Smarter Power Grids: Challenges and Research Directions

Presented by:

Bill Sanders

Thanks to the TCIPG Team for supporting material

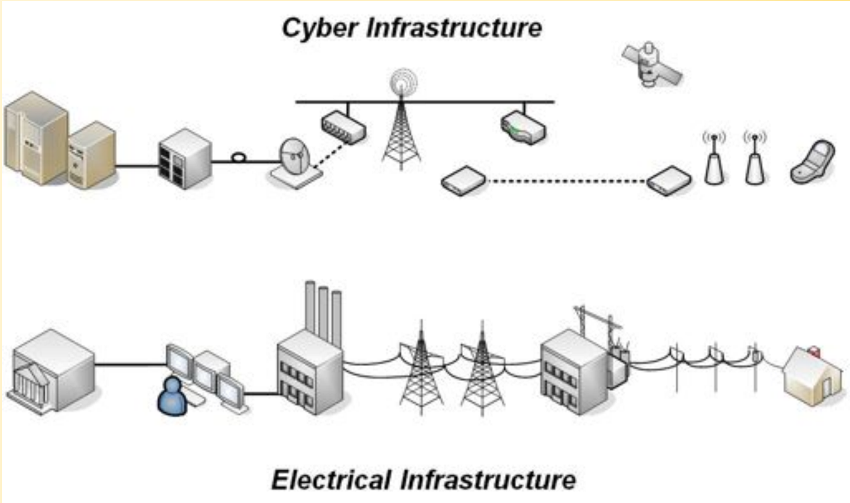
January 13, 2011

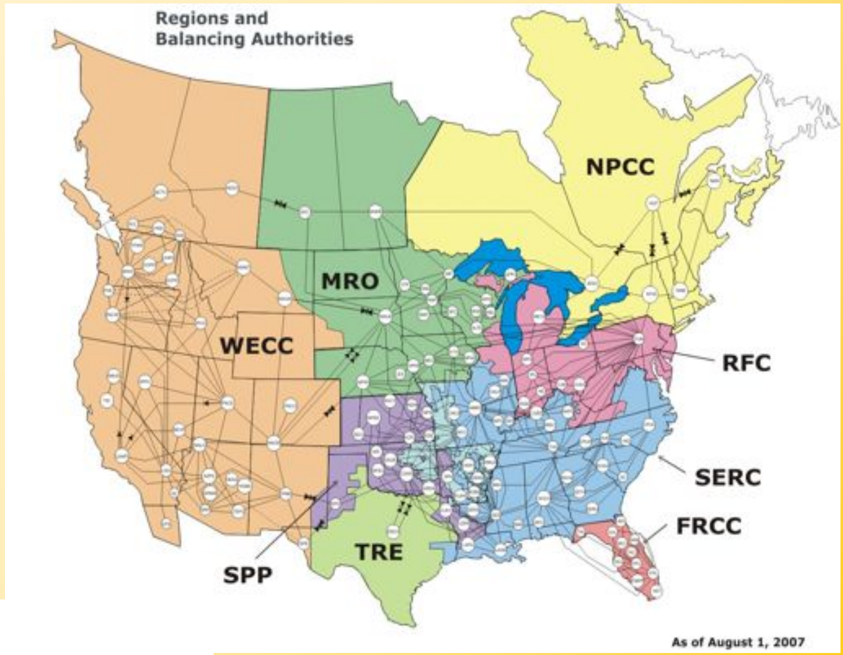
IFIP 10.4 Workshop on Dependability Issues for a Smarter Planet

The Challenge: Providing Trustworthy Power Grid Operation in Possibly Hostile Environments

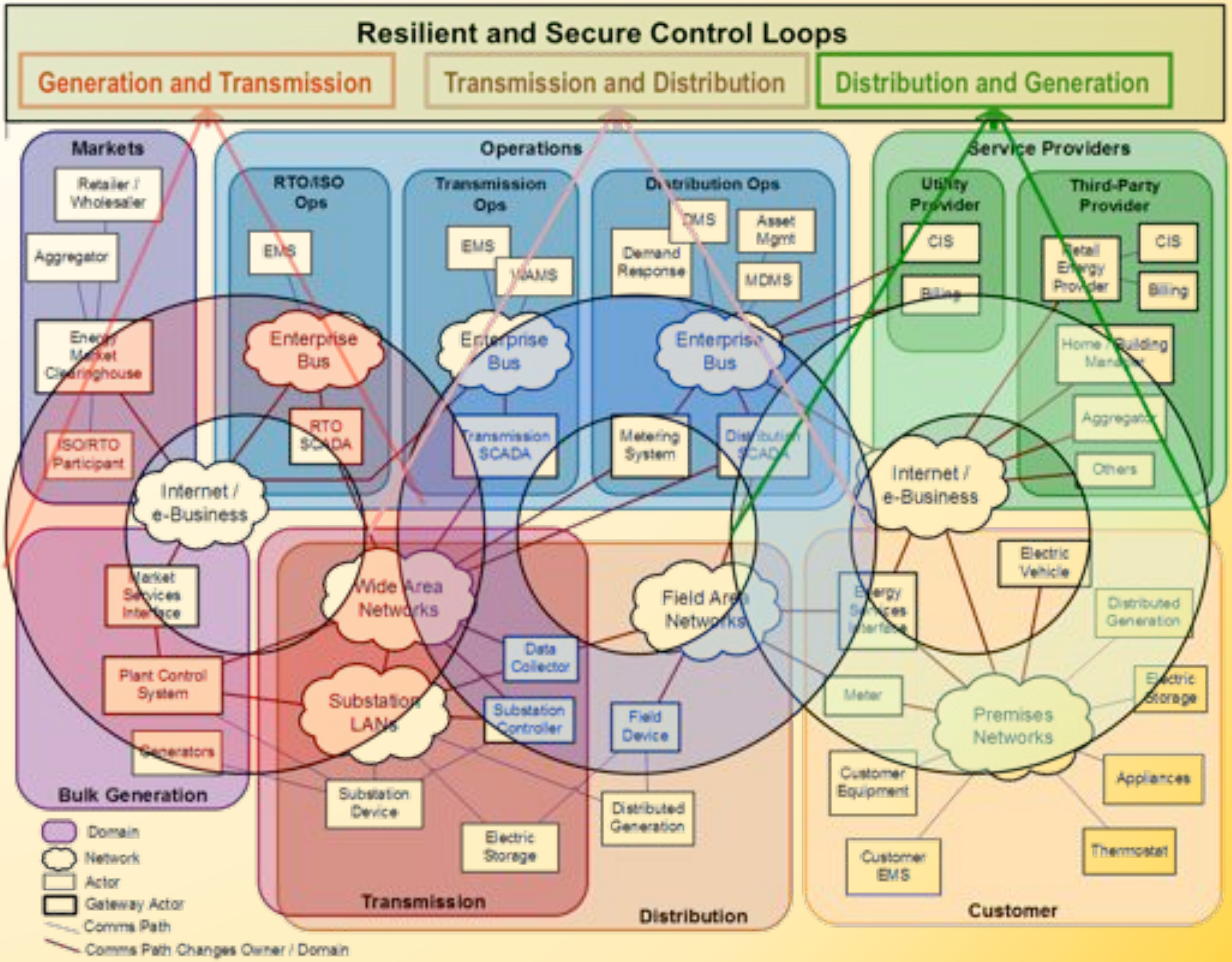
- Trustworthy
  - A system which does what is supposed to do, and nothing else
  - Safety, Availability, Security, …
- Hostile Environment
  - Accidental Failures
  - Design Flaws
  - Malicious Attacks
- Cyber Physical
  - Must make the whole system trustworthy, including both physical & cyber components, and their interaction

Power Grid Infrastructures:
The World’s Largest Cyber Physical Systems





Infrastructure must provide control at multiple levels



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

tcipg.org

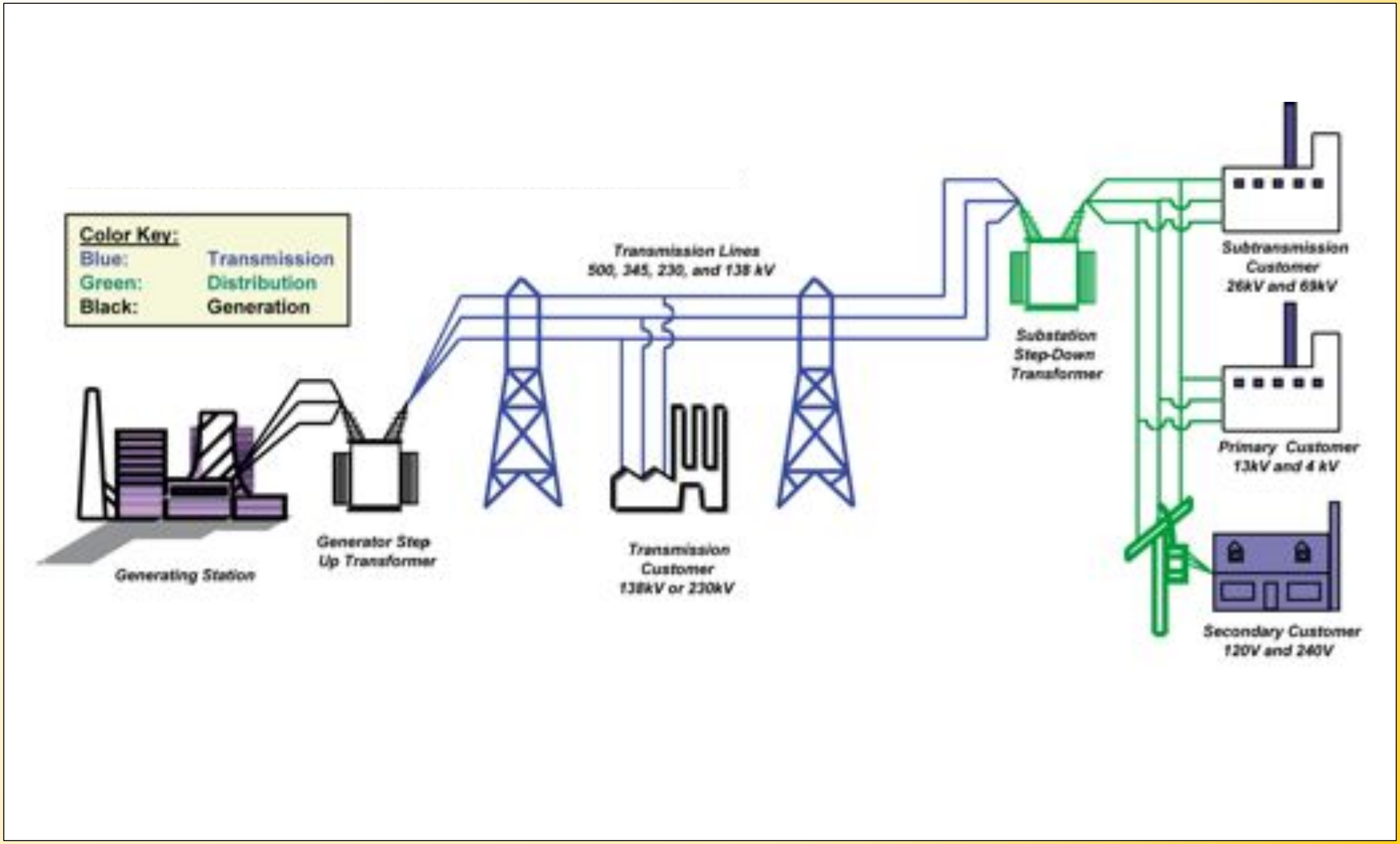
Outline

- Background:
  - Overview of Electrical Power System Basics
    - “Big Wire”
    - IT Infrastructure (“Little Wire”)
  - IT Infrastructure Threats
- Research Challenges:
  - Wide Area Measurement Systems
  - Advanced Metering Infrastructures (AMI)
- Research Directions
  - TCIPG Overview

Outline

- Background:
  - Overview of Electrical Power System Basics
    - “Big Wire”
    - IT Infrastructure (“Little Wire”)
  - IT Infrastructure Threats
- Research Challenges:
  - Wide Area Measurement Systems
  - Advanced Metering Infrastructures (AMI)
- Research Directions
  - TCIPG Overview

Physical ("Big Wire") Infrastructure



Substations

Protection Systems

- **What happens when a short circuit (fault) occurs?**

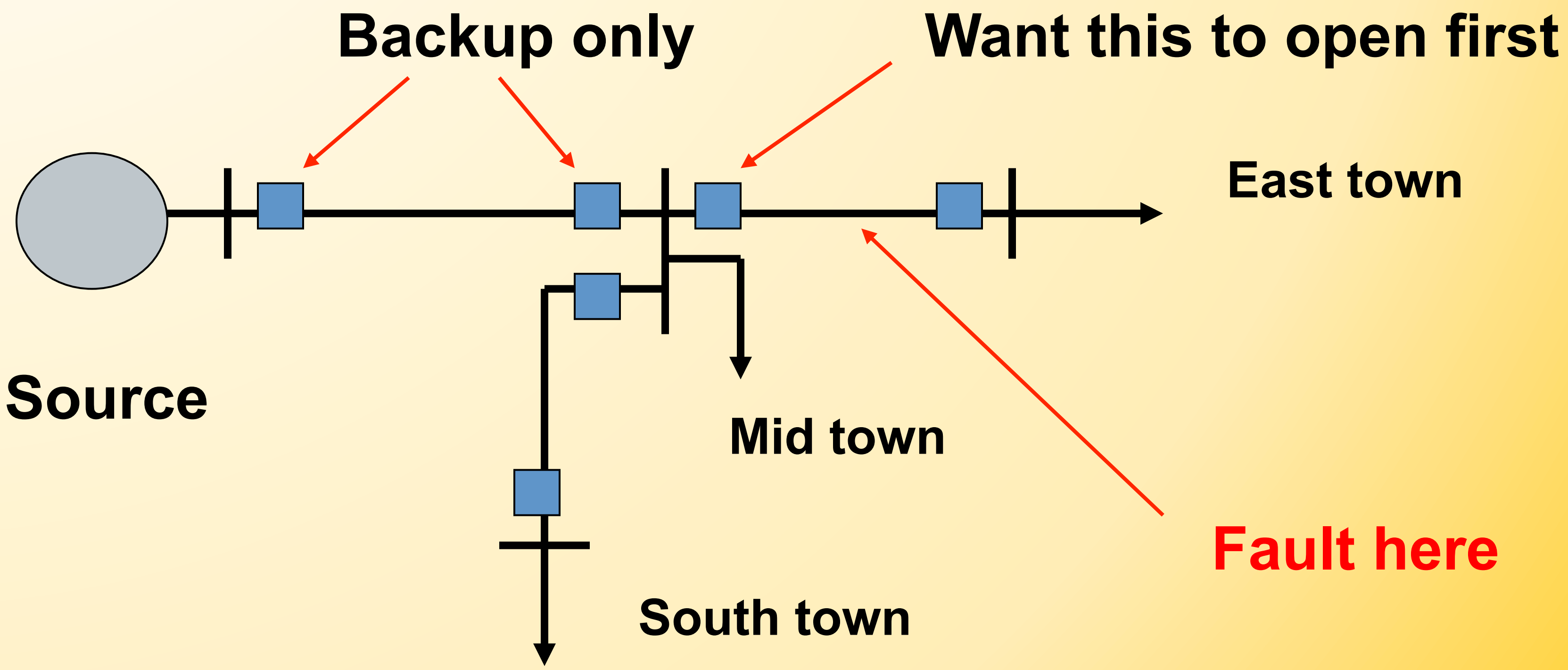
  i.e., tree comes down on some lines
- **The fault must be detected quickly**
- **The fault must be isolated quickly**

How Things Trip

- **Fuses** detect abnormal conditions in lines and trip by melting a wire element. Must be replaced.
- **Relays** detect abnormal conditions through sensors and send signals to tell the circuit breakers to "trip." Settings can be changed.
- **Circuit breakers** open up lines. Can be reused. Can also be remotely "tripped."

Trip Coordination

The right fuses and or circuit breakers need to operate at the right place and right time.



