTMENT OF HOMELAND SECURITY

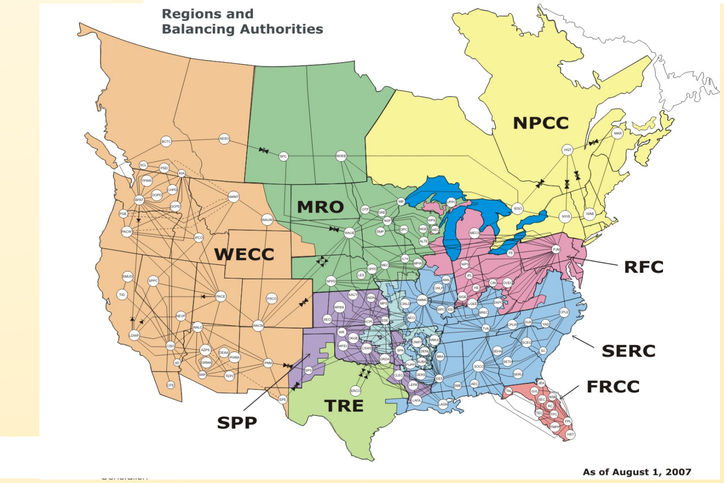
Information Trust INSTITUTE

TCIPG

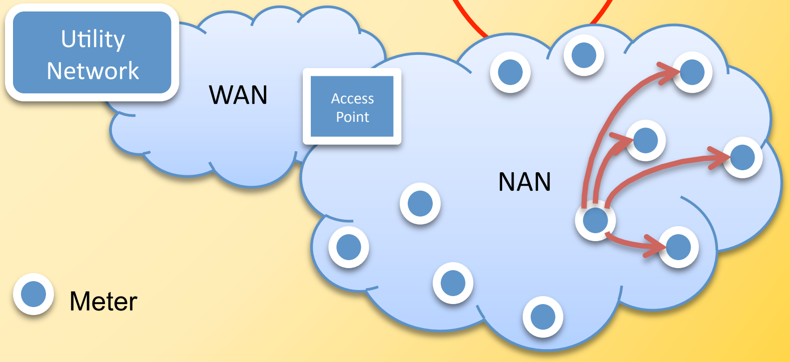
tcipg.org

Research Focus: Transmission and Distribution System





Balancing Authorities/Control Centers



Risks Due to Cyber Attacks and Failures:

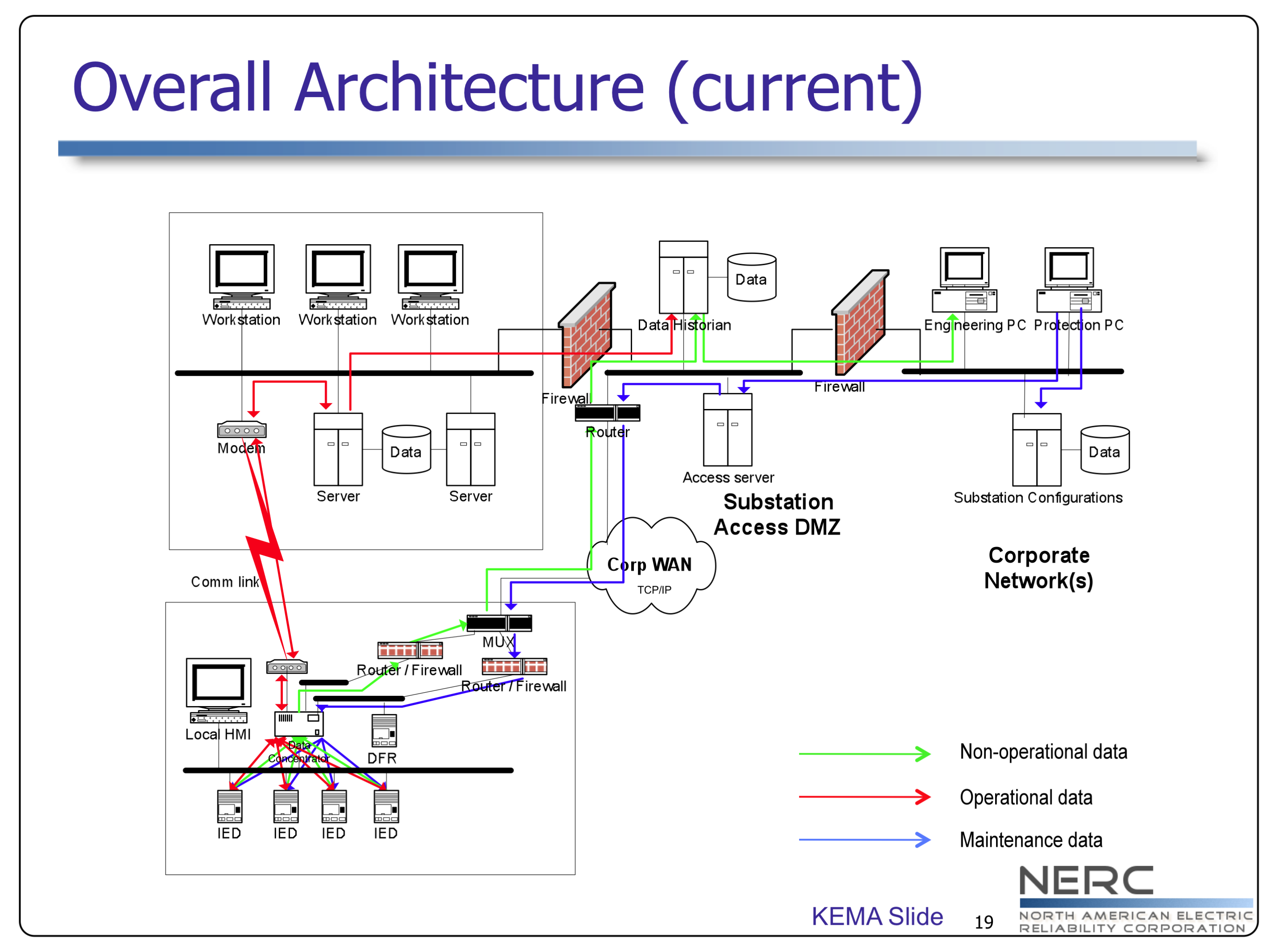
- **Consequences**
  - **Blackouts**
    - Significant economic disruption
    - Safety of the population
    - Secondary effects in other CIs
  - **Market disruption – artificial congestion**
  - **Equipment damage**
    - Transmission transformer - cost in millions, lead time in years
    - Potential long-term blackouts
  - **Extortion**
  - **Privacy violations**
  - **Combined physical and cyber attacks**

- **Adversaries**
  - **Casual hacker**
    - Surprisingly capable antagonists
    - Knowledgeable community
  - **Criminal extortionist**
    - Looking for return on investment
    - Willing to spend a lot of financial return is large enough
  - **National government/organized terrorism**
    - Consequences sought may be non-financial
    - Large resources
  - **Insiders (possibly used by attackers in other categories)**

Research Overview of Select Projects

- Challenges
  - Real-time critical operational environment
  - Bandwidth and connectivity constraints
  - Legacy protocols and systems
  - Emerging applications and systems
- Problems addressed
  - Authentication for SCADA protocol
  - Real-time middleware for SCADA systems
  - Tiered Architecture for Wide Area Measurement Systems
- Approach
  - Application-driven design
  - Eventually "science" of cyber security for power grid will emerge

SCADA Architecture



Overall Architecture (current)