Evolution of substation devices and tools

1900 —— 1950 —— 2000 ——

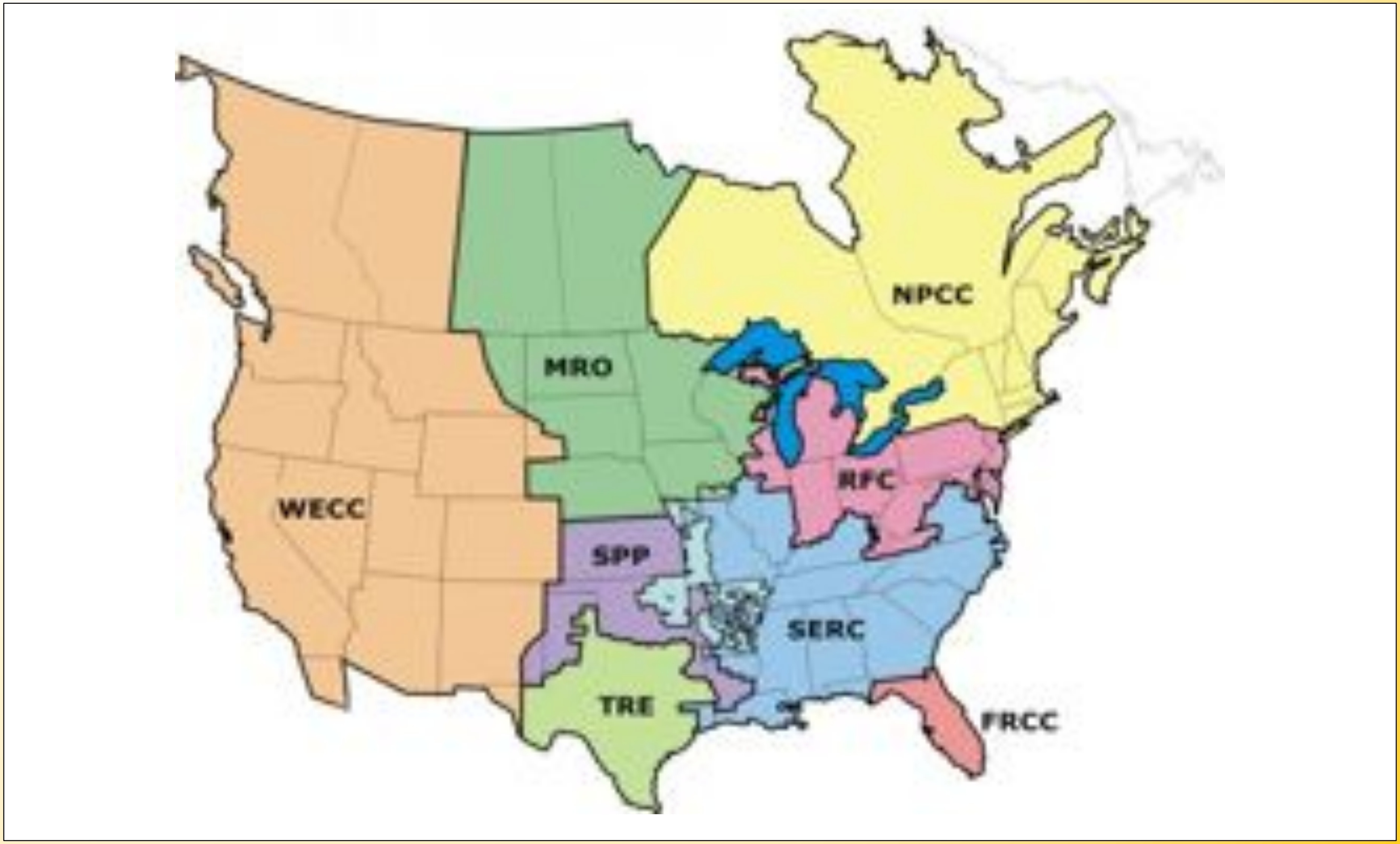
| Electromechanical | Solid state | Digital

(Tools have evolved from screwdrivers to laptops)

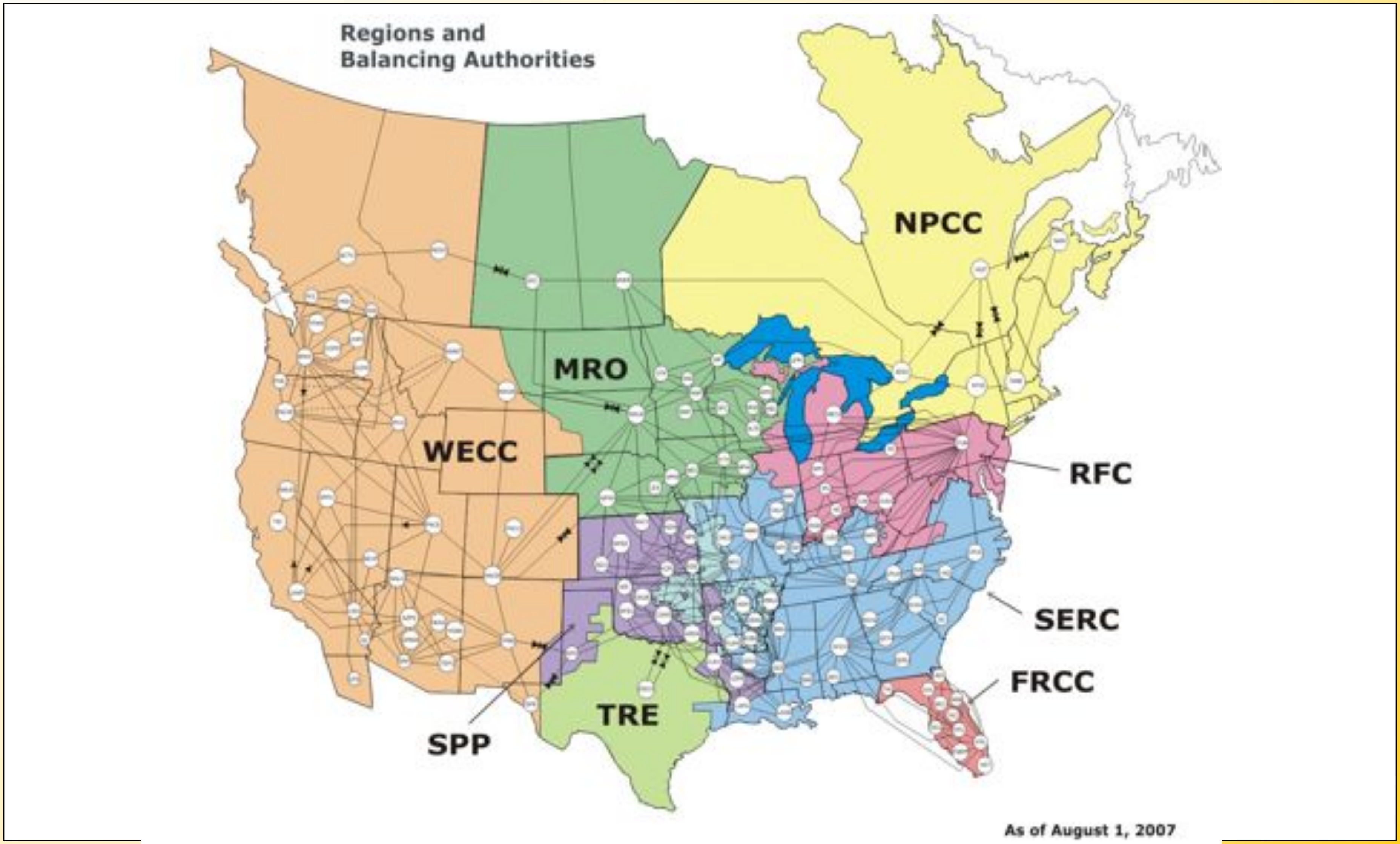
Who’s in charge?

- Federal Energy Regulatory Commission (FERC)
- North American Electric Reliability Corp. (NERC)
- State legislatures
- Regional reliability councils
- ISOs and RTOs
- State commerce commissions
- Control area operators

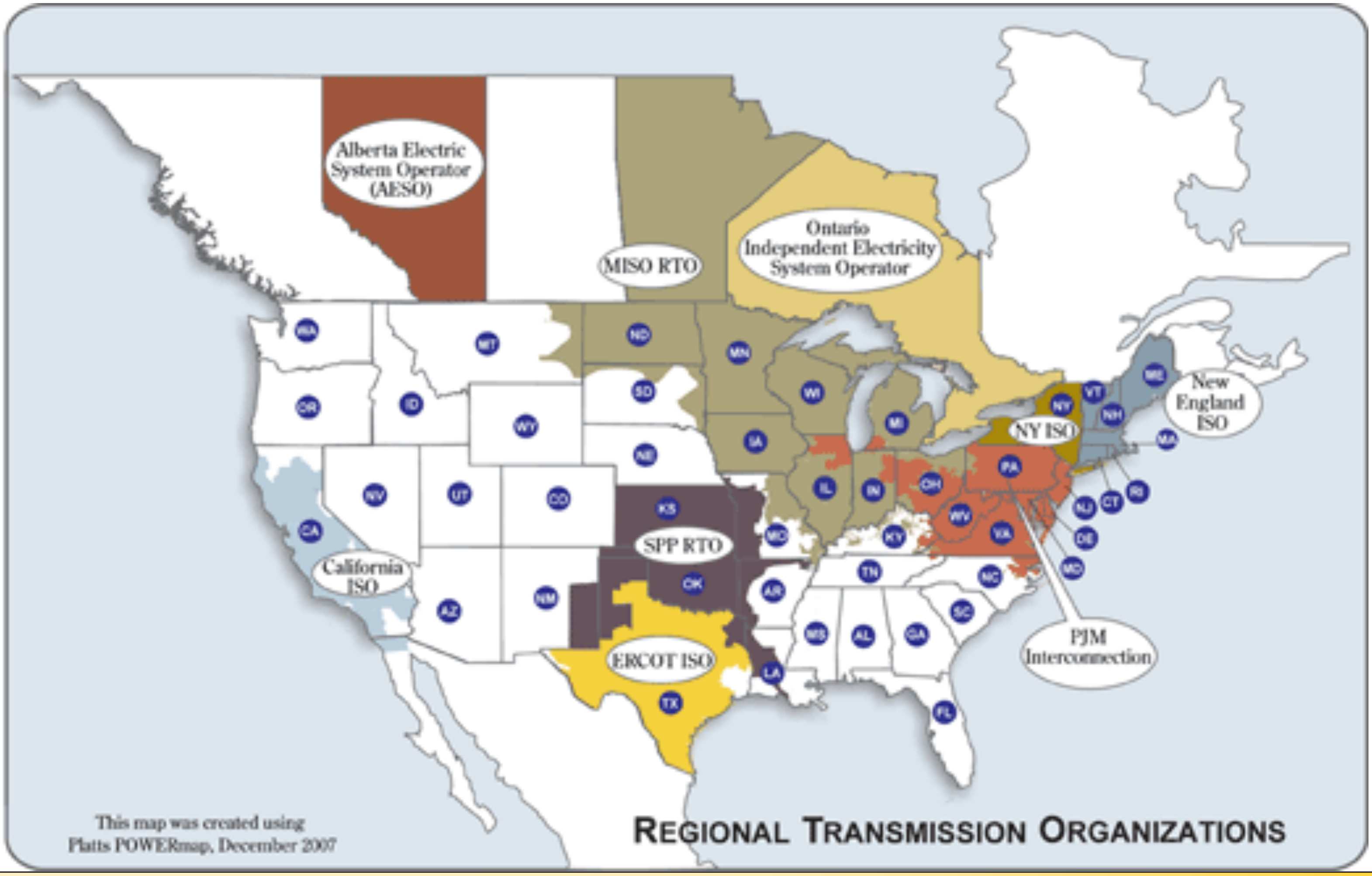
North American Electric Reliability Corporation (NERC)



Balancing Authorities (Control Centers)



Independent System Operators
Regional Transmission Organizations

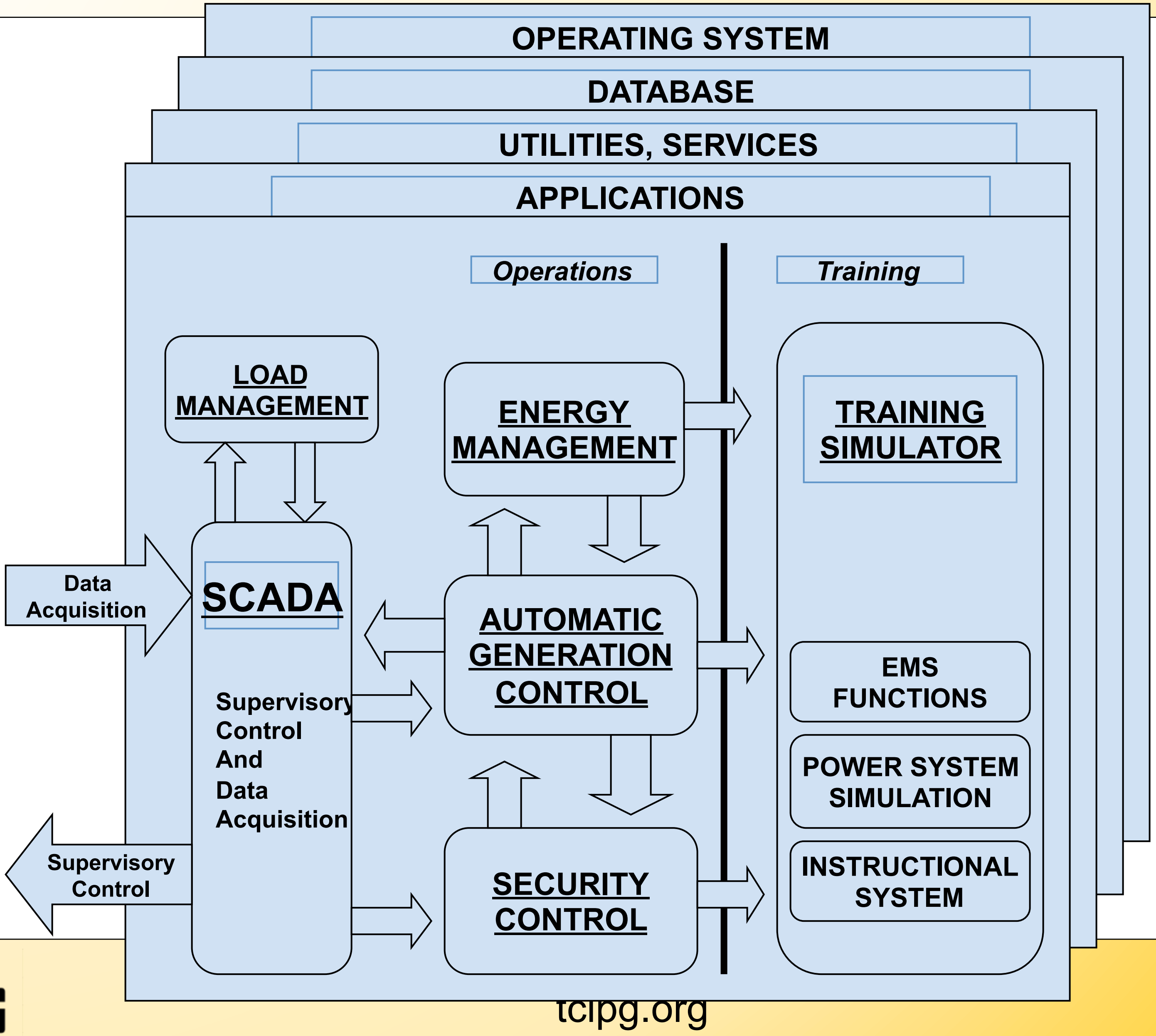

Alberta Electric System Operator (AESO)
MISO RTO
Ontario Independent Electricity System Operator
NY ISO
New England ISO
PJM Interconnection
SPP RTO
ERCOT ISO
California ISO
WA
OR
CA
ID
NV
MT
WY
UT
AZ
CO
NM
ND
SD
NE
KS
OK
TX
MN
IA
MO
AR
LA
WI
IL
MI
IN
OH
KY
TN
MS
AL
GA
FL
SC
NC
VA
WV
PA
NY
VT
NH
ME
MA
RI
CT
NJ
DE
MD
This map was created using Platts POWERmap, December 2007
REGIONAL TRANSMISSION ORGANIZATIONS

Outline

- Background:
  - Overview of Electrical Power System Basics
    - "Big Wire"
    - IT Infrastructure ("Little Wire")
  - IT Infrastructure Threats
- Research Challenges:
  - Wide Area Measurement Systems
  - Advanced Metering Infrastructures (AMI)
- Research Directions
  - TCIPG Overview