Non-operational data

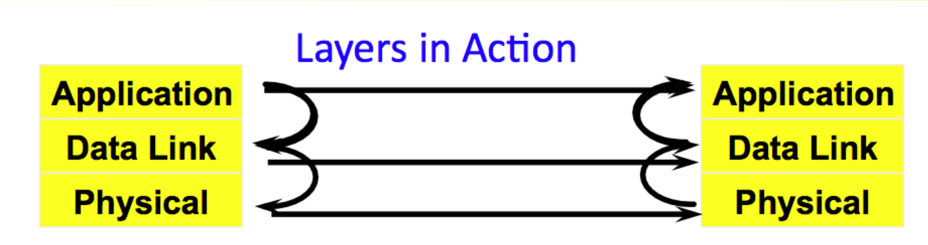
Operational data

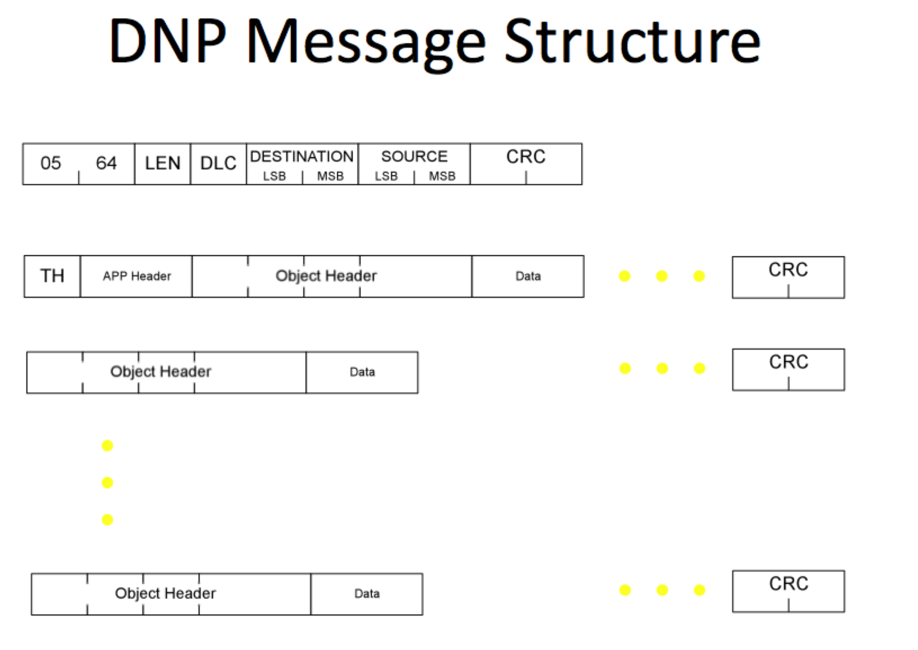
Maintenance data

KEMA Slide 19

SCADA Protocols

- **DNP Overview**
  - Transmits & receives
    - analog and digital values
  - Multi Master
  - Tens-of-millisecond update rate
  - Serial and Ethernet
  - *Extensively used in the Grid toda*



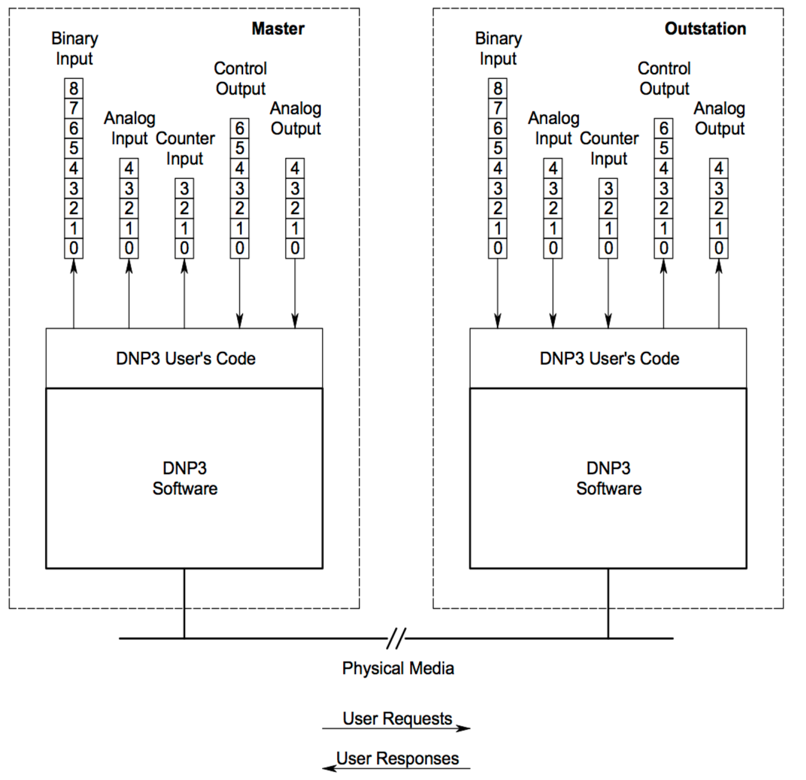


From a presentation by D. Whitehead, "Communication and Control in Power Systems", tcip summer school, June, 2008

Authentication for SCADA Protocols

- **Problem**
  - Message authentication for SCADA
- **Challenges**
  - Bandwidth and computation constraints
  - Legacy integration (with DNP3)
- **Approach**
  - Evaluate industry proposal for DNP3 Secure Authentication Supplement (*funded by EPRI*)
  - Develop principles and improved protocol

- **DNP3 Architecture**



- **DNP3 Secure Authentication**
  - Based on ISO/IEC 9798 Standards (using HMAC)

Security Evaluation

- **Results**
  - Analysis of industry proposal:
    - *Bandwidth* reduction via HMAC truncation
    - *Legacy* integration via challenge-response
  - Issues with industry proposal
    - Recommend 32-bit truncated output &
    - Use both nonces and sequence numbers
      - Efficiency neither optimal nor correct
    - Insufficient resistance in design
      - Protocol-based DoS vulnerability
  - Our feedback
    - Proposed alternative HMAC truncation strategy
    - Proposed approach for DoS resistant design

- **Industry Interactions**
  - Participation in DNP Technical Committee
  - Feedback is being included in the standard
  - Participation in IEEE PSCC for IEC 62351-5 standard

Research Problem #1:Secure Protocol Design for the Power Grid

- **Cyber infrastructure is key to realization of a Smart Grid**
  - Introduces an additional threat element: cyber attacks

- **Cyber security protocols and their standardization are needed to protect against emerging cyber attacks**; e.g.,
  - Authentication protocols protect against attacks such as masquerading, spoofing, replay, etc.
  - Encryption protocols protect against eavesdropping attacks
  - Non-repudiation protocols protect against deniability

- **This work focuses on trustworthy designing of protocols for Smart Grids**

- **Publication**
  - Himanshu Khurana, Rakesh Bobba, Tim Yardley, Pooja Agarwal and Erich Heine, “Design Principles for Power Grid Authentication Protocols”, in proceedings of HICSS, January, 2010.

The need for principles

Protocols	Attacks	Cause/Vulnerability
Authentication Protocol by Woo & Lam	Impersonation attacks	Lack of explicit names
STS by Diffie, Oorschot & Wiener	Impersonation attacks	Change in environmental conditions
Kerberos V4 by Steve & Clifford	Replay attacks	Incorrect use of timestamps
TMN by Tatebayashi, Matsuzaki, & Newman	Oracle attacks	Information flow

Selected Design Principles for Security Protocols

Principle	Attacks Mitigated	Applicability to Power Grid Authentication Protocols
Explicit Names	Impersonation attacks.	Need for explicit names for each entity in power grid.
Unique Encoding	Interleaving and parsing ambiguity attacks.	Insufficiency of legacy protocols to build security on them due to no protocol identifiers in them.
Explicit Trust Assumptions	Prevents errors due to unclear or ambiguous trust assumptions	Need to clearly state all trusted entities in power grid protocols and the extent of trust in them.
Use of Timestamps	Prevents replay attacks.	Need for high granularity for time synchronization.
Protocol Boundaries	Prevents incorrect function of protocol in it's environment.	Need for thorough analysis of the power grid environment.
Release of Secrets	Prevents blinding attacks and compromise of old keys.	Need to ensure that compromise of some remote devices should not compromise large number of keys.
Explicit Security Parameters	Prevents errors due to exceeding the limitations of cryptographic primitives.	Reduction in maintenance overhead by explicitly mentioning security parameters in remote devices.