Control Centers / Balancing Authorities

EMS Information Structure



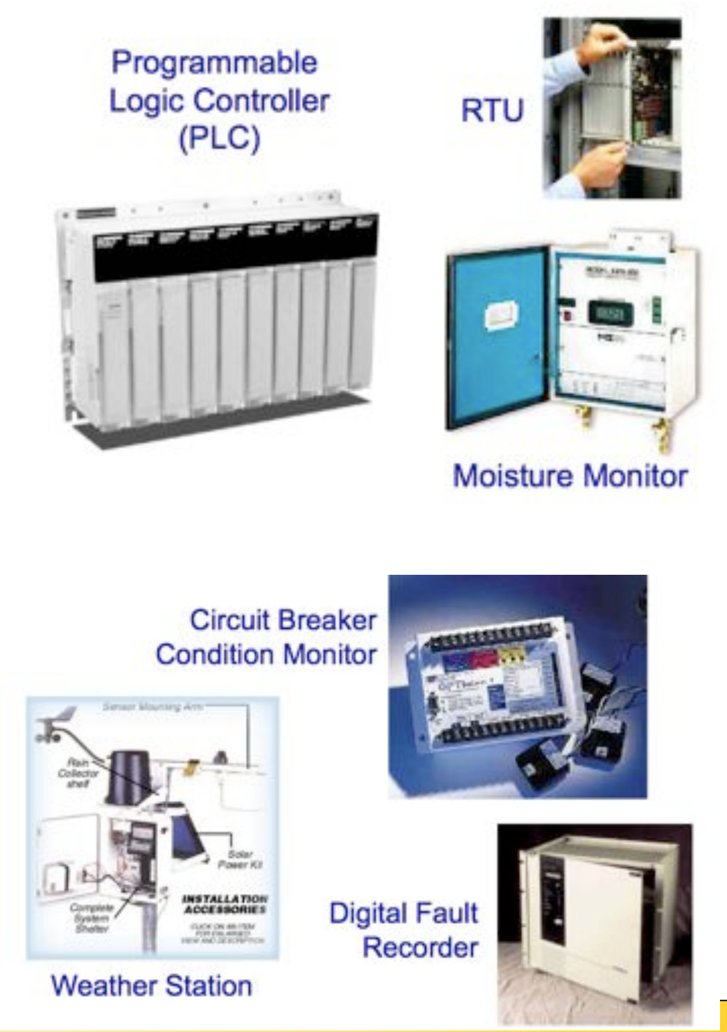
SCADA

- **Supervisory Control and Data Acquisition (SCADA)**
  - Supervisory Control => Remote control of field devices
  - Data Acquisition => Monitoring of field conditions

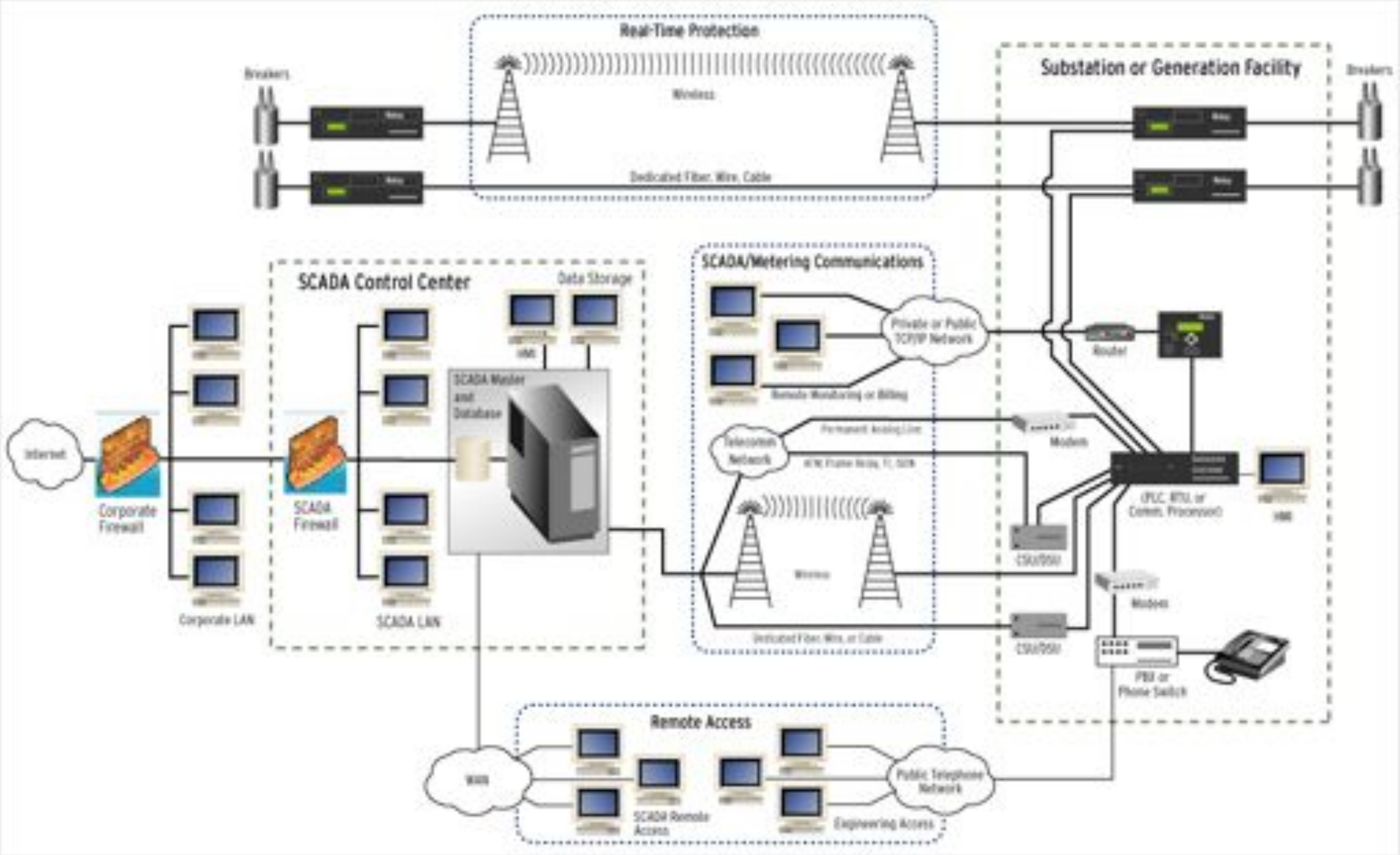
- **SCADA System Components**
  - Master Station => System “nerve center” located in electric utility energy control center; Dispatchers use it to monitor and control the system
  - Field Devices => Needed wherever there is data to be sent to master station (substations, lines or feeders)
  - Communications => Links master station with field devices; Continuous 24 x 7 operation

SCADA Architecture

- Sensors measure the desired quantities – i.e. voltage and current
- These data are fed to a remote terminal unit (RTU)
- The master computer or unit resides at the control center EMS


Programmable Logic Controller (PLC)
RTU
Moisture Monitor
Circuit Breaker Condition Monitor
Weather Station
Digital Fault Recorder

Control Communication Architecture



From a presentation by D. Whitehead, “Communication and Control in Power Systems”, TCIP summer school, June, 2008

Substation Communications

Legacy (older – in place)

Serial communication EIA-232, EIA-422/485
Copper and Fiber Optics
Data Rates as ranging from 300 to 115k BPS

Modern

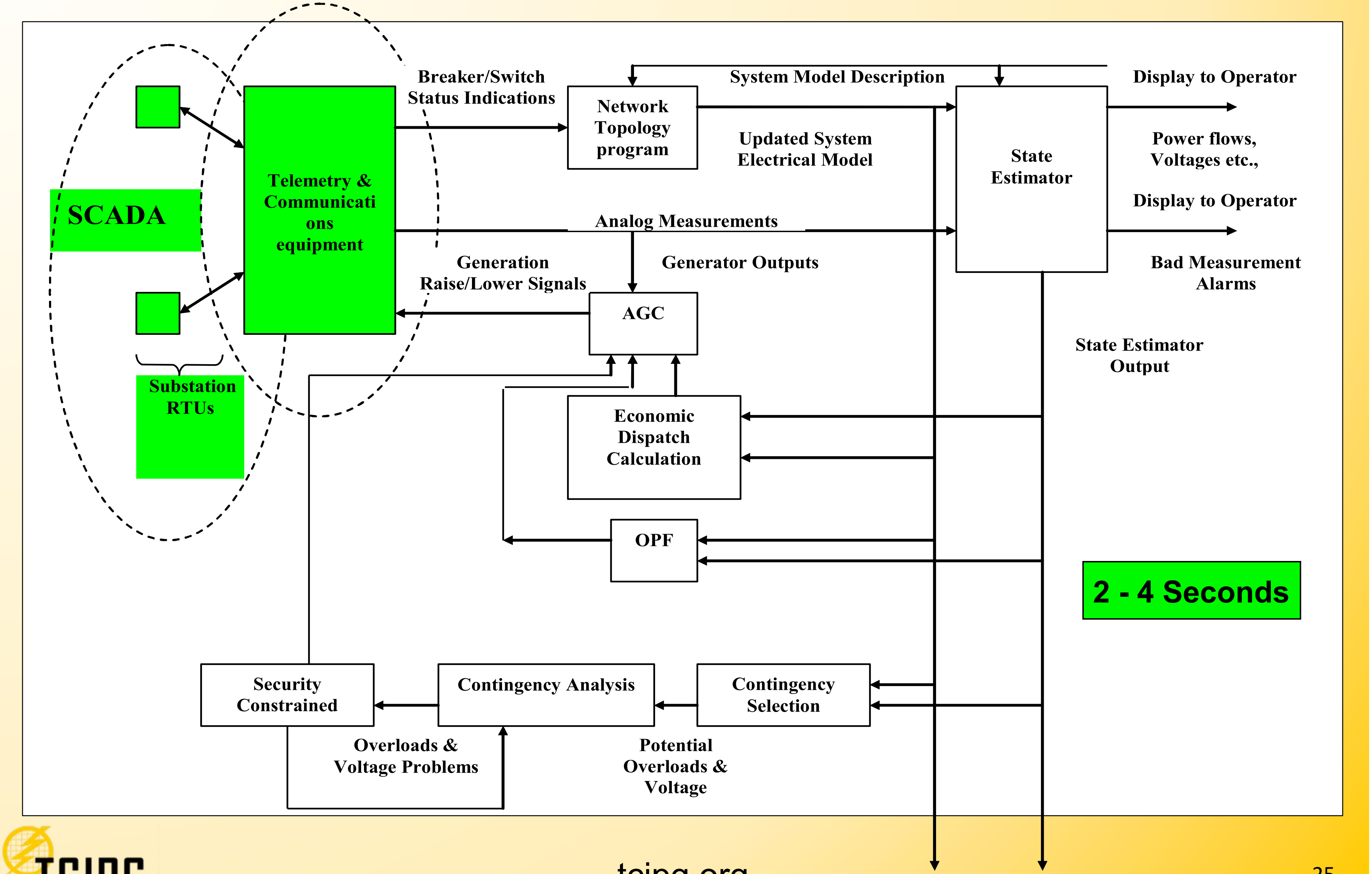
Ethernet
Copper and Fiber Optics
Data rates ranging from 10MBPS to 1GBPS

Communication protocols

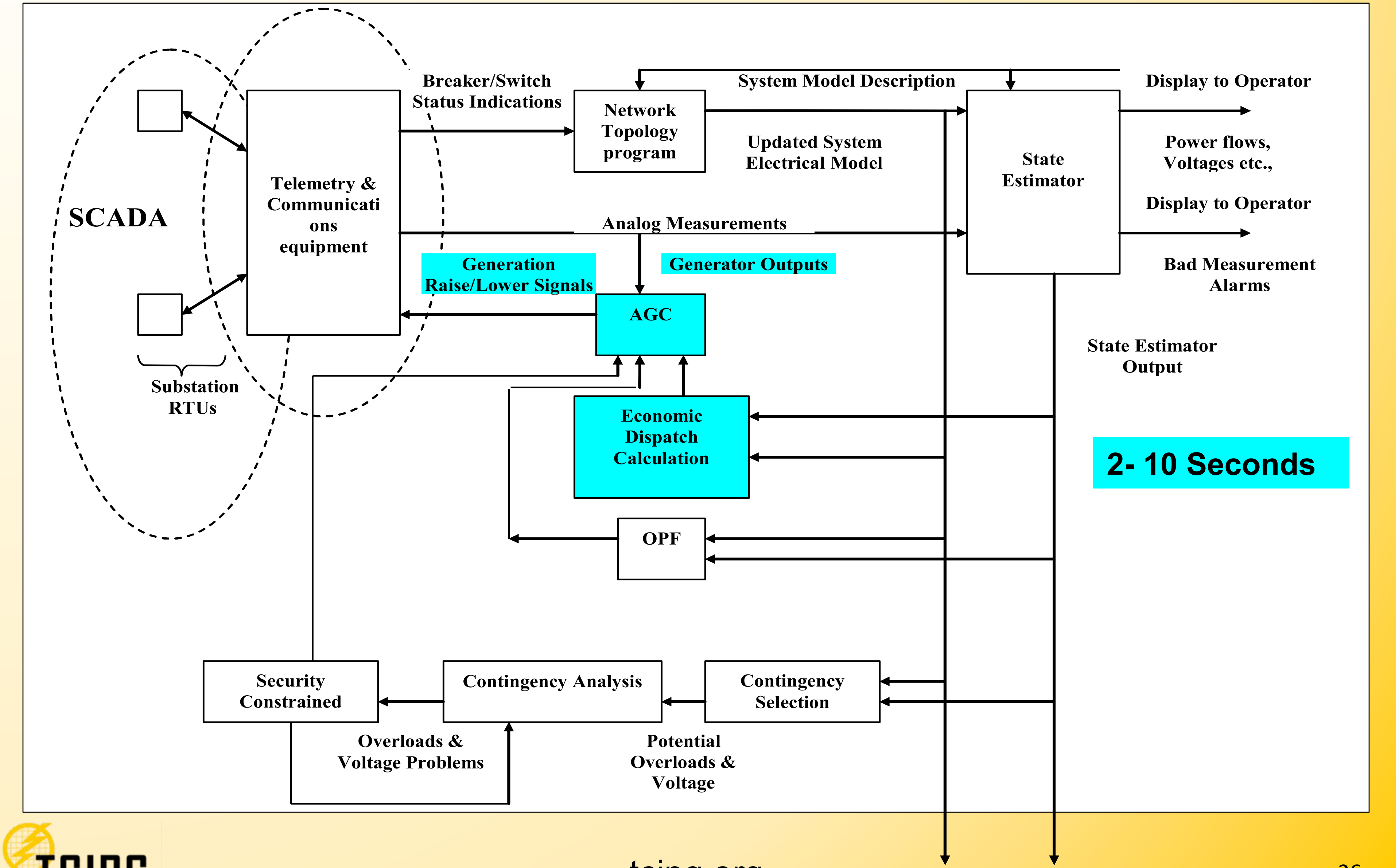
ASCII – Easy to convert to readable text. Slow.
Modbus® – Originally designed to establish communications between two PLCs.
Modbus® Plus – Improvement on original.
DNP3 – Popular in North America & Internationally; well supported.
UCA/MMS - Utility Communications Architecture. Used in the U.S. for communications in power systems.
IEC 61850 - New Standard. Popular outside the US. Used for control and intra-substation data exchange between IEDs.
TASE.2/ICCP - Used for communication between SCADA masters.