Applying Known Authentication Principles

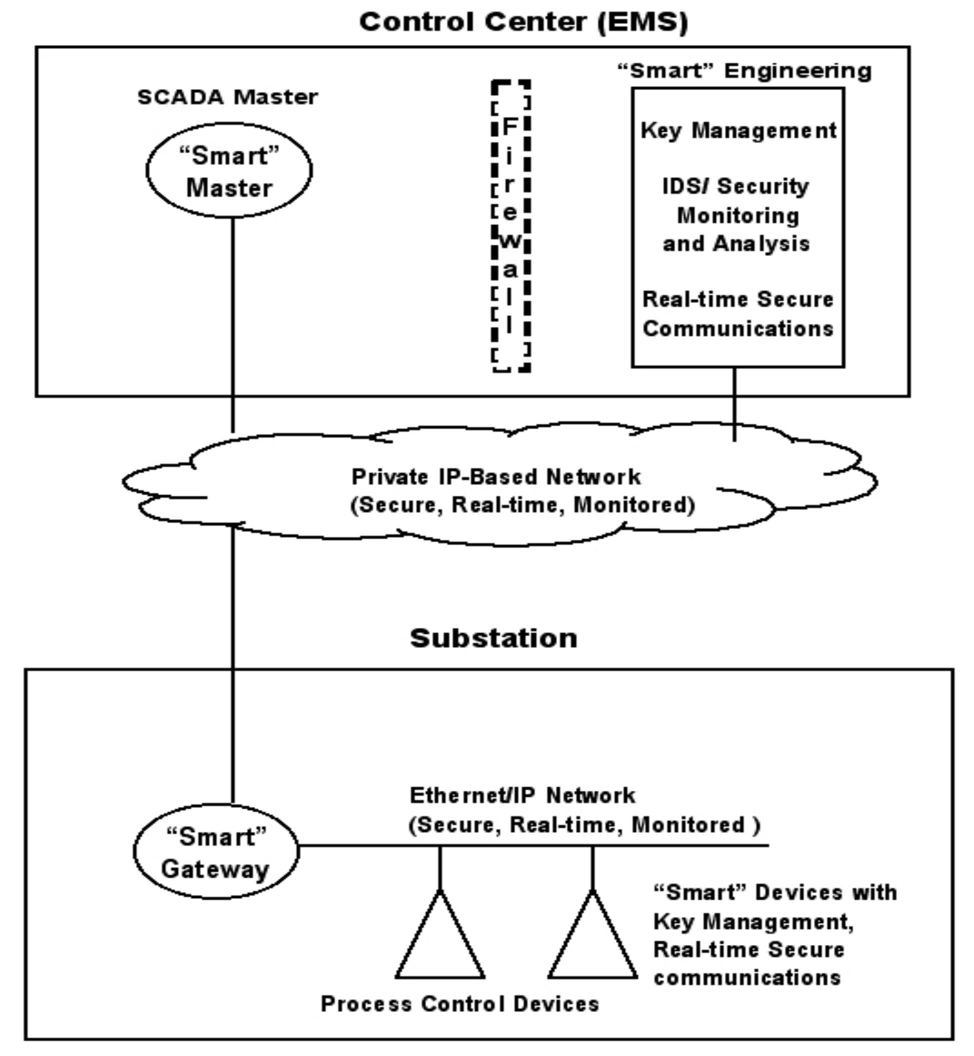
- **Principle of Explicit Trust Assumptions**
  - DNP3 Secure Supplement V2.0 claimed non-repudiation as a property using symmetric keys
    - Assumption: master is fully trusted

- **Principle of Protocol Boundaries**
  - DNP3 Secure Supplement v2.0 allows unauthenticated messages to preempt execution of ongoing operation
    - Limitation: DNP3 designed for serial environments

- **Principle of Explicit Names**
  - DNP3 does not use explicit names
    - Limitations: Globally unique names do not exist
    - Solution: (adopted by DNP3) use unique keys in each direction

Research Problem #2: Real-time Middleware for SCADA Systems

- Objective: Enable network convergence for Control system applications
  - Multiple traffic paradigms
    - SCADA and other control
    - Monitoring
    - Engineering
    - Enterprise
  - Understand and support communications requirements/ properties for existing and emerging applications
- Implications for a range of emerging monitoring and control applications



Joint work with Erich Heine and Tim Yardley

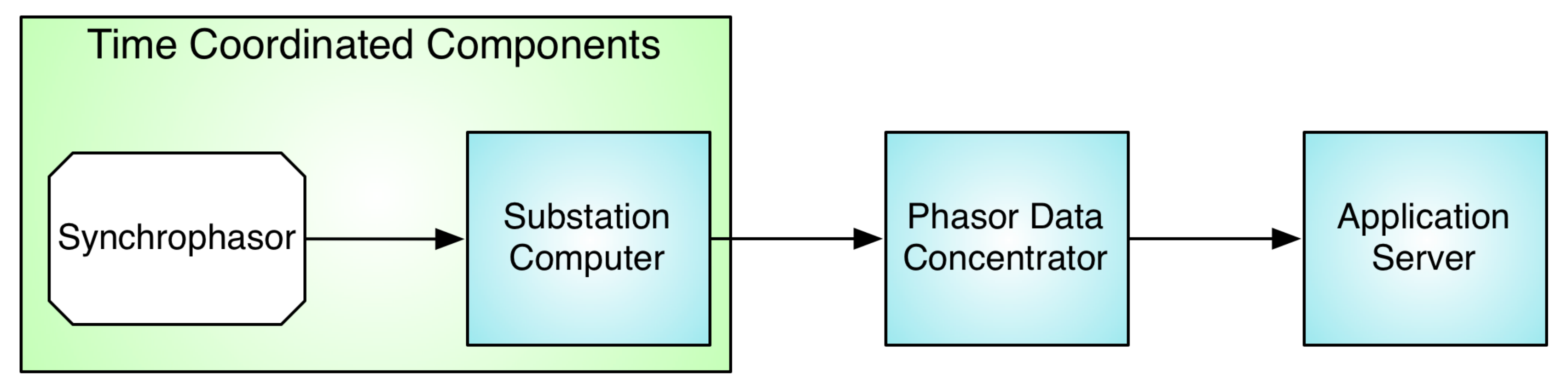
Research Challenges

- Technical Challenges:
  - Resource management
    - Quality of Service, Real-time scheduling, Wide area network optimization
  - Security
    - Access control, Integrity, Availability
- Development and Integration challenges
  - Use commercial, off-the-shelf platforms and tools
  - Minimal use of custom software
  - Support legacy devices and applications
  - Support existing and emerging applications