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

Timescale of Communications

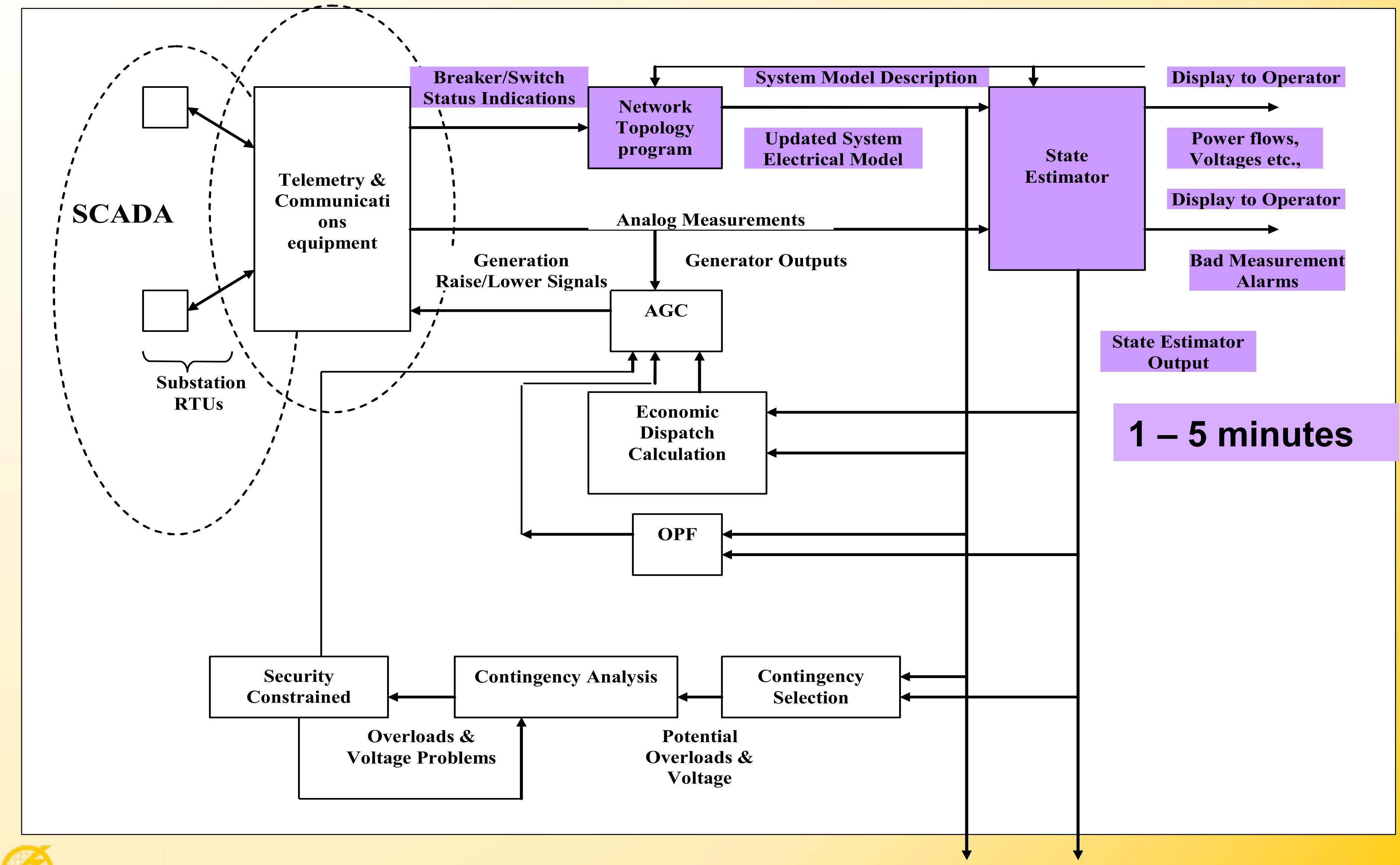


Timescale of Communications



2- 10 Seconds

Timescale of Communications



SCADA

Substation RTUs

Telemetry & Communicati ons equipment

Breaker/Switch Status Indications

Network Topology program

System Model Description

Updated System Electrical Model

State Estimator

Display to Operator

Power flows, Voltages etc.,

Display to Operator

Bad Measurement Alarms

State Estimator Output

Analog Measurements

Generation Raise/Lower Signals

Generator Outputs

AGC

Economic Dispatch Calculation

OPF

Security Constrained

Contingency Analysis

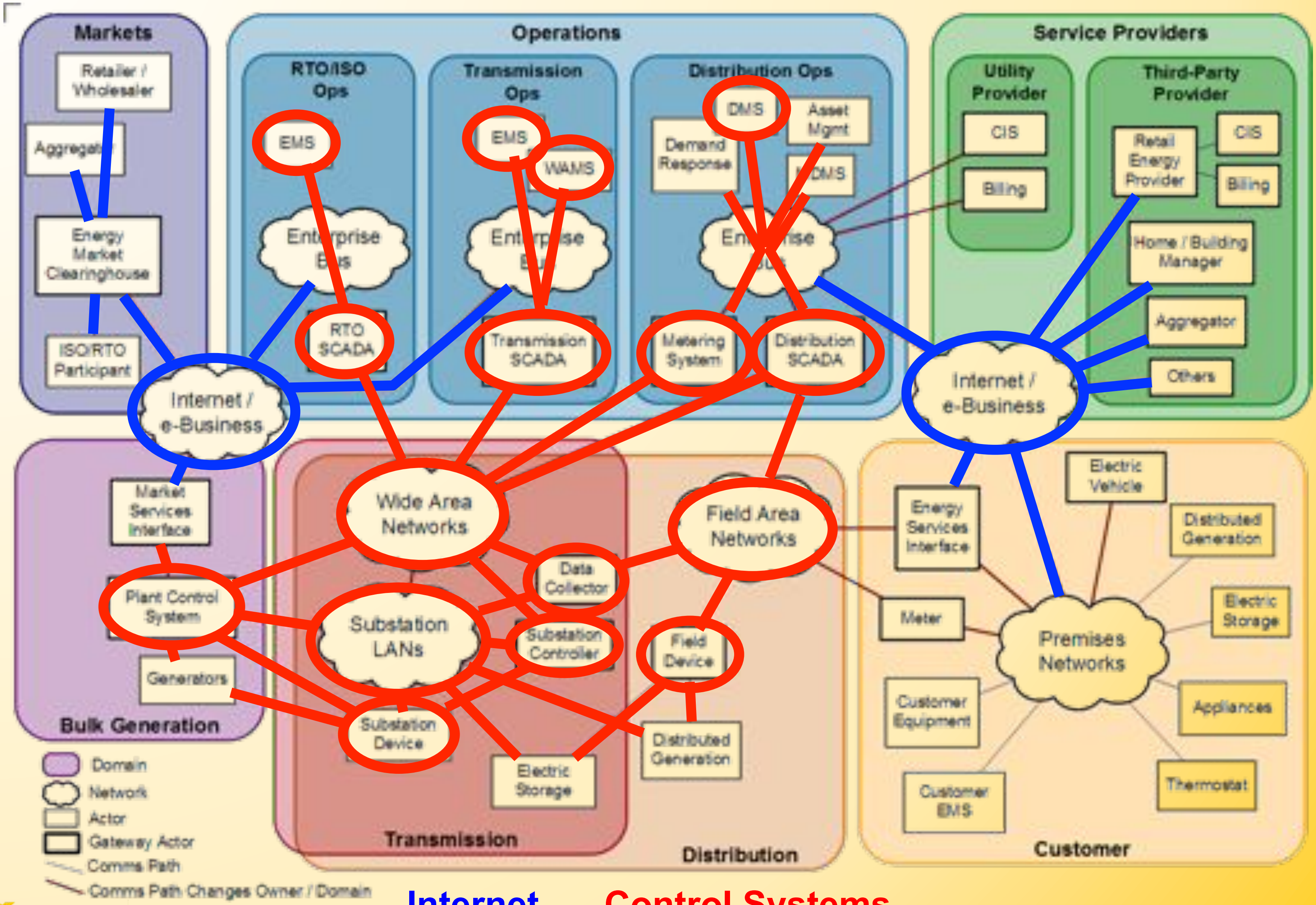
Contingency Selection

Overloads & Voltage Problems

Potential Overloads & Voltage

1 – 5 minutes

Networks in the coming Smart Grid Infrastructure



Internet **Control Systems**

borrowed from NIST Smart Grid Twiki

TCIPG

tcipg.org

Outline

- Background:
  - Overview of Electrical Power System Basics
    - "Big Wire"
    - IT Infrastructure ("Little Wire")
  - IT Infrastructure Threats
- Research Challenges:
  - Wide Area Measurement Systems
  - Advanced Metering Infrastructures (AMI)
- Research Directions
  - TCIPG Overview

IT technology Risks (Traditional Grid)

Cost issues drive equipment towards commodity hardware, software, protocols, e.g.

- Even out in the field, older protocols (e.g. MODBUS, DNP3) that once defined layer-2 behavior are carried by TCP or UDP
- Operating systems
- Networking protocols, e.g., HTTP, SMTP, etc.
- Networking hardware
- Enterprise application software
- Use of wireless networking

The control system is connected to the business network

- Gathering and reporting of data

The Resulting Problems

- All the problems of commodity IT
- Additional vulnerabilities
  - Old software, run unpatched
  - Sensitivity to misconfiguration of devices, security
  - Availability trumps security
  - Very weak access controls
  - Fragility of system to scans

Vulnerabilities: Field Devices

- Web-based configuration and status
- Software/firmware Updates required
- Expected interactions highly structured
  - Code may not be tested against environments outside expectations
    - Many instances of a control system failing as a result of a vulnerability scan
    - Other interactions may cause a freeze up or crash (e.g. ping sweep)

Vulnerabilities: Unpatched Software

- Many control systems run old versions of Windows (reports of (gasp) Windows 96, Windows 98)
  - No longer supported by MS
- Patches may cause other behavior that interferes with the control system
  - Unanticipated because patches are tested for “normal” IT
- Patching may require a re-boot
- Potential warranty issues

Vulnerabilities: Authentication

Control systems often have weak authentication standards

- E.g. same password, all devices, never changed
- Password painted on control station door
- Very limited crypto, so
  - Passwords sent in cleartext
  - Communication between machines sent in the clear
- Passwords never changed from vendor's default
  - And operation of vendor's system may require that! (Stuxnet…)

Vulnerabilities: Constrained AV

Anti-virus technology common in IT has problems in a control system

- Keeping signatures up-to-date under strict network constraints
- AV in embedded systems limited
- No time is a good time for a full blown analysis of the system disk

Outline

- Background:
  - Overview of Electrical Power System Basics
    - "Big Wire"
    - IT Infrastructure ("Little Wire")
  - IT Infrastructure Threats
- Research Challenges:
  - Wide Area Measurement Systems
  - Advanced Metering Infrastructures (AMI)
- Research Directions
  - TCIPG Overview

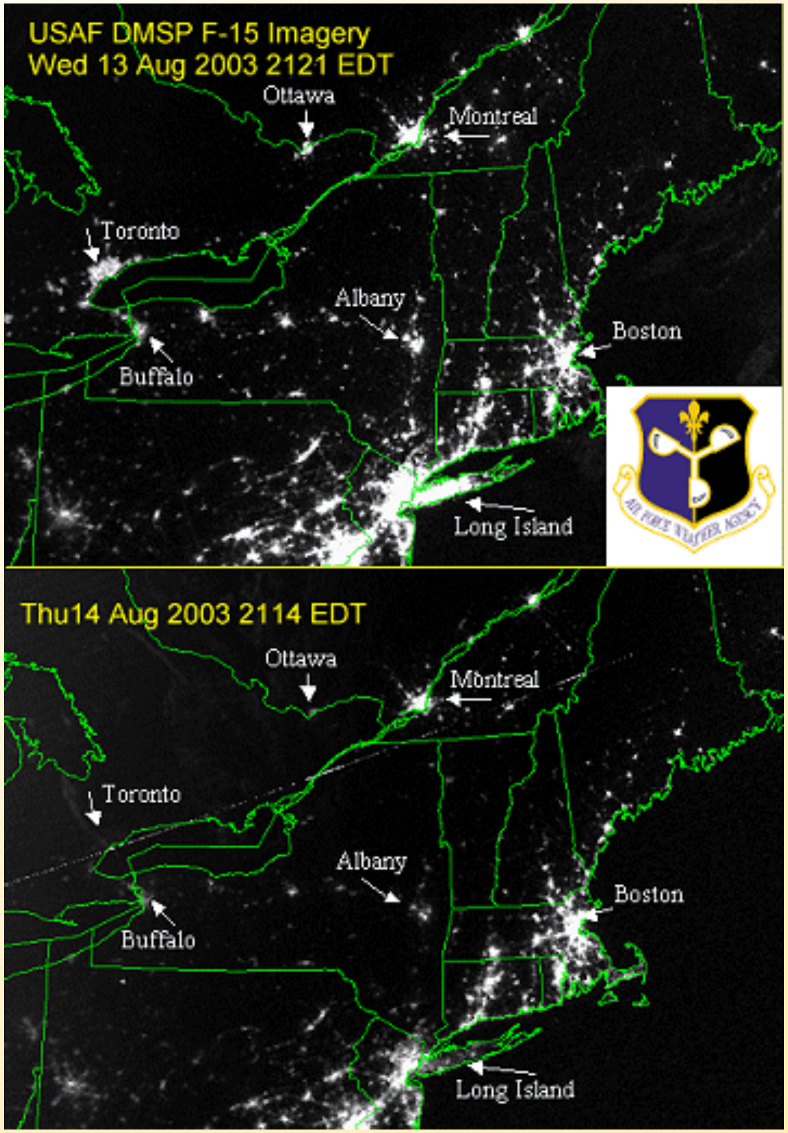
Outline: Wide Area Measurement Systems

- August 2003 blackout
  - Analysis and recommendations
- North American SynchroPhasor Initiative (NASPI)
  - PMUs and SynchroPhasors
  - PMU Systems and Data Networks
- Challenges:
  - Distributed networking
  - Quality of service
  - Cyber security

Major North American Blackouts

Date	Location	Load Interrupted
November 9, 1965	Northeast	20,000 MW
July 13, 1977	New York	6,000 MW
December 22, 1982	West Coast	12,350 MW
January 17, 1994	California	7,500 MW
December 14, 1994	Wyoming, Idaho	9,336 MW
July 2, 1996	Wyoming, Idaho	11,743 MW
August 10, 1996	Western Interconnection	30,489 MW
June 25, 1998	Midwest	950 MW
August 14, 2003	Northeast	61,800 MW

Blackout of August 14, 2003



THE NATION'S NEWSPAPER

NFL preseason

'One good day' at the PGA

USA TODAY

NO. 1 IN THE USA

Married – with cameras

Blackout misery

50 million affected in Northeast and beyond as power grid fails

Transportation Many 'wait it out,' by air and land ■ 4A | Scene Moms in labor, cars stuck in car washes ■ 5A | Impact Offices close, ATMs idle, cellphones jam ■ 1B

What's next for Mr. Vick?

A Super Bowl isn't far-fetched for Atlanta. Not with him at QB ■ 1C

Fri/Sat/Sun, August 15-17, 2003

Newsline

California ballot is a field of dreamers

U.S. captures suspect in Bali, Jakarta bombings

LifeSavers changing flavors

USA TODAY Snapshots

Outage spawns rush-hour chaos from Detroit eastward

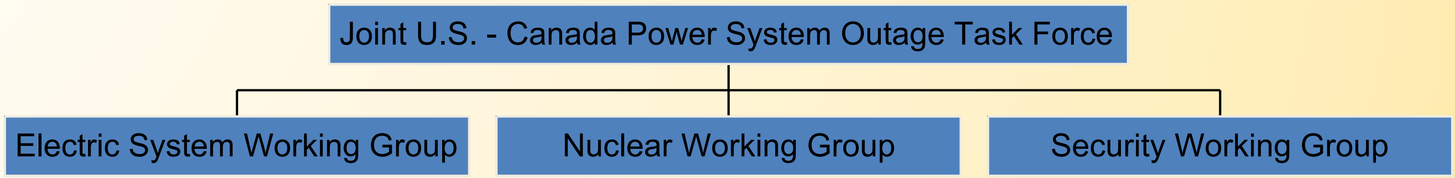
More annoyance than angst in NYC, despite early fears

Exodus recalls images of 9/11

Cover story

Credit: Jeff Dagle

August 14, 2003 Blackout Investigation



Joint U.S. - Canada Power System Outage Task Force

Electric System Working Group

Nuclear Working Group

Security Working Group

Investigate the cascading electrical failure.

Review performance of plants and assess possibility of damage.

Determine if failures were caused with malicious intent.