Application Characterization with Industry Input

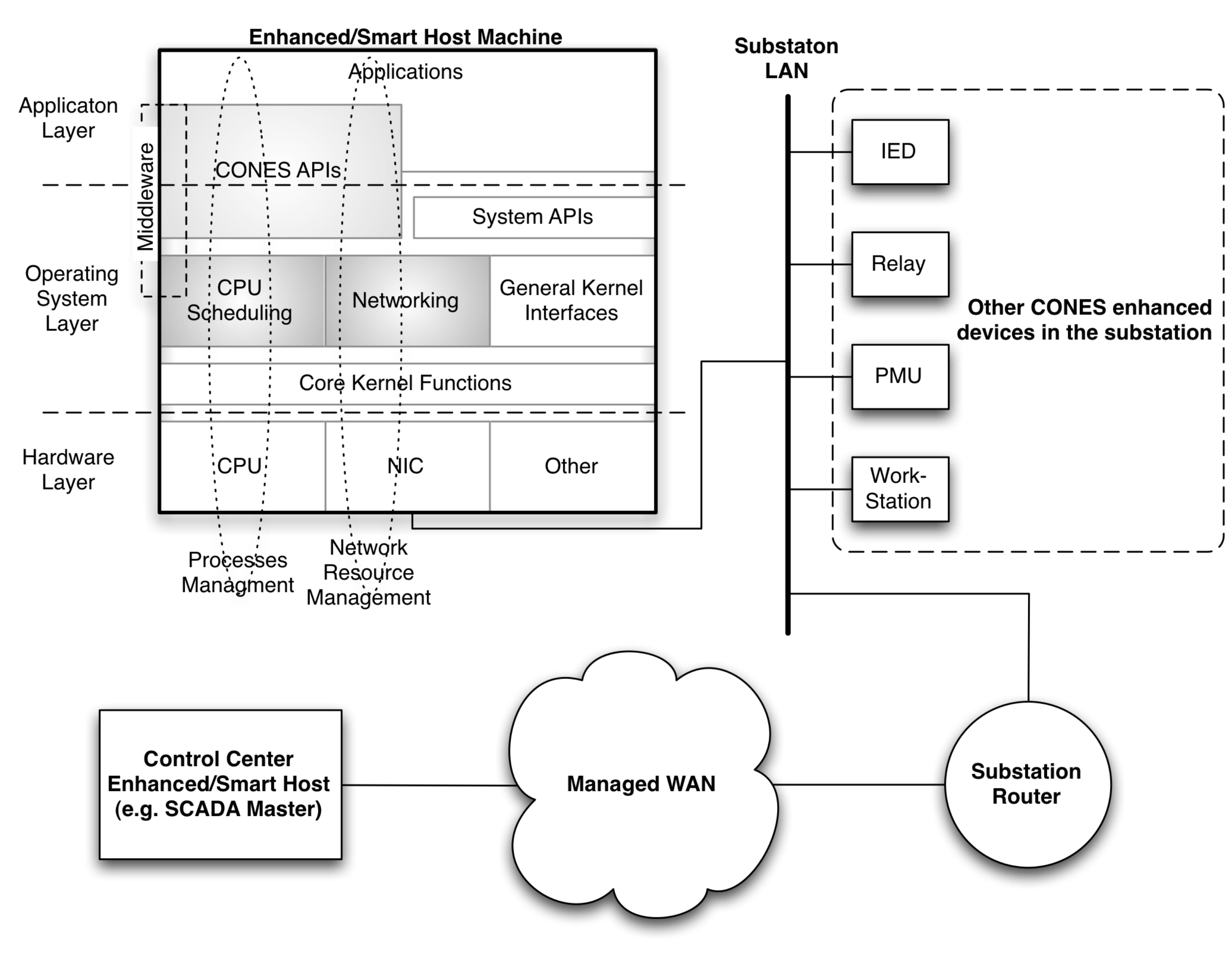
Power Systems Application	Traffic Type	Traffic Path	Qualitative Quality of Service (QoS) Parameters	Packet Characteristics (size, timing) per device	Scalability considerations	Stream Bandwidth Characteristics (per device, total)
Protection/ Control	SCADA	IED(substation) -> Control Center	Low latency, high priority, no loss	Size: 256B – 1KB Frequency: 1 packet every 2-4s	~5 devices per bus	.5KB/s per device 2.5-5KB/s per bus
	SMV/ GOOSE	IED -> IED	High speed/low latency, high priority.	Size: typically less than 1 Ethernet frame Frequency:	1 event per second per bus	1-15KB per protection event
Monitoring	PMU	IED/PMU -> Phasor Data Concentrator (Control Center)	Low latency, medium priority.	Size: 128 Bytes Frequency: 30 – 120 samples/sec	2 PMUs per bus	30Kbps per device, 60Kbps per bus
	Other Monitoring Data	IED/master -> Control Center	Low latency, medium priority.	Size: 32-64 Bytes Frequency: 1 sample/sec	20-25 Devices/substation	256-512Kbps per device 1-5 Mbps per substation (not all data leaves the substation)
Engineering	Interactive	Control Center <-> Substation	Medium latency, medium priority	N/A (these are not critical timings and can vary greatly)		1M per occasional request
	Data Transfer	Control Center <-> Substation	Low priority	N/A (Big packets, but not a standard size)	A flow 1-2 times per day	1-5M per occasional request
Surveillance	Video	Substation -> Control Center	Medium – High latency, medium priority.	Varied video frame sizes and rates	2-10 cameras per substation.	100 Kb/s -1Mb/s per camera ~5Mbps per substation

Example Scenario



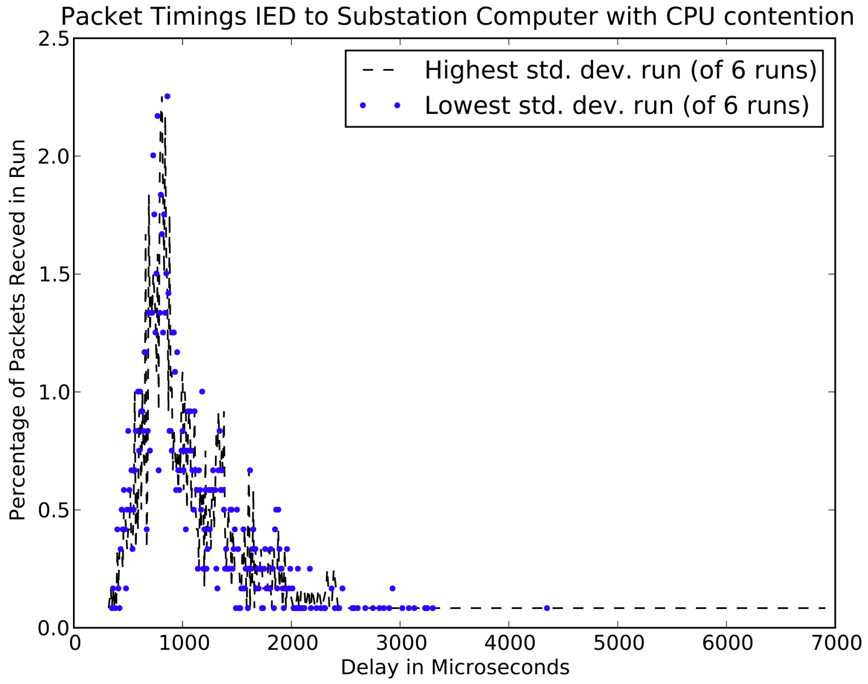
- Special purpose and Common Off The Shelf systems in datapath *(blue boxes)*:
  - End-to-end deadlines (10s of ms for protection applications)

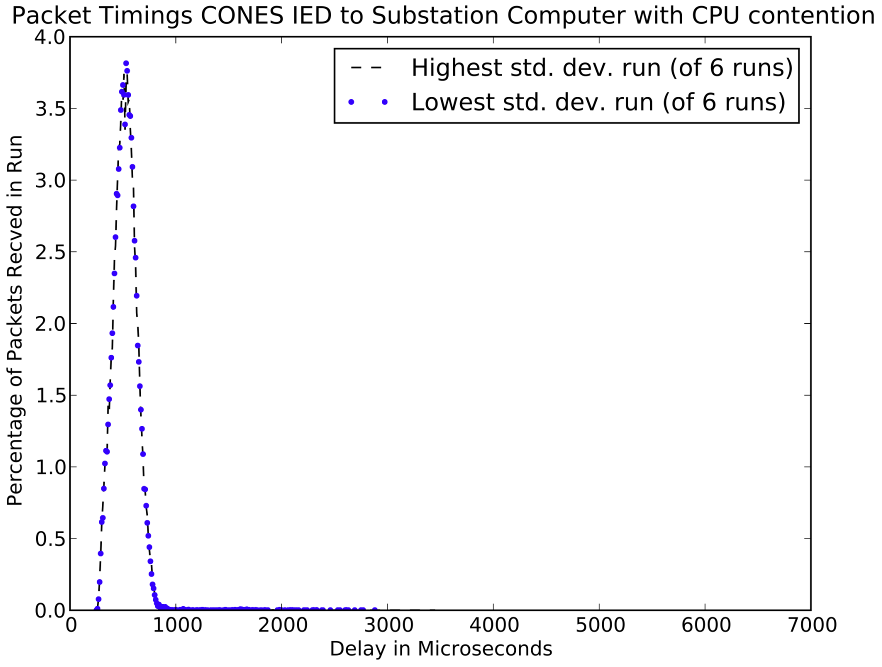
Results: Architecture



TCIPG

Results: Performance

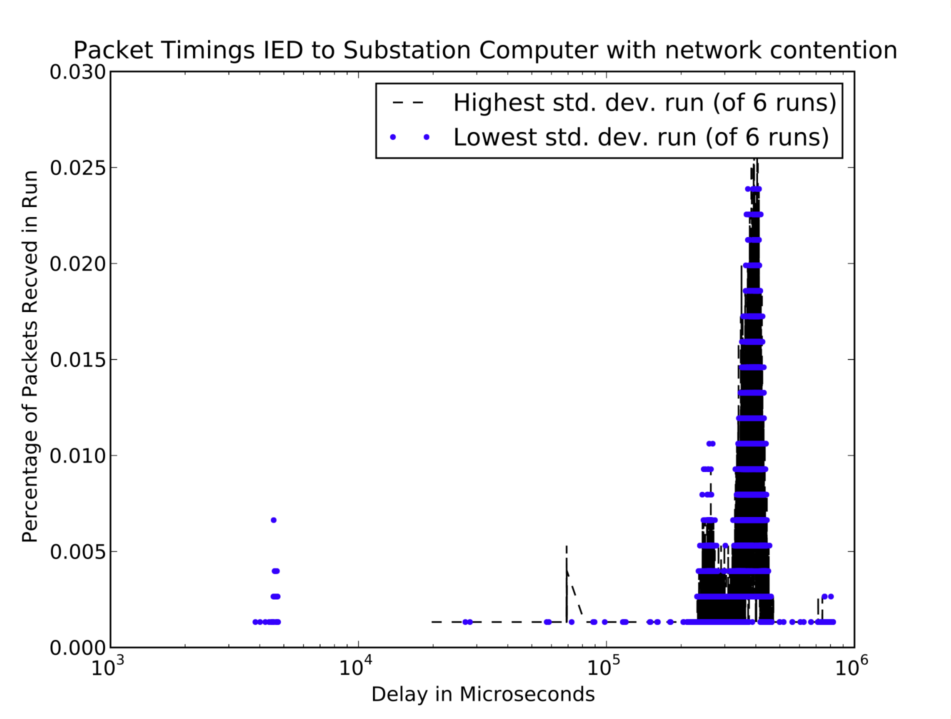


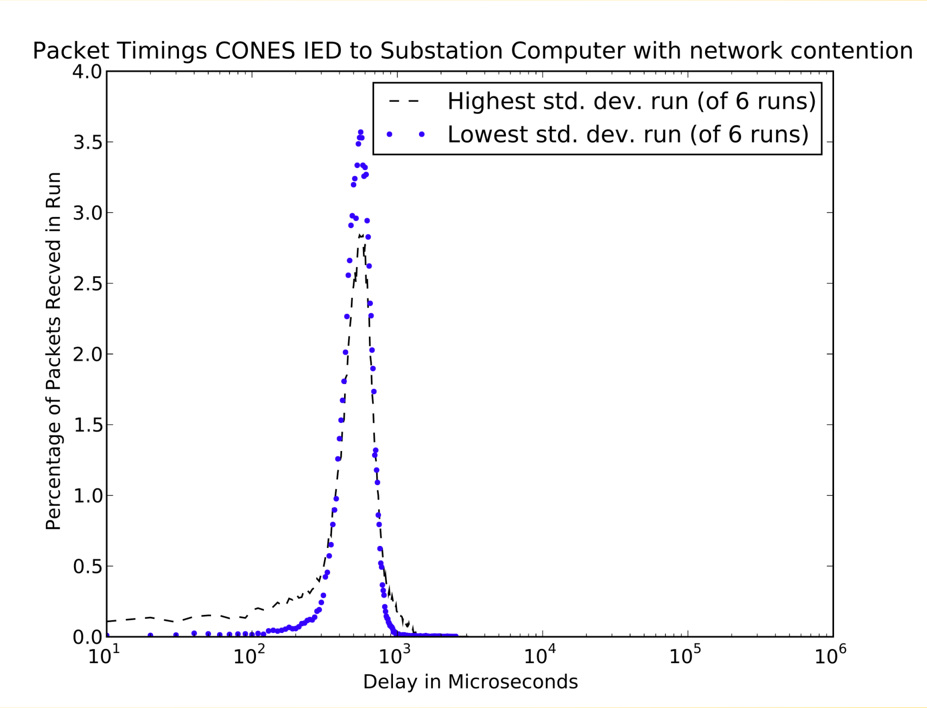


Packet latency timings with CPU contention

Left: unenhanced host Right: CONES enhanced host

Results: Performance



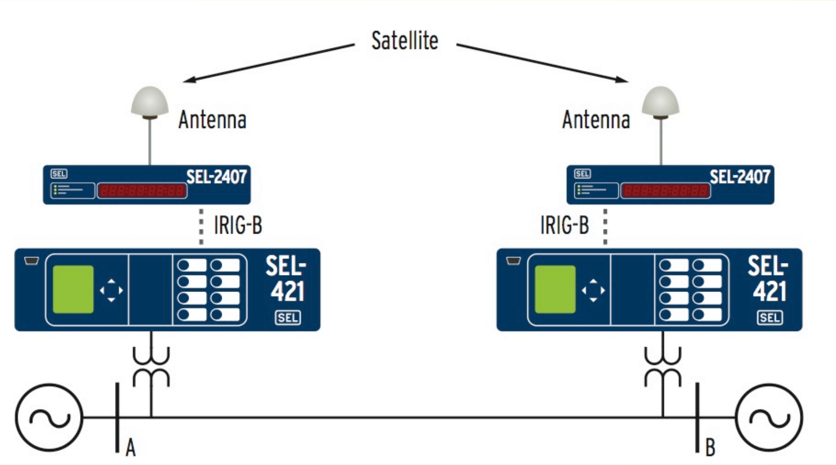


Network latency timings with network interface contention.