- Phase I
  - Investigate the outage to determine its causes and why it was not contained
  - Interim report released November 19, 2003
- Phase II
  - Develop recommendations to reduce the possibility of future outages and minimize the scope of any that occur
  - Final report released April 5, 2004

U.S.-Canada Power System Outage Task Force

Interim Report:

Causes of the
August 14th Blackout
in the
United States and Canada

Canada

November 2003

U.S.-Canada Power System Outage Task Force

Final Report on the
August 14, 2003 Blackout
in the
United States and Canada:

Causes and
Recommendations

Canada

April 2004

Credit: Jeff Dagle

Blackout Root Causes

- **Situational Awareness**: lack of effective
  - contingency analysis capability
  - procedures to ensure operators were aware of the status of critical monitoring tools
  - procedures to test monitoring tools after repairs
  - monitoring tools after alarm system failed
- **Vegetation management**
- **Reliability Coordinator Diagnostics**
  - Lack of wide area visibility, monitoring, coordination

Selected Blackout Report Recommendations

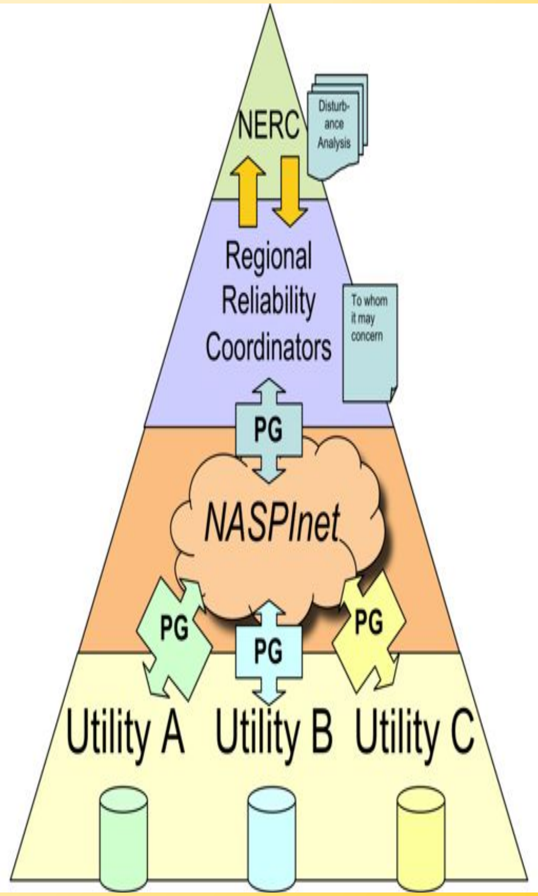
- Better real-time tools for grid monitoring and operation
- Establish physical and cyber-security capabilities

A Mandate for Wide Area Situational Awareness

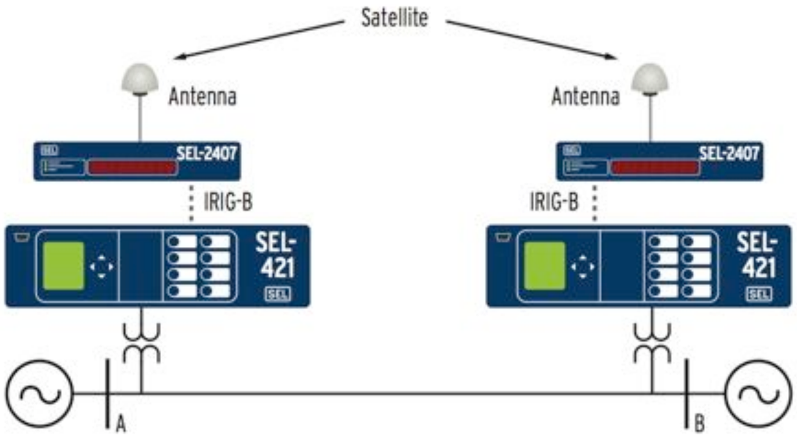
- **A FERC/NIST Priority Area**
  - Monitoring and display of power system components and performance across interconnections and wide geographic areas in real time
  - Enable understanding, optimized management, performance, prevent/ respond to problem
- **Other relevant priorities**
  - **Cyber Security: "**Measures to ensure the confidentiality, integrity and availability of the electronic information communication systems, necessary for the management and protection of the Smart Grid's energy, information technology, and telecommunications these infrastructures"
  - **Network Communications: "**Encompassing public and non-public networks, the Smart Grid will require implementation and maintenance of appropriate security and access controls tailored to the networking and communication requirements of different applications, actors and domains"

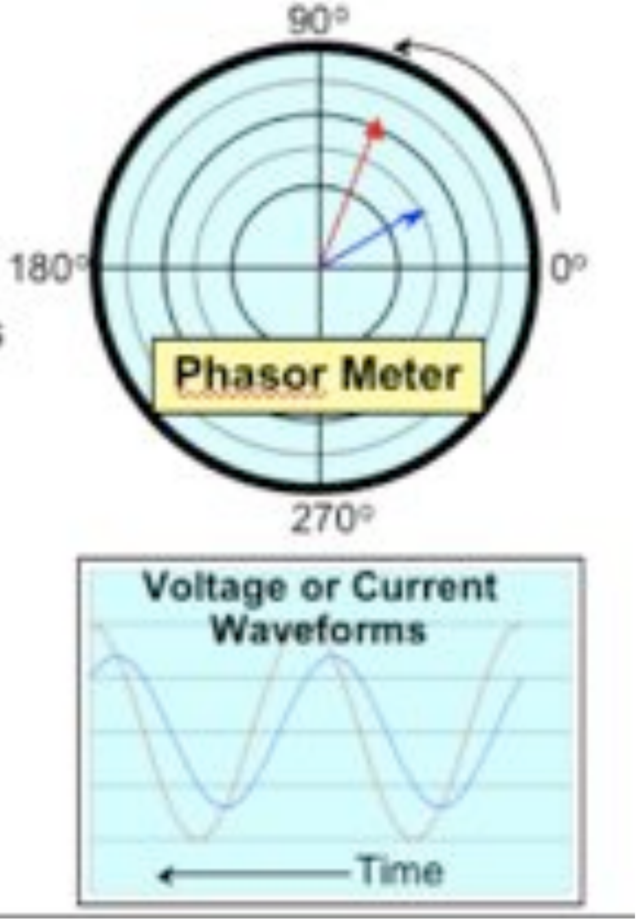
Wide Area Measurement Systems

- **A Wide Area Measurement System (WAMS) is crucial for the Grid**
- **One very promising data source for WAMS: Synchrophasors**
  - GPS clock synchronized; Fast data rate > 30 samples/sec
  - Phasor Measurement Unit (PMU)
- **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



PMUs and Synchrophasors

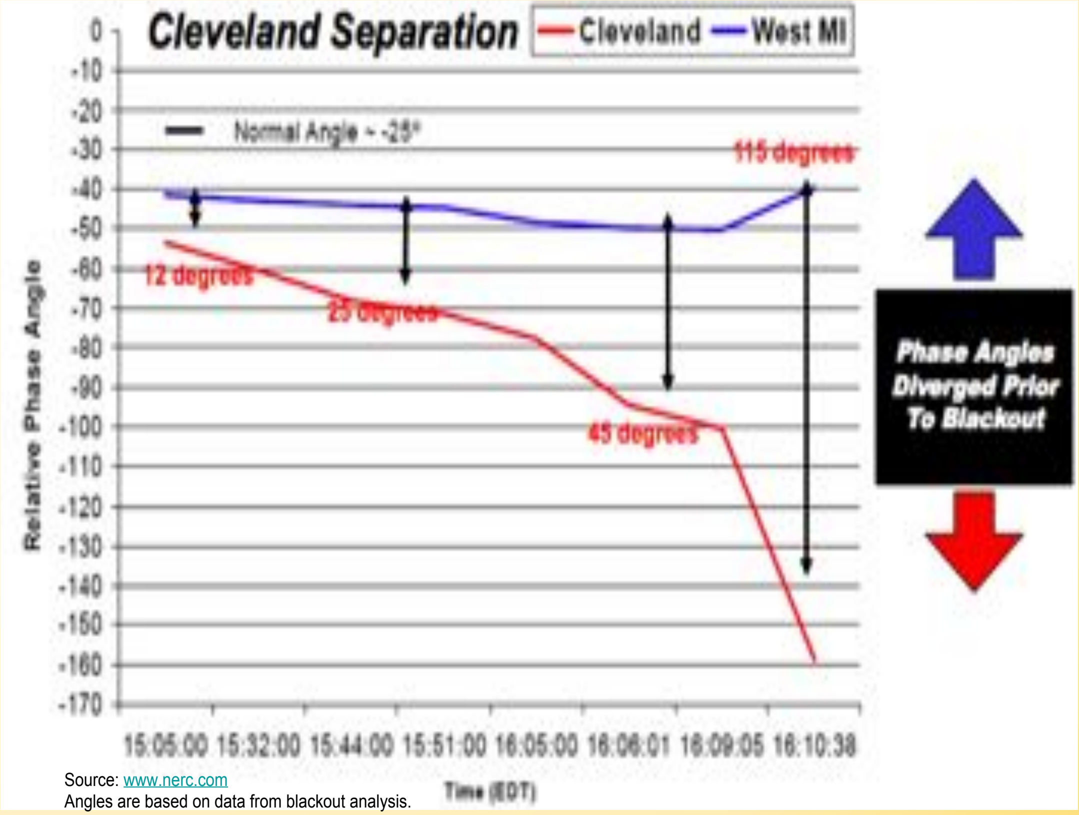




- **Traditional SCADA data since the 1960's**
  - **Voltage & Current Magnitudes**
  - **Frequency**
  - **Every 2-4 seconds**
- **Phasor Measurement Units (PMU's)**
  - **Voltage & current phase angles**
  - **Rate of change of frequency**
  - **Time synchronized using GPS and 30 - 120 times per second**

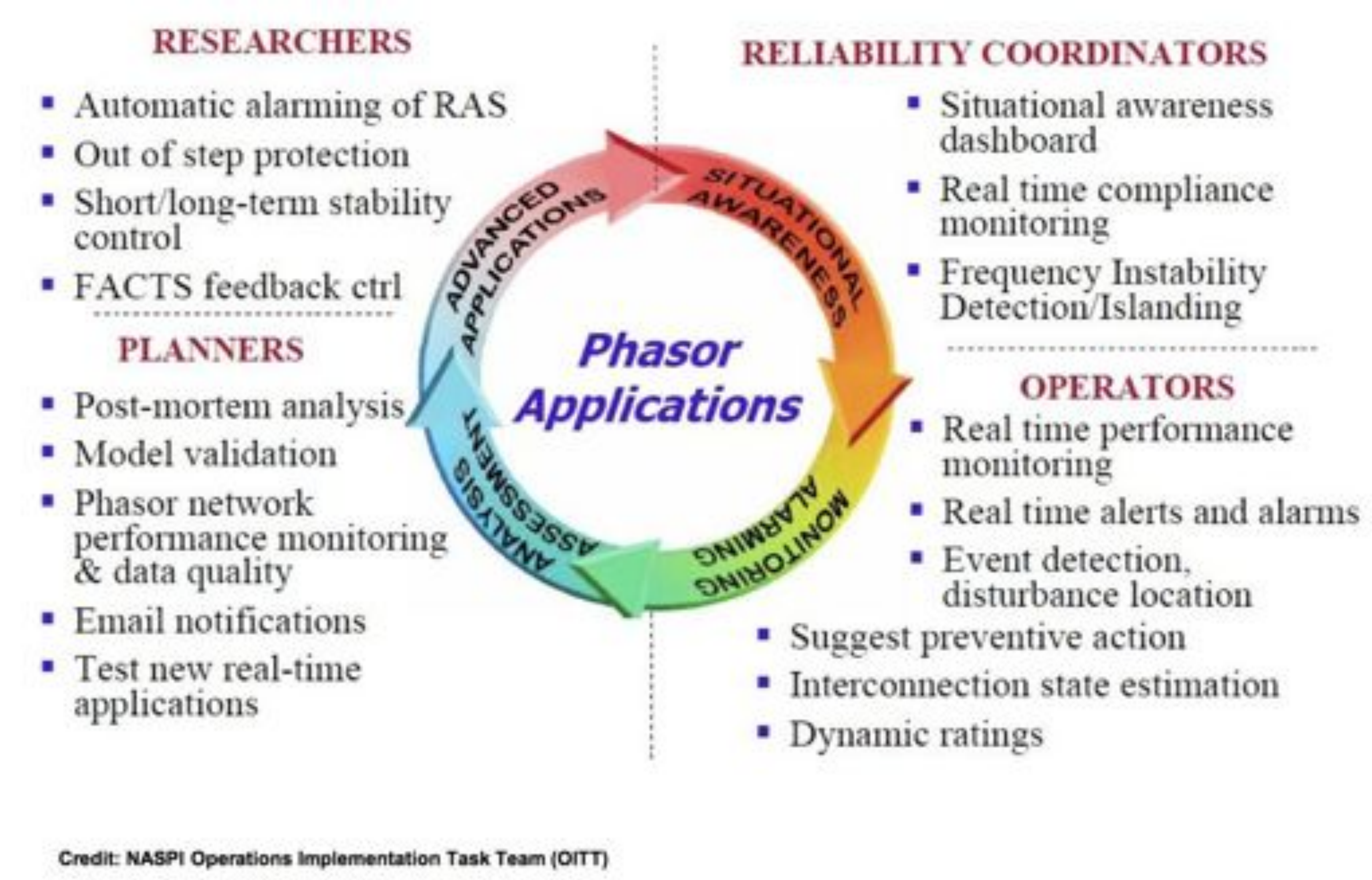
Why do Phase Angles Matter?

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.

Phasor Application Taxonomy



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

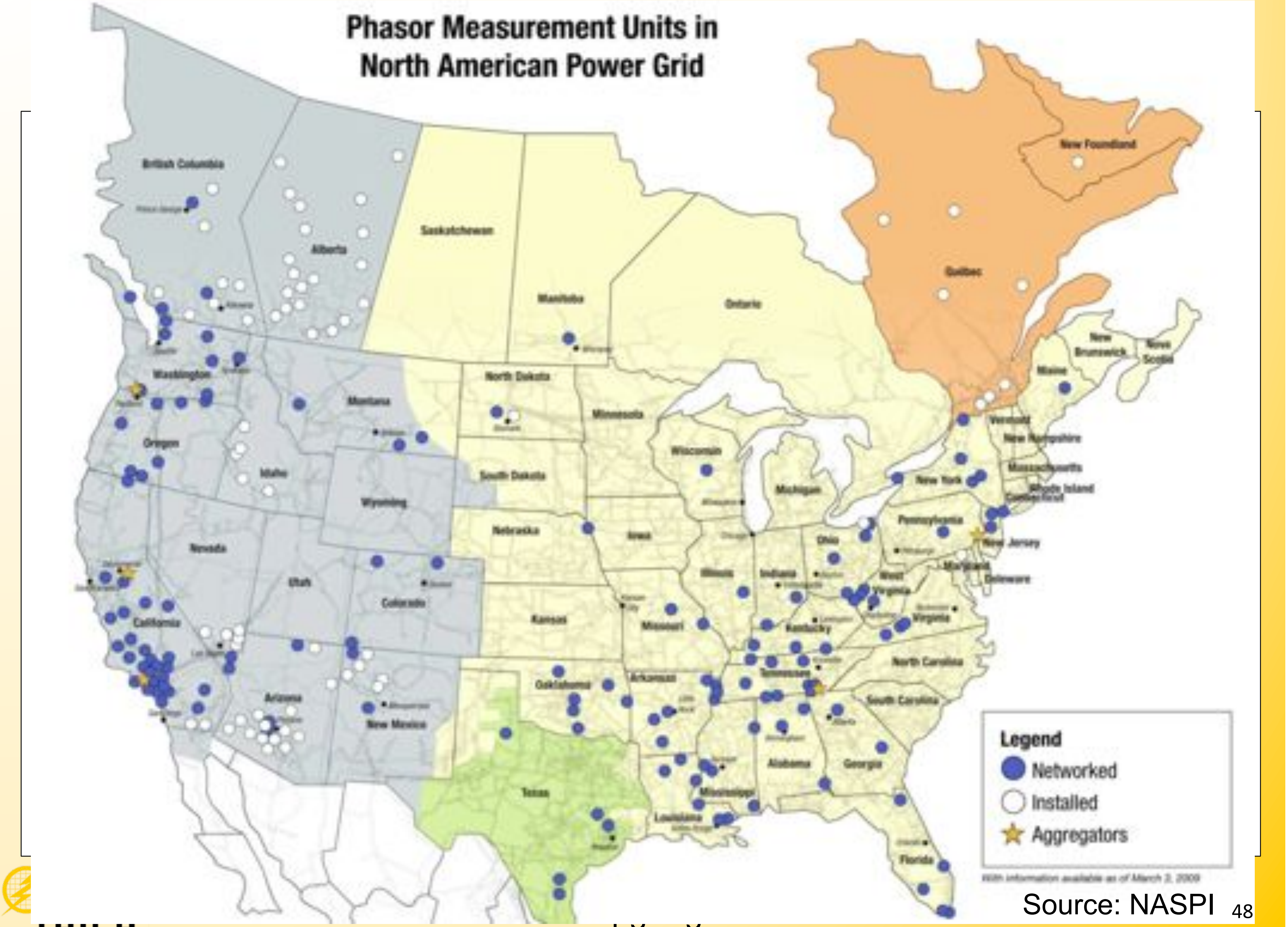
- Situational awareness dashboard
- Real time compliance monitoring
- Frequency Instability Detection/Islanding

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)