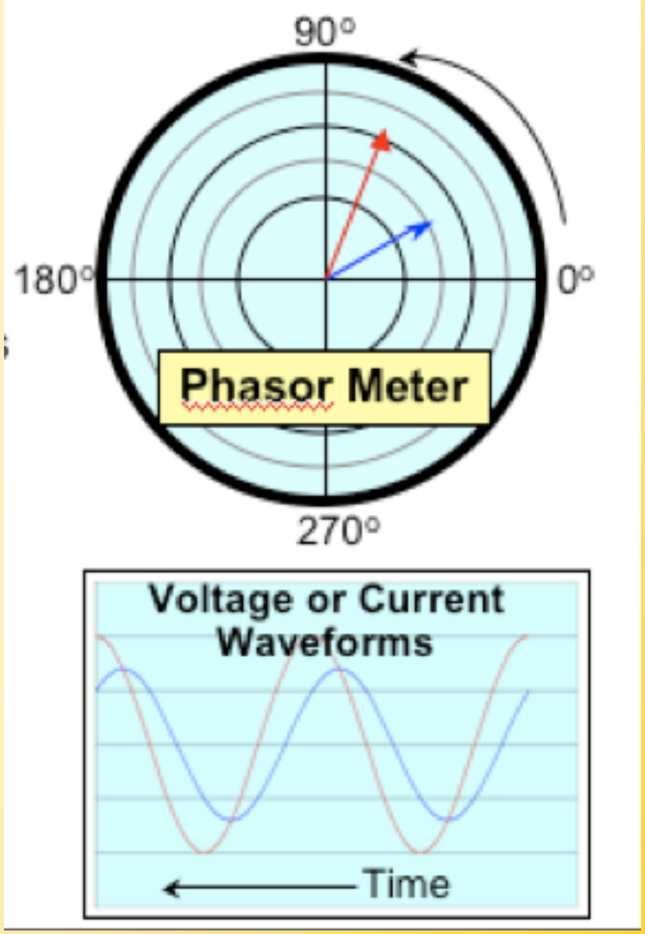
Left: unenhanced host

Right: CONES enhanced host

PMUs and Synchrophasors

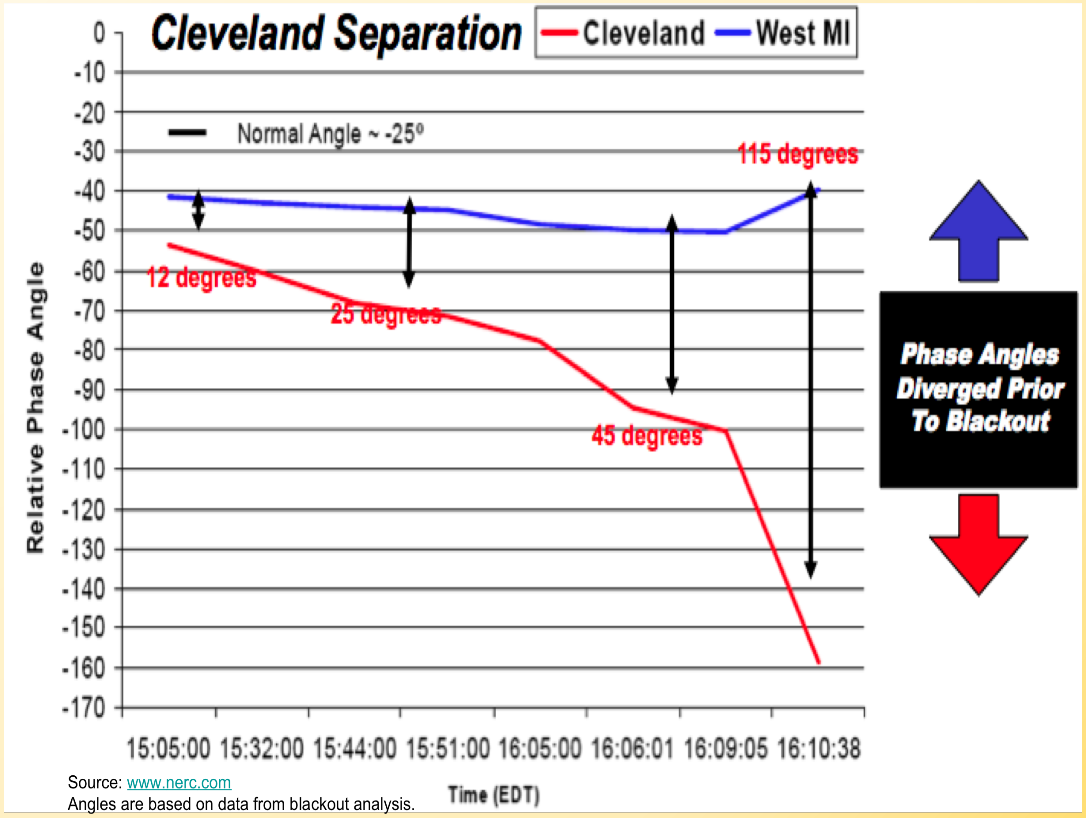


- **Traditional SCADA data since the 1960's**
  - **Voltage & Current Magnitudes**
  - **Frequency**
  - **Every 2-4 seconds**
- **Future data from Phasor Measurement Units (PMU's)**
  - **Voltage & current phase angles**
  - **Rate of change of frequency**
  - **Time synchronized using GPS and 30 -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



Why do Phase Angles Matter?

Wide-area visibility could have helped prevent August 14, 2003 Northeast blackout

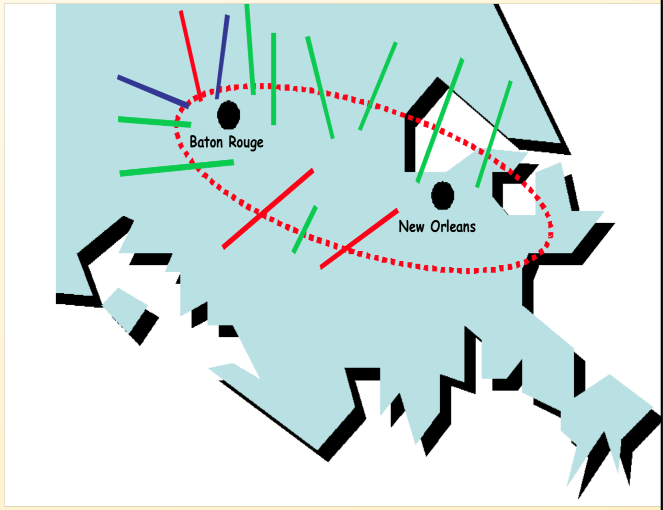


Source: www.nerc.com
Angles are based on data from blackout analysis.
Angle reference is Browns Ferry.

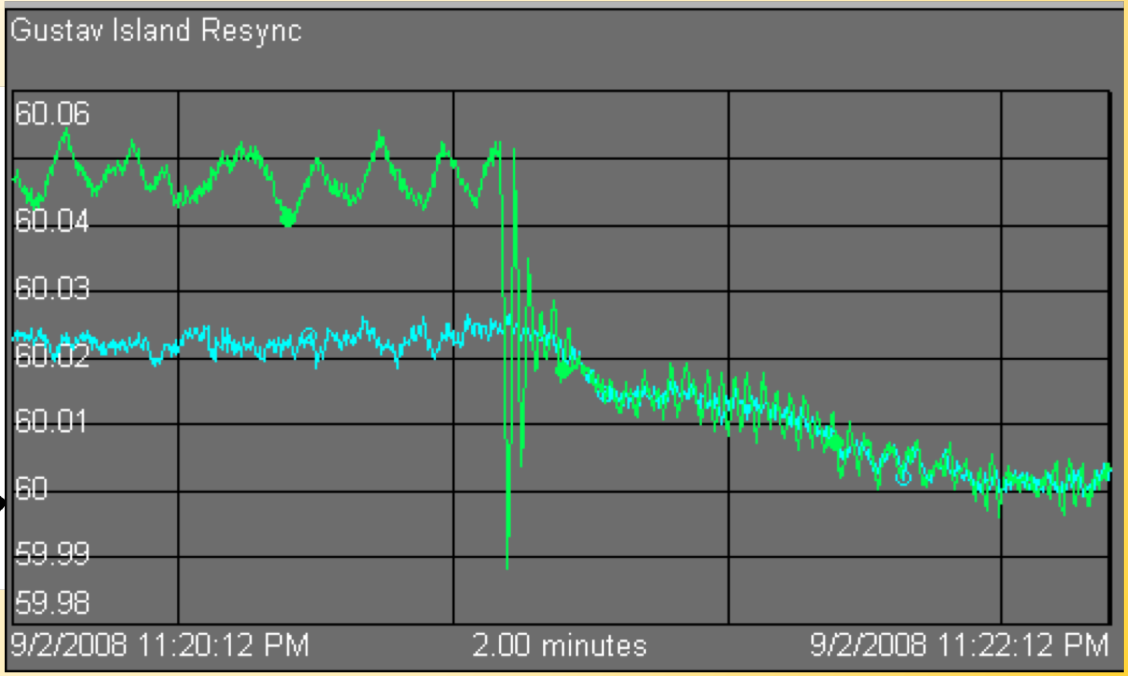
Why do Phase Angles Matter?