Phasor Measurement Units in North American Power Grid



With information available as of March 3, 2009

Source: NASPI

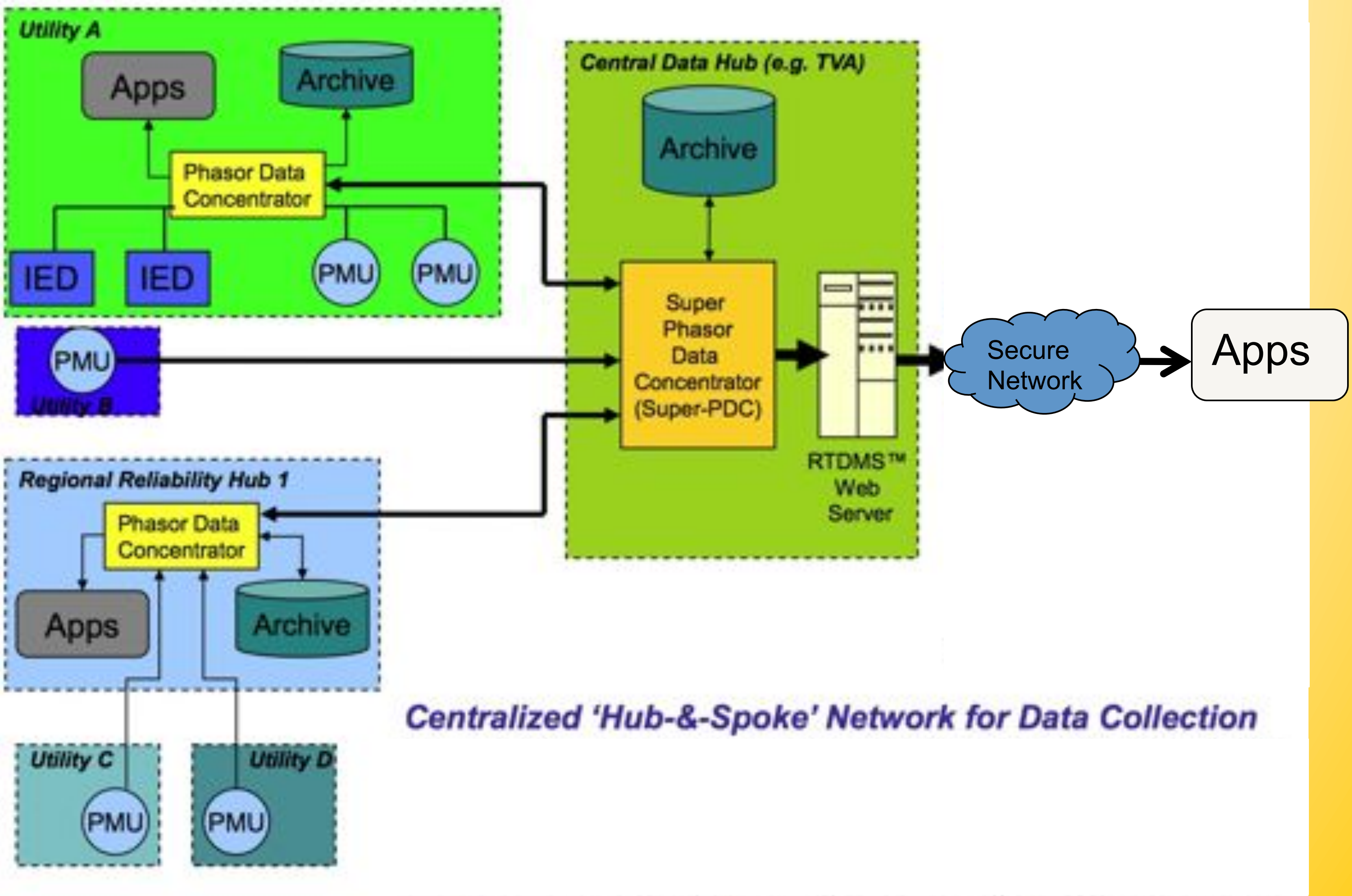
Overview of PMU Systems and Data Networks

- Substation systems and networks
  - PMU, relays, clocks, Ethernet/similar, switches, routers,
- Utility-wide systems and networks
  - Phasor data concentrators, data historian, switches, routers, multiple networking technologies
- NASPInet systems and networks
  - Phasor gateways, data bus, management systems, wide area communication systems
- Applications and users
  - Monitoring, control, protection

Key Cyber Security Requirements

- Data security
  - Desired properties: confidentiality, integrity and availability
  - Threats: eavesdropping, message insertion/modification, denial-of-service
- System security
  - Desired measures: protection, detection and response
  - Threats: intrusions, denial-of-service, malware, insider misuse, others
- Regulation and compliance
  - NERC CIP
  - Recent FERC response to petition and its implications for cyber security of synchrophasor systems

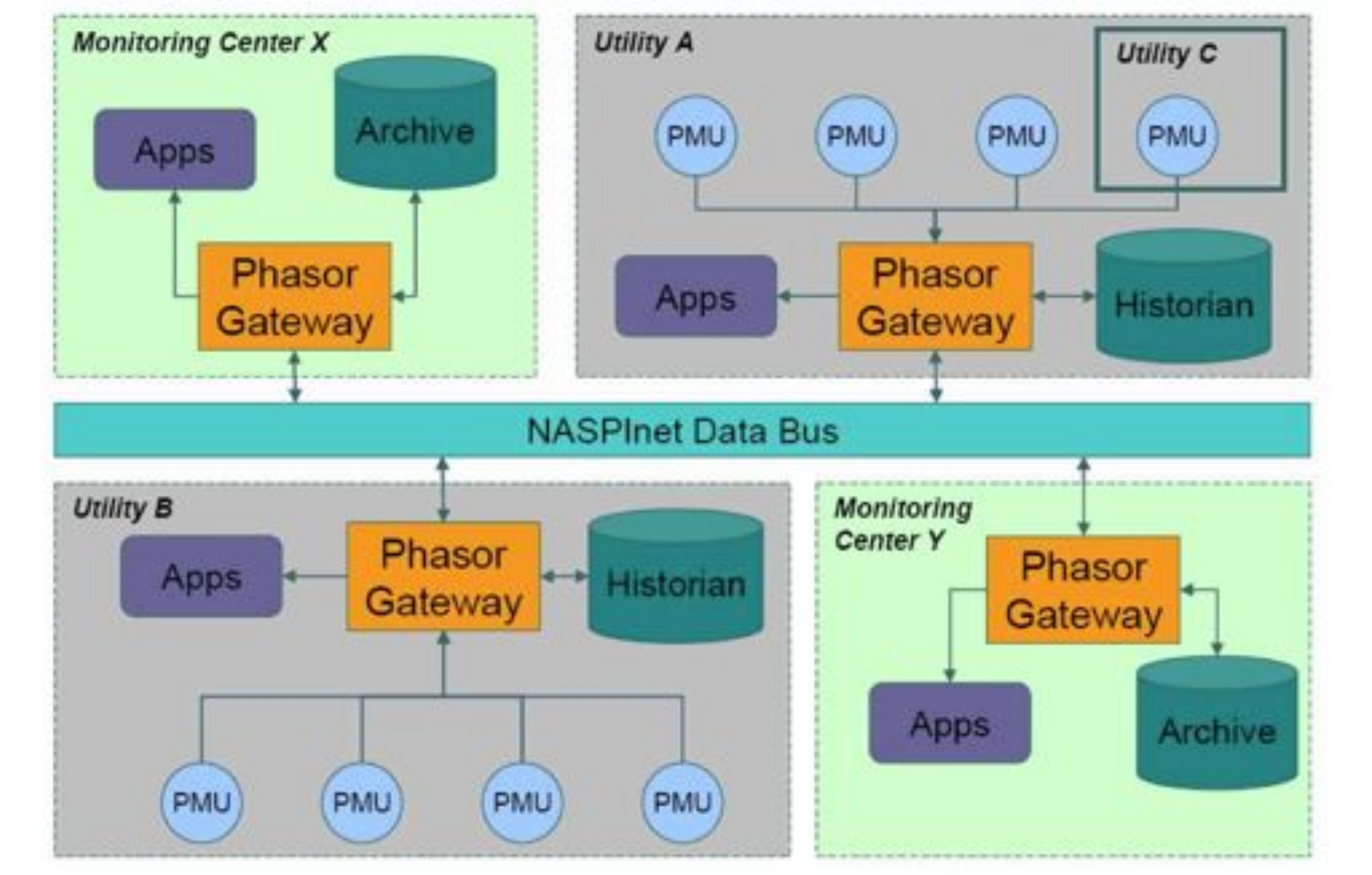
Current Architecture for PMU Data Sharing



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

Source: NASPI

Envisioned PMU Data Flow in NASPInet



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 NASPInet**
  1. Distributed wide-area network design
  2. Network management
  3. Quality of Service and real-time delivery
  4. Cyber security

  - – Progress on these topics made in recently released NASPInet specification document (Quanta Technologies)

1. Distributed Wide-Area Network Design

- Should:
  - Leverage data locality
  - Leverage the existing hierarchy
    - power grid operators, monitors and regulators
  - Allow for incremental growth/formation of NASPInet
  - Simplify trust and key management needed for securing PMU data
  - Simplify network management with localized providers
  - Simplify QoS management

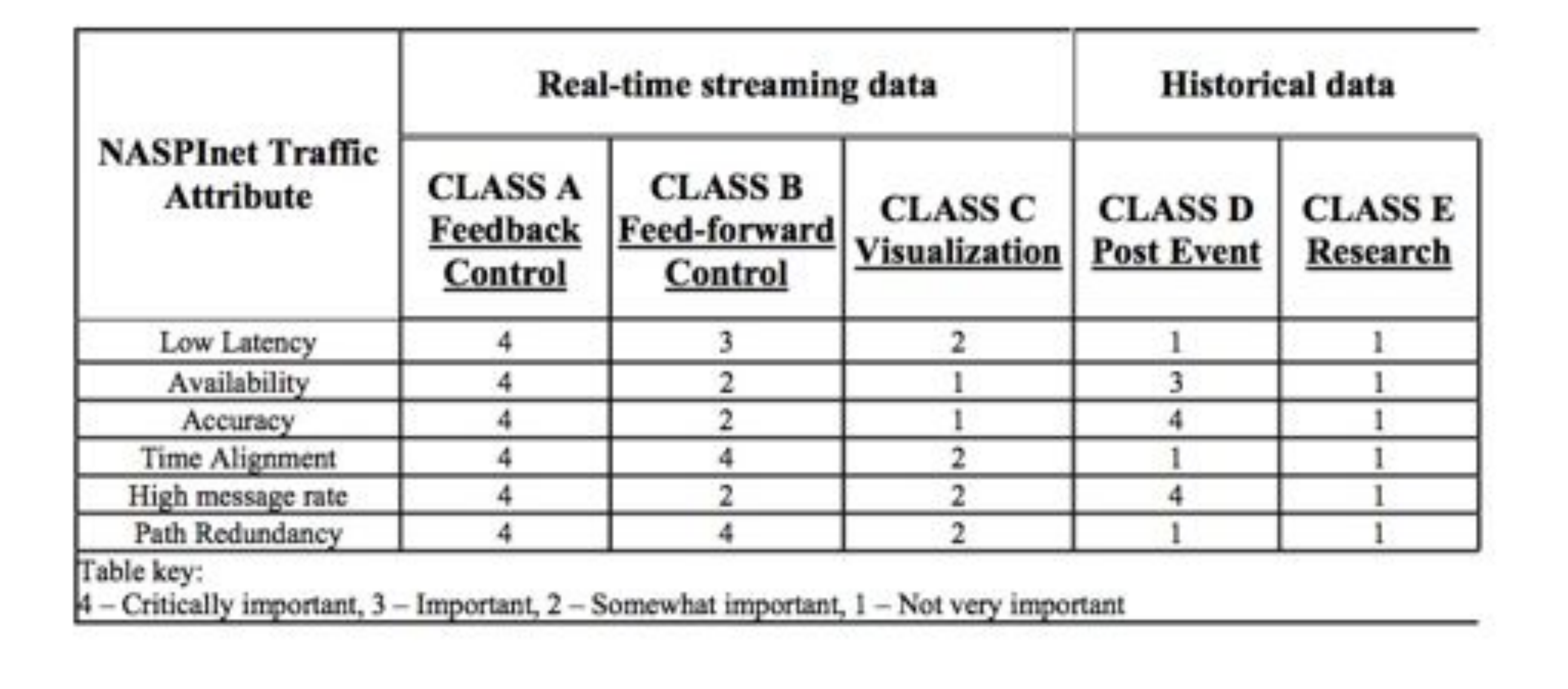
2. Network Management

- **Network management functions**
  - Performance
  - Configuration
  - Accounting
  - Fault management
  - Security management

- Need for appropriate services in NASPInet and means to coordinate between organizations

3. Quality of Service

- 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



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

4. Cyber Security

- Today's approach*: physical and electronic perimeter protection, uniform security level, coarse-grained access control, auditing
  - Addresses baseline security requirements, common threats and attack modes
  - Aligned with current regulatory requirements
- Where do we need to go?
  - Risk-driven graded security levels, granular access control, cross-layer security designs
    - Address sophisticated attacks, provide strong assurances for decision making
    - In line with regulatory changes?
      - Recent proposed CIP changes point towards graded security levels and NIST 800-53 style security controls

* This is a generalization and not correct in all cases.

Outline

- Background:
  - Overview of Electrical Power System Basics
    - "Big Wire"
    - IT Infrastructure ("Little Wire")
  - IT Infrastructure Threats
- Research Challenges:
  - Wide Area Measurement Systems
  - Advanced Metering Infrastructures (AMI)
- Research Directions
  - TCIPG Overview

AMI: Outline

- Technology Overview
  - Goals and features
  - Deployment status
  - Introduction to Smart meters and AMI
  - Manufacturers
- Risk Analysis
  - Vulnerabilities
  - Impact
- Securing AMI
  - Current efforts and challenges
  - Research topics

Part 1/3

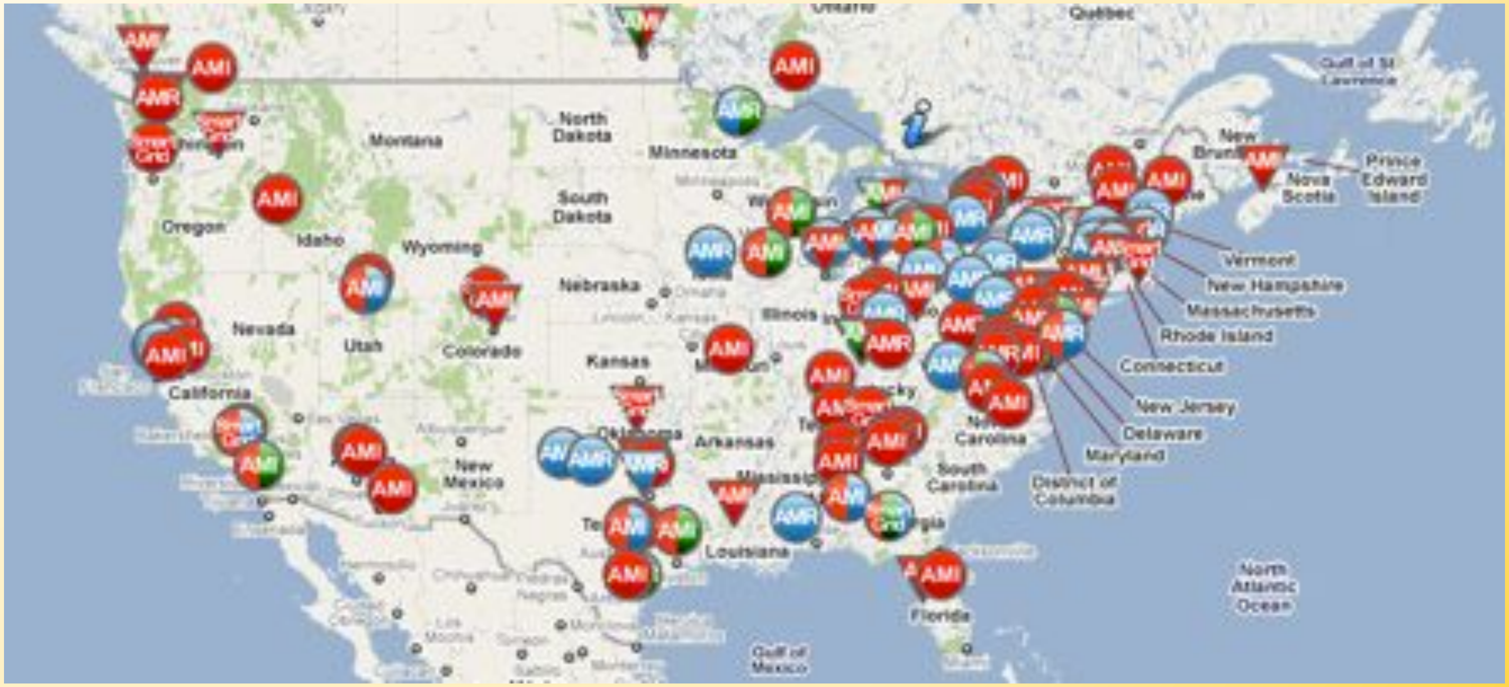
TECHNOLOGY OVERVIEW

AMI Goals and Features

- Automated and remote meter reading
  - Two-way communications
- Increase grid reliability
  - Outage detection and load control
  - Solid-state digital meters
- Enables time-of-use and demand-response (energy and cost savings)
  - Frequent sampling with time-tagged storage
- Empower customers
  - Outage notification
  - Customer web portal
  - Meters potentially used as gateway to the Home Area Network (HAN)

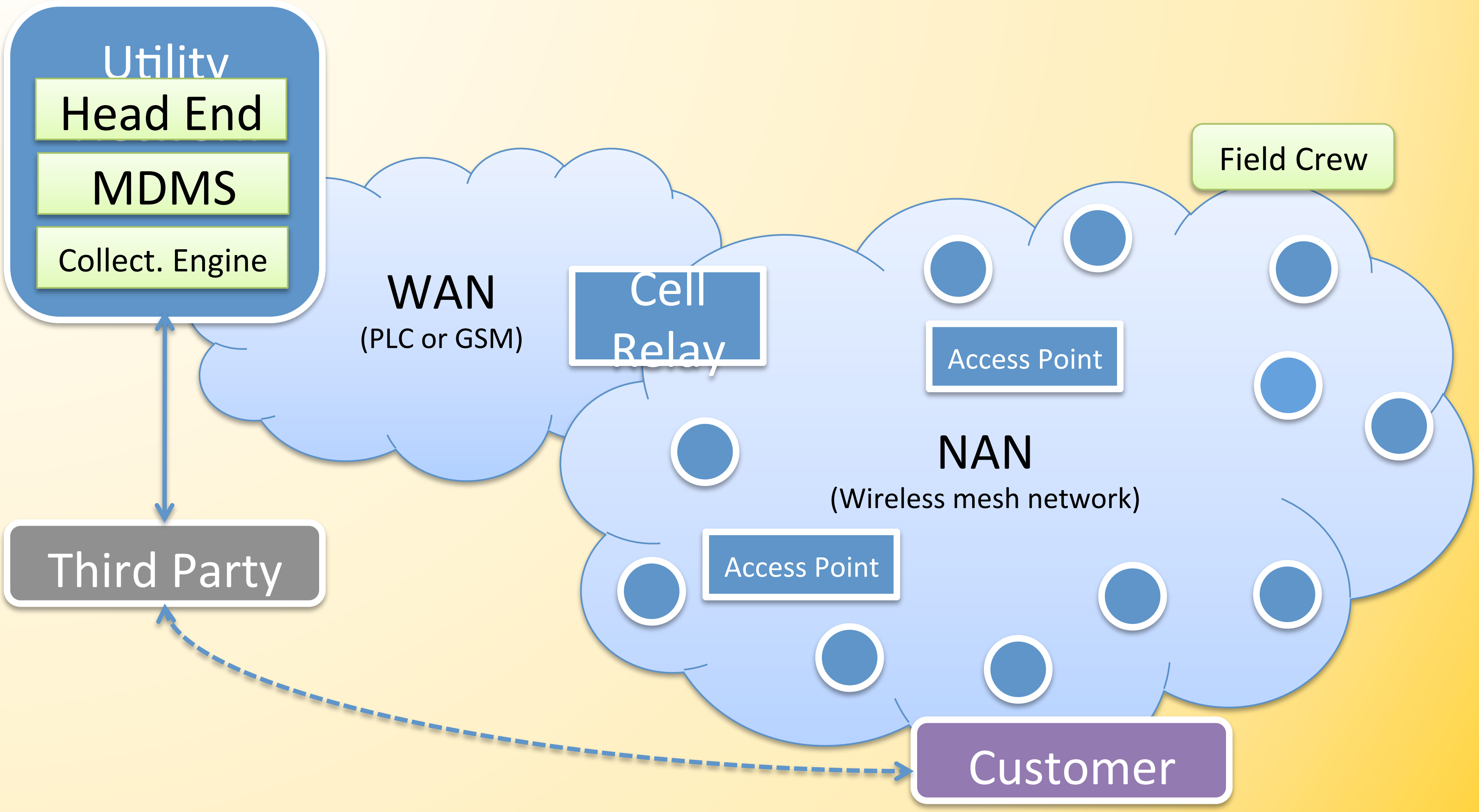
Deployment Status

- US meter deployment (end of 2010):
  - 21 million smart meters
  - Total number of meters: 340 million: 222 million legacy meters (all sectors), 118 million automated (AMR + AMI)
- Total planned: 57.9 million (90 active utilities)



Smart Metering Projects Map on Google Map and http://meterpedia.com/

Advanced Metering Infrastructure (AMI)

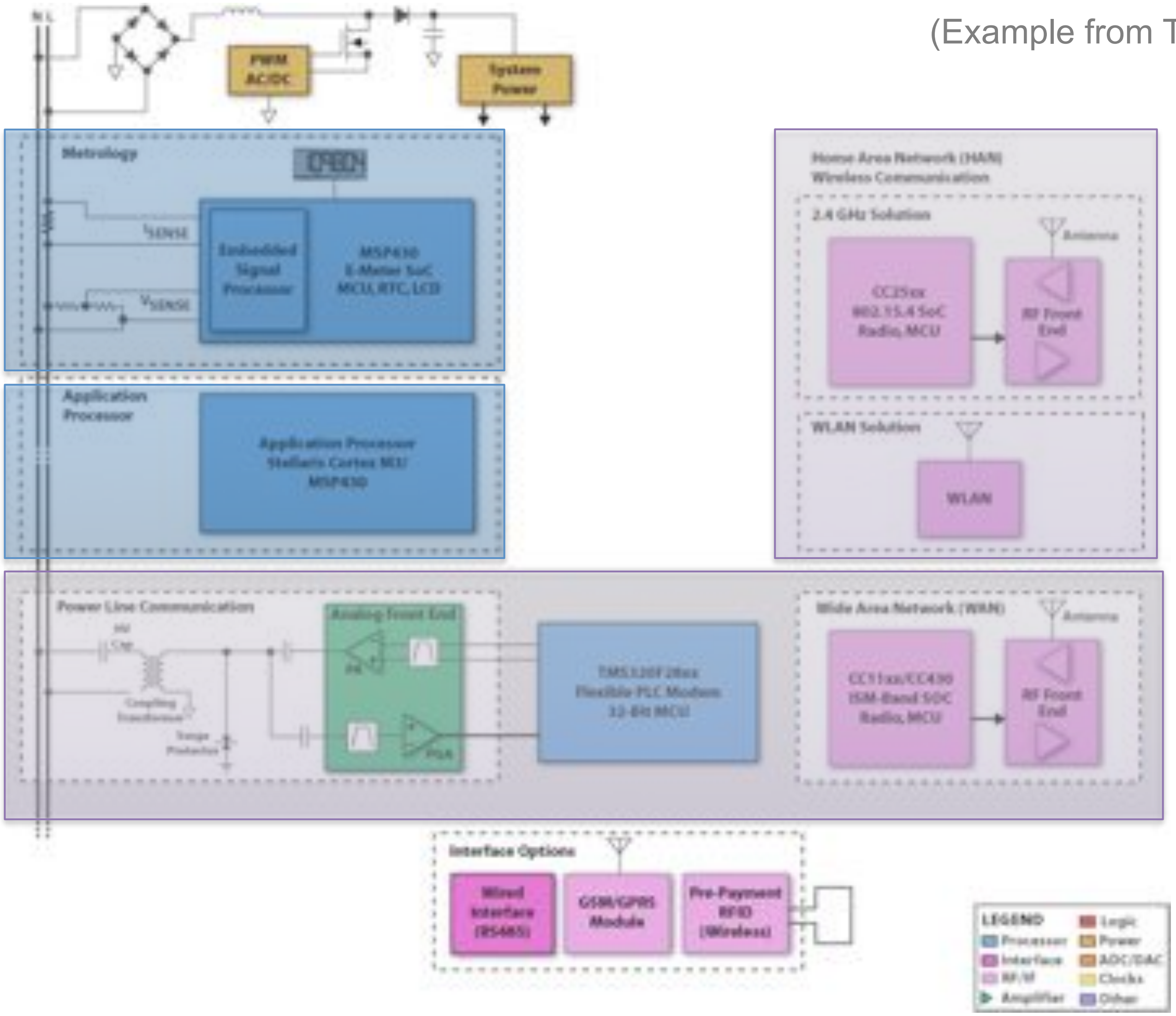


LEGEND: WAN: Wide Area Net., NAN: Neighborhood Area Net.,
PLC: Power Line Comm., MDMS: Meter Data Management System,

● Smart Meter

Smart Meter: Anatomy (cont.)

(Example from Texas Instrument)

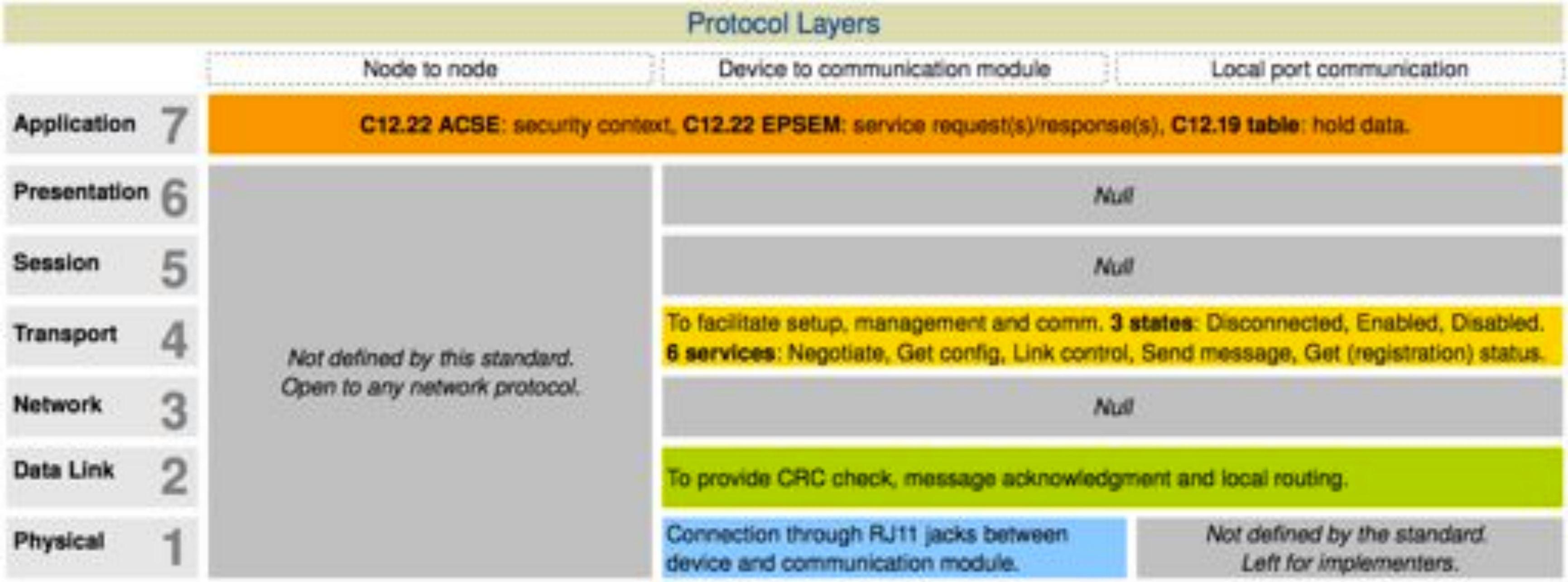


Smart Meter: Anatomy (cont.)

- Technologies & Performances:
  - Metrology
    - CPU: low power 16-bit RISC, up to 25 Mhz
    - Memory: Flash, up to 256 KB and RAM, up to 16 KB
  - Application Processor:
    - CPU: 32-bit ARMv7 (Cortex-M), up to 170 Mhz
    - Memory: Flash, up to 2MB
  - Communication:
    - HAN: Zigbee, Wifi
    - NAN: Proprietary unlicensed wireless (900 Mhz)
    - WAN: GSM, PLC, BLP, WiMax

AMI (cont.)

- Communication Protocols
  - **C12.22**: communication over any reliable network
  - **C12.19**: table data definition
  - C12.21: communication over telephone modem
  - C12.18: point-to-point communication over optical connection



Protocol Layers

		Node to node	Device to communication module	Local port communication
Application	7	**C12.22 ACSE**: security context, **C12.22 EPSEM**: service request(s)/response(s), **C12.19 table**: hold data.		
Presentation	6	*Not defined by this standard. Open to any network protocol.*	*Null*	
Session	5		*Null*	
Transport	4		To facilitate setup, management and comm. **3 states**: Disconnected, Enabled, Disabled. **6 services**: Negotiate, Get config, Link control, Send message, Get (registration) status.	
Network	3		*Null*	
Data Link	2		To provide CRC check, message acknowledgment and local routing.	
Physical	1		Connection through RJ11 jacks between device and communication module.	*Not defined by the standard. Left for implementers.*

Manufacturers and Technologies

Manufacturer	Architecture	WAN	NAN	Security Provider
Itron	OpenWay	GSM, CDMA, Ethernet, WiMax	RFLAN	Certicom Industrial Defender
Elster	EnergyAxis	*WAN agnostic*	EA_LAN	
Landis+Gyr	GridStream	Gridstream PLC	Gridstream RF	RSA
Sensus	FlexNet	FlexNet	FlexNet RF	
GE	Advanced Distribution Infrastructure	RF, PLC, GSM		

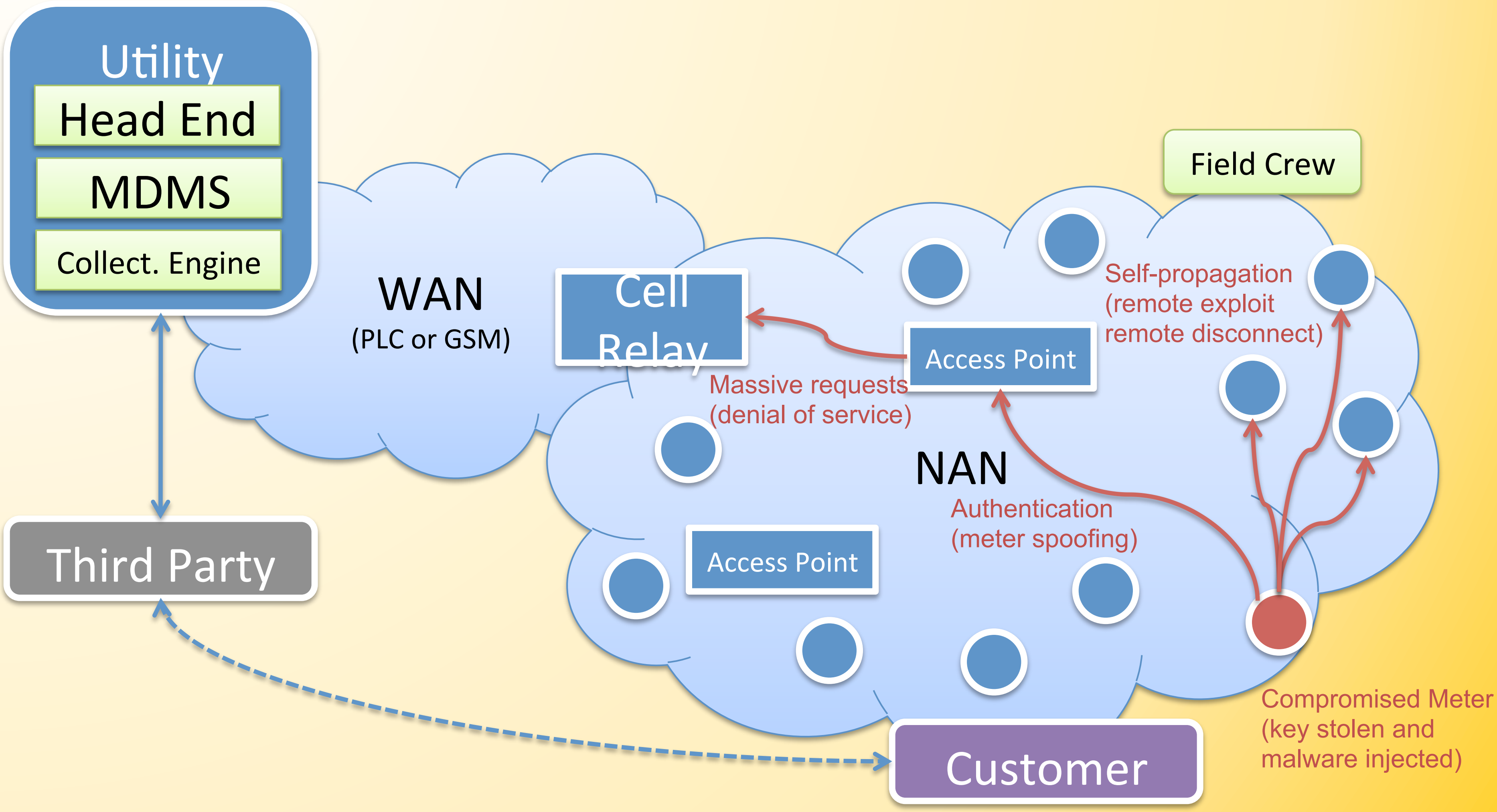
Part 2/3

RISK ANALYSIS

Attack Motivation

- Energy fraud
- Denial of service
  - Extortion
- Power Disruption
  - Outages and instability
- Targeted remote disconnect
- Stealing personal information
- Abuse of communication infrastructure
- Loss of customer trust and adoption