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

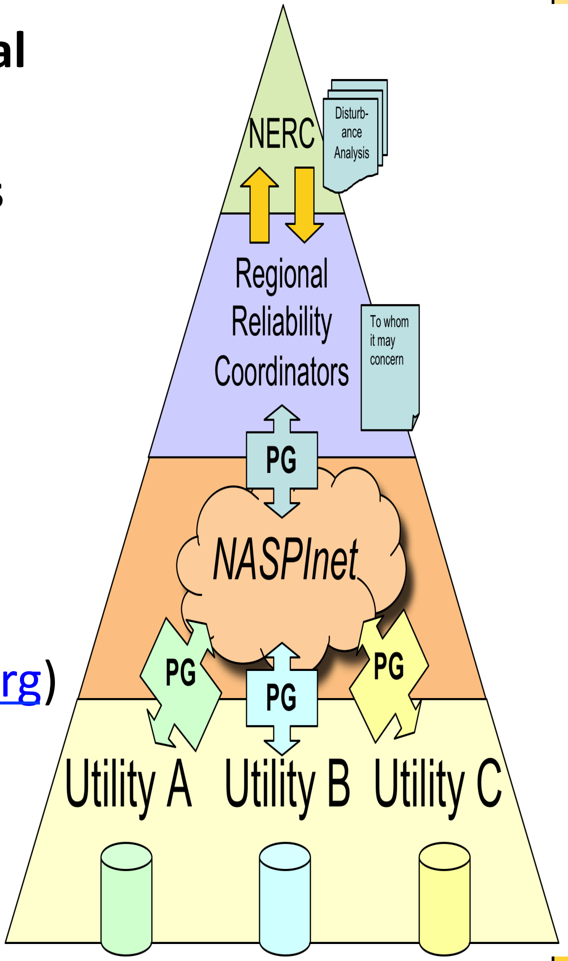


Source: Entergy

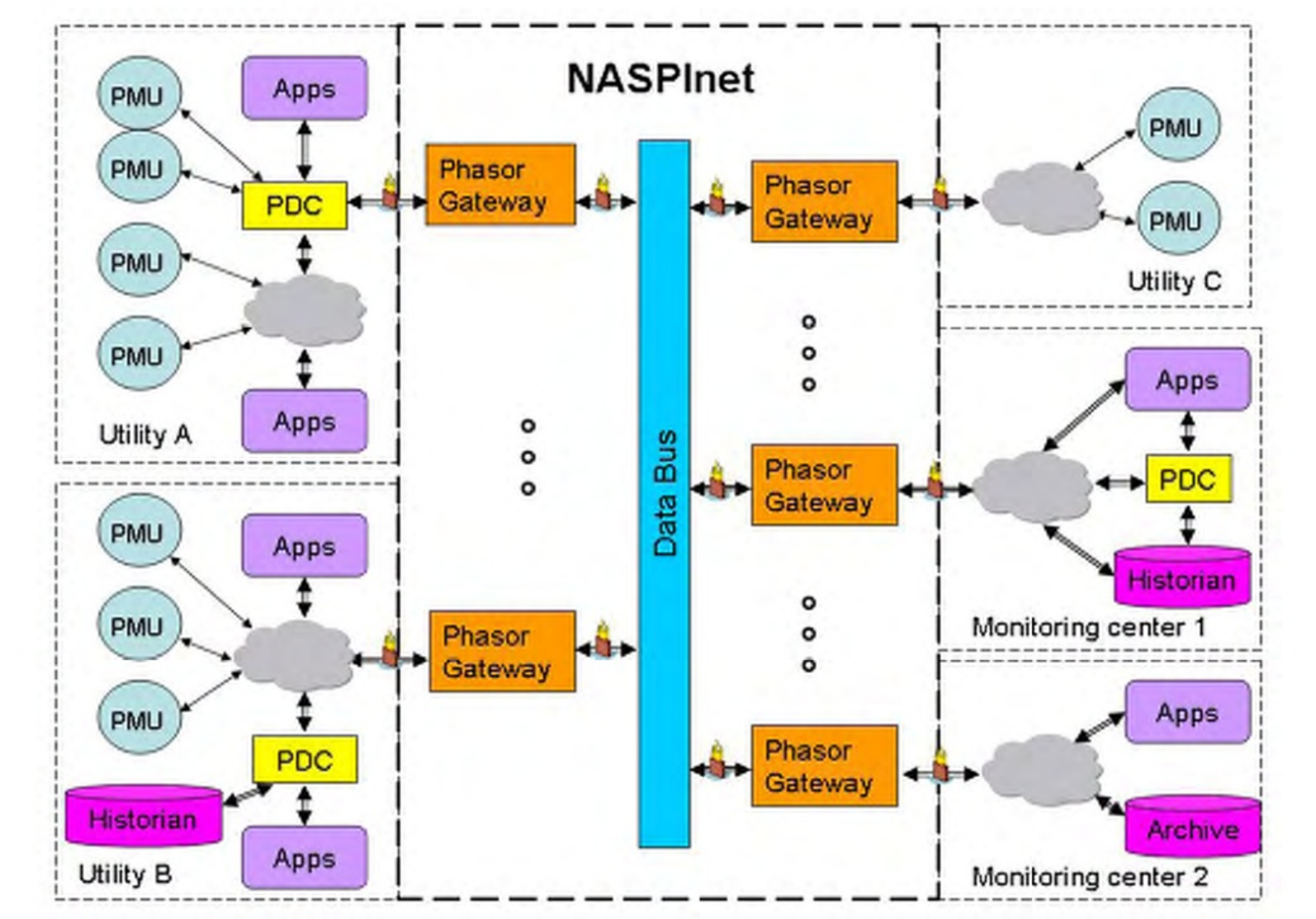


Wide Area Measurement Systems and NASPI

- **Wide Area Measurement System (WAMS) is crucial for the Grid**
- **Promising data source for WAMS: Synchrophasors**
  - GPS clock synchronized
  - Phasor Measurement Unit (PMU)
  - Fast data rate ~ 30 samples/second
- **Future applications will rely on large number of PMUs envisioned across Grid (>100k)**
- **WAMS Design and Deployment underway: North American Synchrophasor Initiative** - (www.naspi.org)
  - *Collaboration* - DOE, NERC, Utilities, Vendors, Consultants and Researchers
  - *NASPInet* – distributed, wide-area network



Conceptual NASPInet Architecture



Source: NASPInet Specification

Research Problem #3: Towards a Distributed PMU Data Network

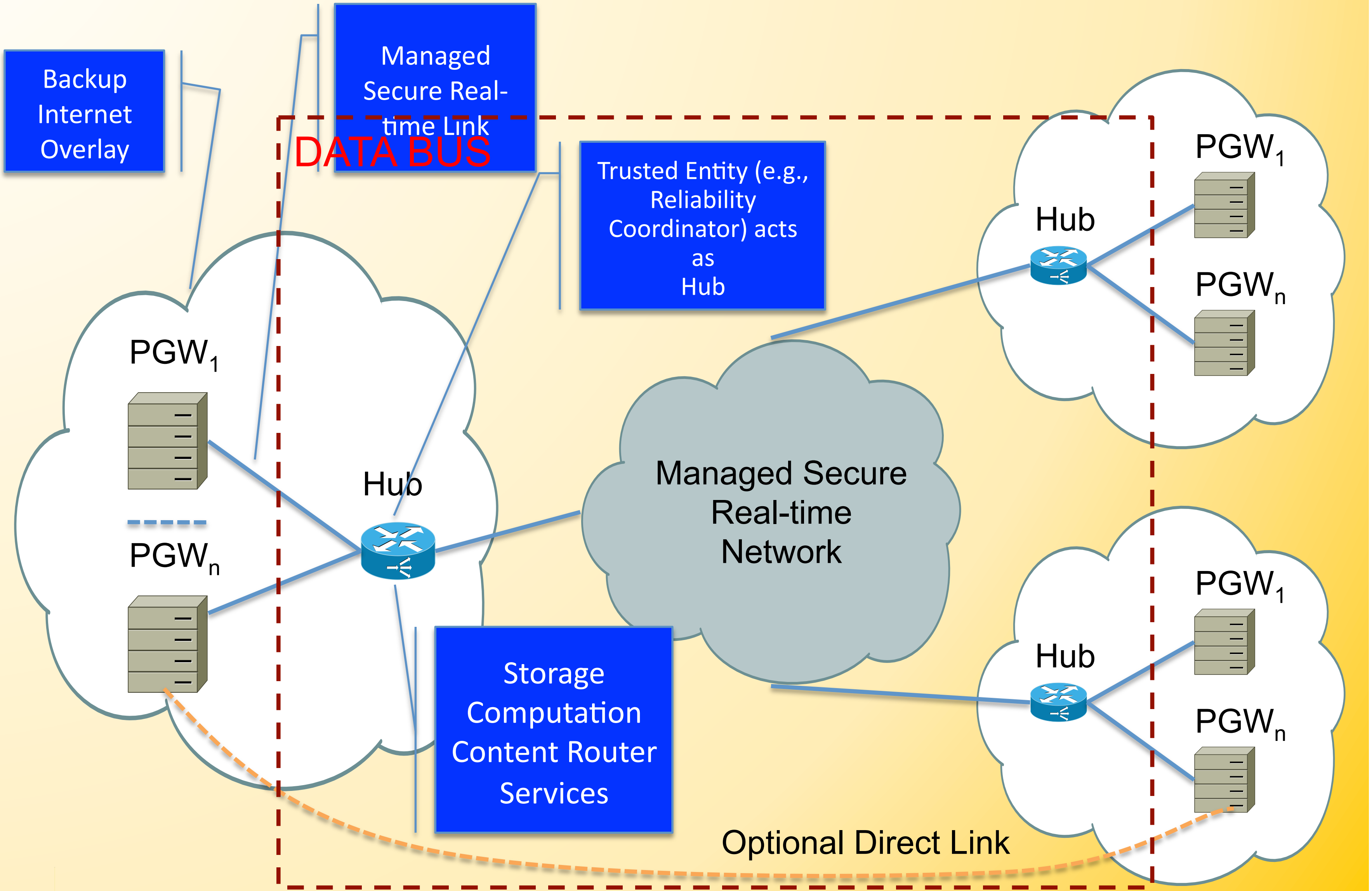
- Technical Challenges for NASPInet
  - large distributed network - continental scale
  - quality of service (QoS) - prioritization of traffic, latency management etc
  - securing PMU data – integrity, availability and confidentiality, key and trust management, network admission control, intrusion detection, response, recovery
  - network management – performance, configuration, accounting, fault management, security management
- Business/Organizational challenges for NASPInet
  - who owns/manages/provides the network
  - high initial costs

- Rakesh Bobba, Erich Heine, Himanshu Khurana and Tim Yardley. Exploring a Tiered Architecture for NASPInet. In Proceedings of the IEEE Innovative Smart Grid Technologies Conference, Gaithersberg, MD, January 2010.

Exploring a Tiered Architecture

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

Proposed Tiered Architecture



Backup Internet Overlay

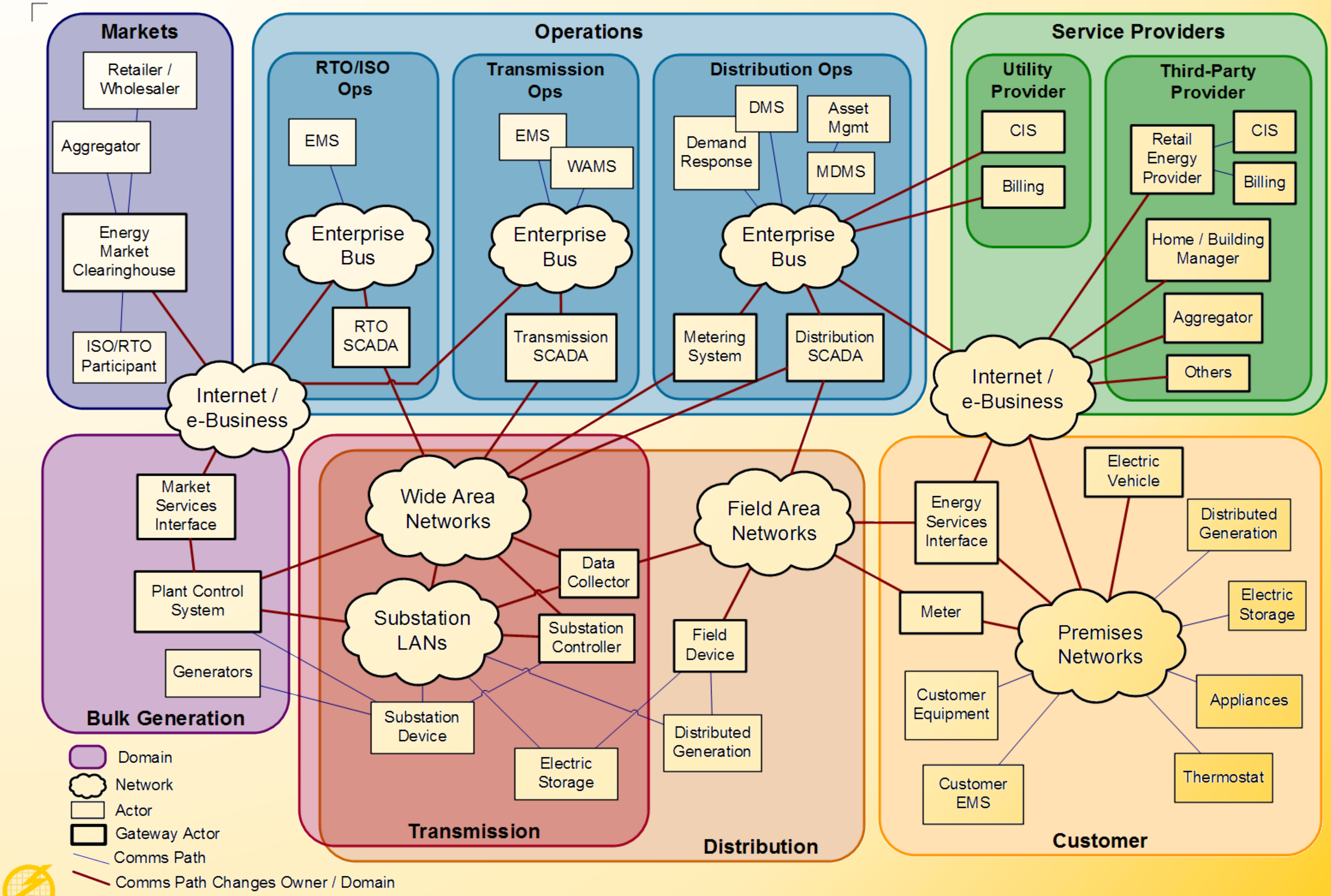
Managed Secure Real-time Link

Trusted Entity (e.g., Reliability Coordinator) acts as Hub

Managed Secure Real-time Network

Storage Computation Content Router Services

Smart Grid Architecture (Source: NIST)

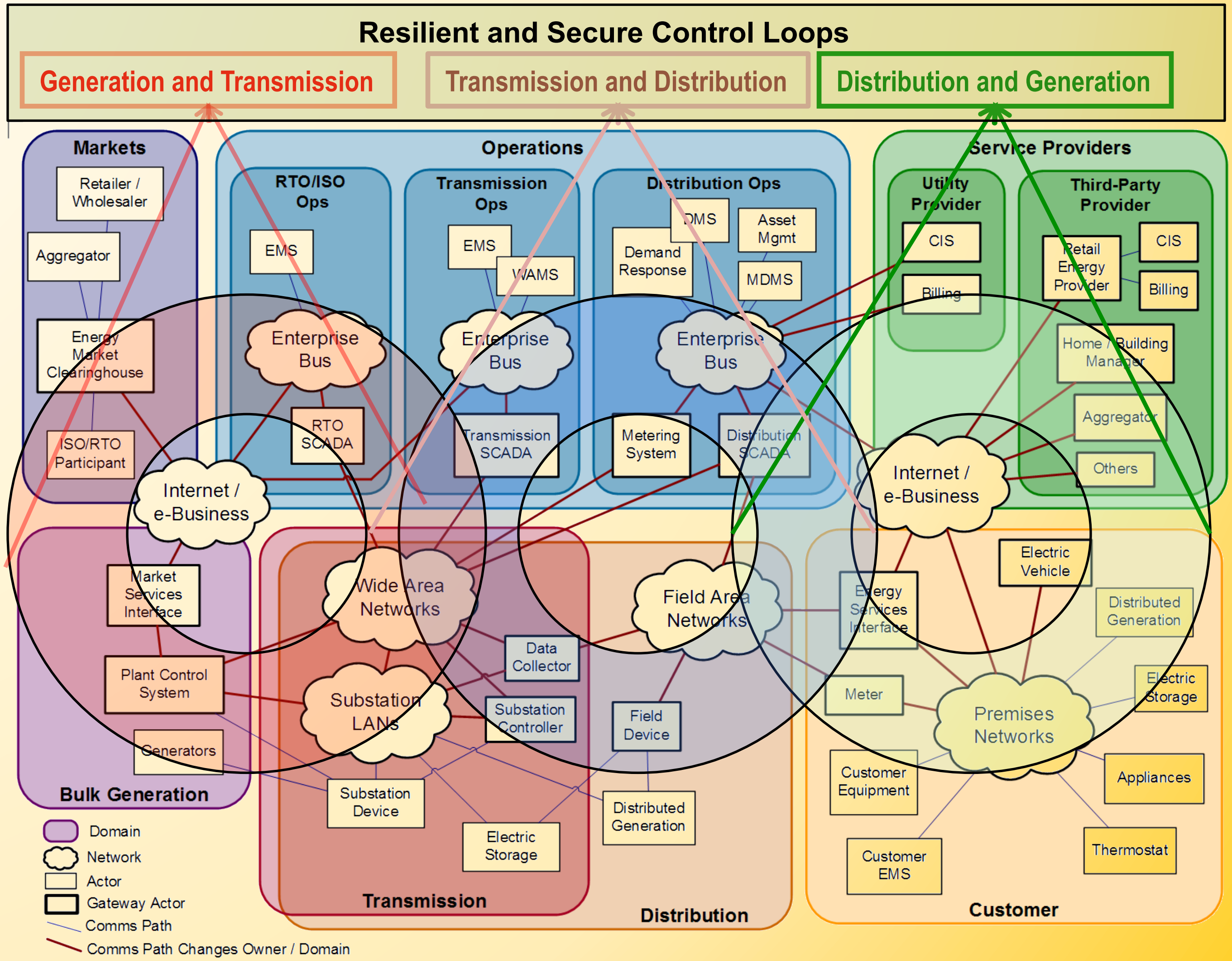


TCIPG

tcipg.org

Next Generation Smart Grid “Secure” Controls

- ✧**Multi-layer Control Loops**
  - ✧*Multi-domain Control Loops*
    - ✧ Demand Response
    - ✧ Wide-area Real-time control
    - ✧ Distributed Electric Storage
    - ✧ Distributed Generation
  - ✧ *Intra-domain Control Loops*
    - ✧ Home controls for smart heating, cooling, appliances
    - ✧ Home controls for distributed generation
    - ✧ Utility distribution Automation
- ✧ **Resilient and Secure Control**
  - ✧ *Secure and real-time communication substrate*
    - ✧ Integrity, authentication, confidentiality
    - ✧ Trust and key management
    - ✧ End-to-end Quality of Service
  - ✧ *Automated attack response systems*
  - ✧ *Risk and security assessment*
    - ✧ Model-based, quantitative validation tools



Note: the underlying Smart Grid Architecture has been developed by EPRI/NIST.

TCIPG

tcipg.org

Thank you.
Questions?

Contact Information:
hkhurana@illinois.edu