Example of Attack Scenarios



LEGEND: WAN: Wide Area Net., NAN: Neighborhood Area Net., PLC: Power Line Comm., MDMS: Meter Data Management System,

● Smart Meter

TCIPG

AMI Attack Vectors

Attack Techniques	Attack Consequences
Network Compromise	
Communication interception and traffic analysis	Integrity of configuration and routing operations Inconsistent traffic origin or destination
Traffic modification, injection, and replay	Integrity of communication traffic Illegitimate system or network operations Inconsistent traffic origin or destination
System Compromise	
Authorization or authentication violation	Illegitimate system or network operations Inconsistent traffic origin or destination Illegitimate use of credentials
Spoofing of utility system	Illegitimate system or network operations Inconsistent traffic origin or destination
Node compromise, spoofing of metering device	Integrity of node software or hardware Illegitimate system or network operations Inconsistent traffic origin or destination
Denial of Service	
Resource exhaustion	Unresponsive nodes, high bandwidth usage
Signal jamming	Unresponsive nodes, high signal power level
Packet dropping	Integrity of communication traffic

Smart Meter Vulnerabilities

- Communication protocol vulnerabilities
  - Routing
  - Configuration
  - Name service
- Software and firmware vulnerabilities
- Hardware vulnerabilities
- Read and write access to data storage
- Access to encryption keys
- Weak random generator
- Lack of replay protection

Password sent clear over optical port
Usage data not integrity protected

Replaced anti-tampering seal

Password stored in clear in EEPROM

Encryption key derived from password

Replayed authentication and spoofed meter

Multi-vendor Penetration Testing in the Advanced Metering Infrastructure (2010), and *Energy Theft in the Advanced Metering Infrastructure* (2009) by S. McLaughlin et al.

Smart Meter Vulnerabilities (cont.)

- Communication protocol vulnerabilities
  - Routing
  - Configuration
  - Name service
- Software and firmware vulnerabilities
- Hardware vulnerabilities
- Read and write access to data storage
- Access to encryption keys
- Weak random generator
- Lack of replay protection

Inject executable code
Reverse engineer firmware
Guess password by timing
Sniff/inject frames on internal bus
Replace firmware
Jam the radio
Enter a disabled bootloader

Predictable keys can be exploited remotely

Low-level design vulnerabilities in wireless control systems hardware (2009) and *PRNG vulnerability of Z-Stack Zigbee* (2010) by T. Goodspeed et al.

Smart Meter Vulnerabilities (cont.)

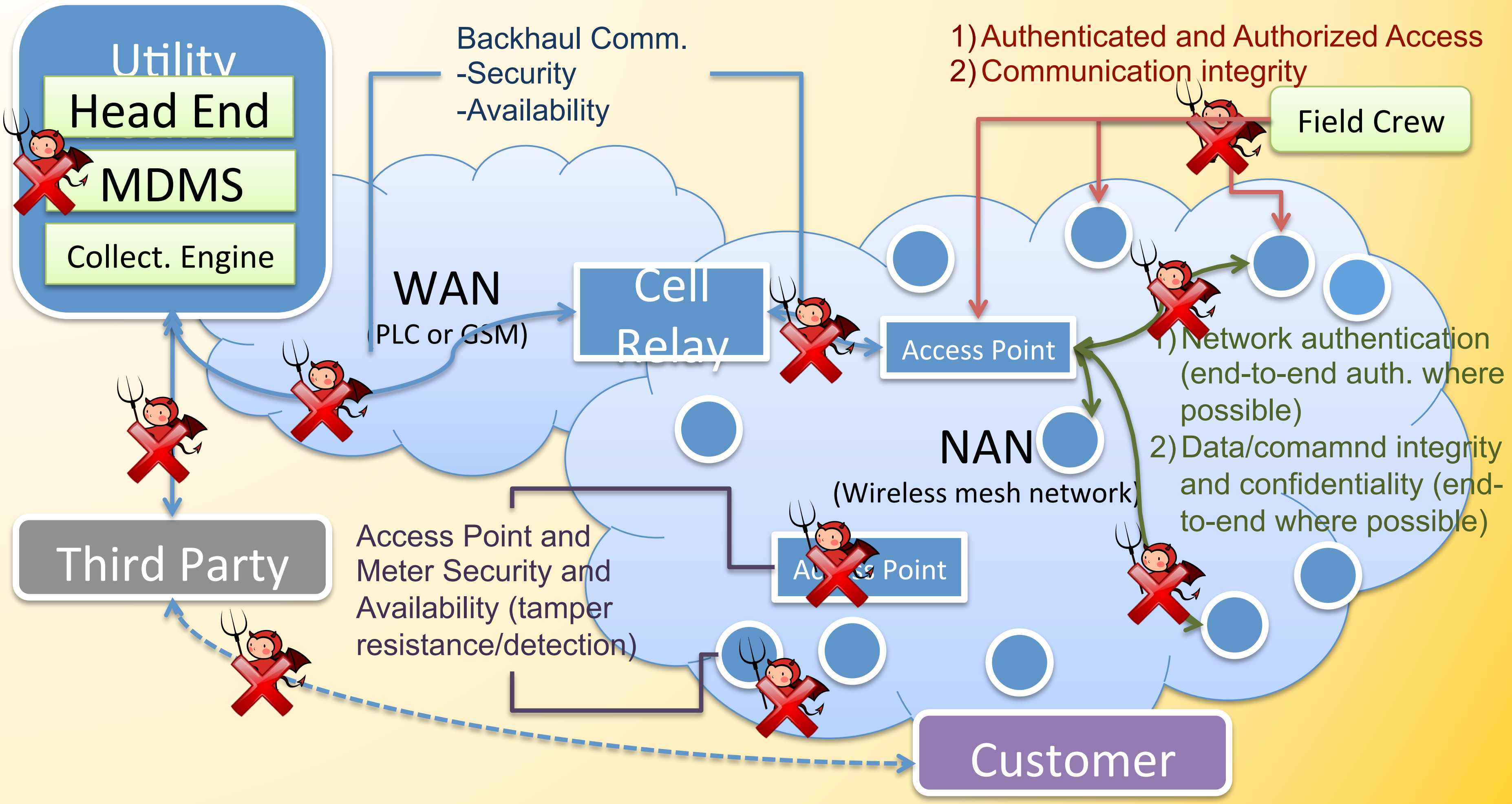
- Communication protocol vulnerabilities
  - Routing
  - Configuration
  - Name service
- Software and firmware vulnerabilities — Local variables promoted to global; Vulnerable to buffer overflow
- Hardware vulnerabilities — Very small stack space, no memory protection; Vulnerable to timing attacks
- Read and write access to data storage — “r/w” flag often disabled
- Access to encryption keys
- Weak random generator
- Lack of replay protection

Smart meter worm developed and tested by IOActive (BlackHat 2009)
Self-replicating and self-propagating code

Part 3/3

SECURING AMI: CHALLENGES AND EFFORTS

Security Controls



Utility

Head End

MDMS

Collect. Engine

Third Party

Backhaul Comm.
-Security
-Availability

WAN
(PLC or GSM)

Cell Relay

1) Authenticated and Authorized Access
2) Communication integrity

Field Crew

Access Point

1) Network authentication (end-to-end auth. where possible)
2) Data/comamnd integrity and confidentiality (end-to-end where possible)

NAN
(Wireless mesh network)

Access Point and Meter Security and Availability (tamper resistance/detection)

Access Point

Customer

LEGEND: WAN: Wide Area Net., NAN: Neighborhood Area Net.,
PLC: Power Line Comm., MDMS: Meter Data Management System,

● Smart Meter

Recent Efforts

- NIST
  - NISTIR 7628
    - A logical architecture with actors in Smart Grid and interfaces between those actors including for AMI
    - High-level security requirements for the identified interfaces including for AMI
    - High-level requirements for key-management systems for the Smart Grid (AMI is implicit)
  - SGIP-PAP00: Meter Upgradeability Standard (by NEMA)
    - Provides requirements for securely upgrading smart meter firmware

Recent Efforts

- ASAP-SG
  - AMI Security Profile (for AMI-SEC (UCAIug) and NIST CSWG)
    - Provides a risk assessment and a catalog of required security controls (based on DHS Catalog of Control System Security)for AMI systems and interfaces.
  - Security Profile for 3rd Party Data Access (for NIST CSWG and SG Security Working group (UCAIug))
    - Defines set of security-centric use-cases and adapts controls form DHS Catalog of Control System Security.

Conclusions

- Large set of suggestions & requirements available
  - NISTIR & AMI-SEC: security requirements for every interface
  - Academic publications on AMI security
- Issues are:
  - System specific: how to apply standards?
  - Optimization: how to select the right cost/security tradeoff?
  - Complexity: how to keep security manageable and solutions interoperable?
- Importance of a security process applied to AMI
  - Defining the right security environment
  - Implementing security by design
  - Constant monitoring and validation of security solutions

Outline

- Background:
  - Overview of Electrical Power System Basics
    - "Big Wire"
    - IT Infrastructure ("Little Wire")
  - IT Infrastructure Threats
- Research Challenges:
  - Wide Area Measurement Systems
  - Advanced Metering Infrastructures (AMI)
- Research Directions
  - TCIPG Overview

Smart Grid Security Efforts @ Illinois

TCIPG

TCIPG: Trustworthy Cyber Infrastructure for the Power Grid

- Drive the design of an resilient cyber infrastructure electric power which operates through attacks
- $18.8 M over five year, started Oct. 1, 2010
- Univ. Illinois, Cornell, Dartmouth, U.C. Davis, Wash. State Univ.
- Funded by DOE and DHS
- Follow-on to $7.5 M NSF CyberTrust Center

ADSC

Ilinois's Singapore Adv. Digital Sciences Center Smart Grid Subprogram

~$15M effort / 5 years

Projects in Microgrids, DERs, and HANs

ETRI

Korean National Smart Grid TestBed on Jeju Island.

Project concerning tesbed and cyber security research (DDSOS)

CACAIS

Testbed

Products tested & validated in CACAIS testbed: $1.2M FY10 funding from ONR

Illinois Center for a Smarter Electric Grid

Validation & Compliance Services

- $2.5M, YR1 DCEO funding
- Test bed & lab equipped with HW/SW to perform validation of Smart Grid systems
- Critical Infrastructure Protection (CIP): pre-audit check for compliance to NERC standards
- Prepare for NERC reliability compliance audits

4 New DOE Office of Electricity Security Projects with:

EPRI ELECTRIC POWER RESEARCH INSTITUTE

Entergy THE POWER OF PEOPLE

GRID PROTECTION ALLIANCE

DTE Energy

Telcordia

EPRI ELECTRIC POWER RESEARCH INSTITUTE

Pacific Northwest NATIONAL LABORATORY

pjm

GRID PROTECTION ALLIANCE

ALSTOM

Honeywell

INL

TCIPG

tcipg.org

TCIPG Vision & Research Focus

Vision: Drive the design of an adaptive, resilient, and trustworthy cyber infrastructure for transmission & distribution of electric power, which operates through attacks

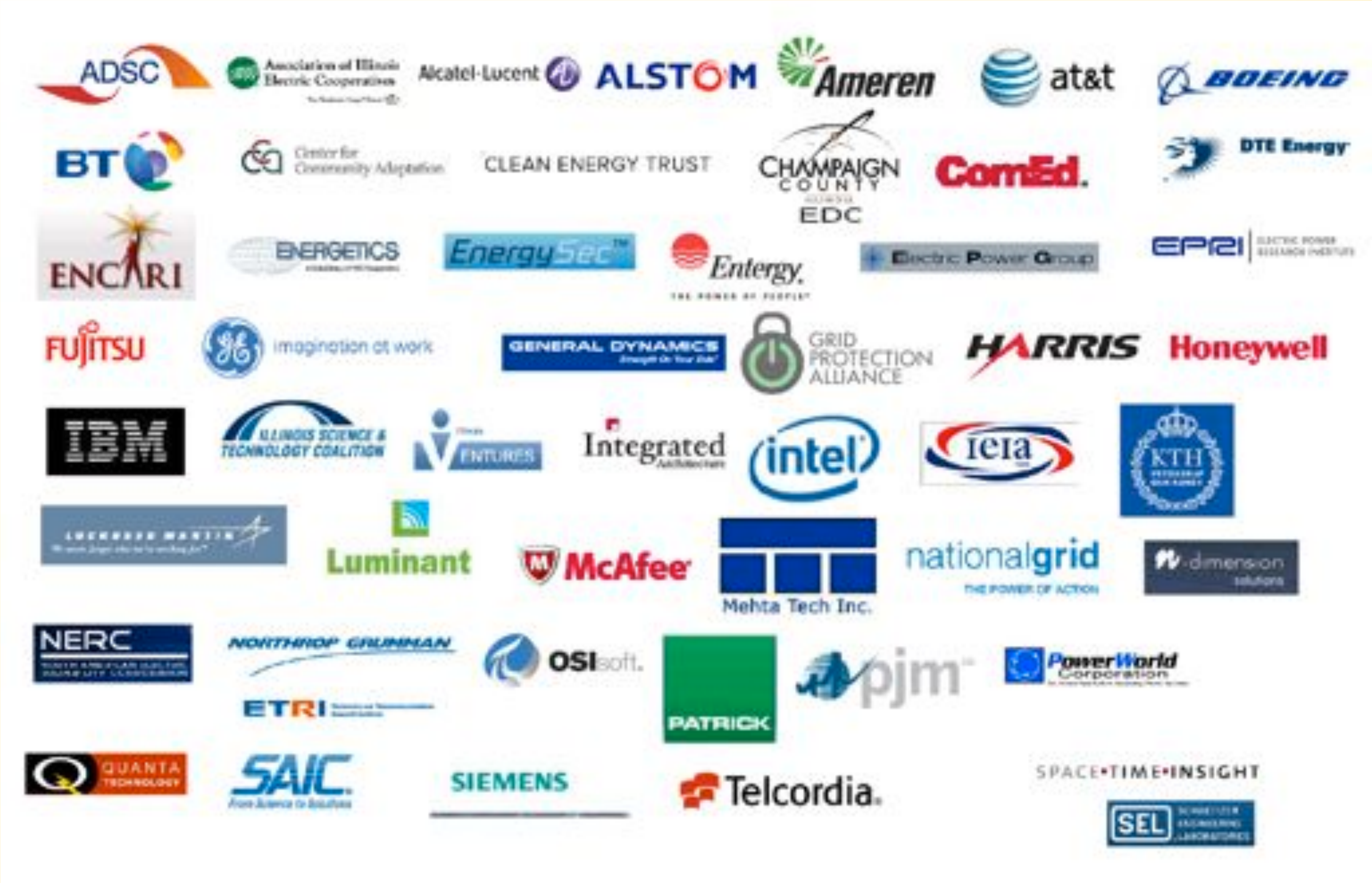
Research focus: Resilient and Secure Smart Grid Systems

- Protecting the cyber infrastructure
- Making use of cyber and physical state information to detect, respond, and recover from attacks
- Supporting greatly increased throughput and timeliness requirements for next generation energy applications
- Quantifying security and resilience

TCIPG Statistics

- Build upon $7.5M NSF TCIP CyberTrust Center 2005-2010
- $18.8M over 5 years, starting Oct 1, 2009
- Funded by Department of Energy, Office of Electricity and Department of Homeland Security
- 5 Universities
  - University of Illinois at Urbana-Champaign (20 Senior Investigators, 24 Graduate students)
  - Washington State University (5 Senior Investigators, 3 Graduate students)
  - University of California at Davis (2 Senior Investigators, 1 Graduate student)
  - Dartmouth College (2 Senior Investigators, 1 Graduate student)
  - Cornell University (1 Senior Investigator)

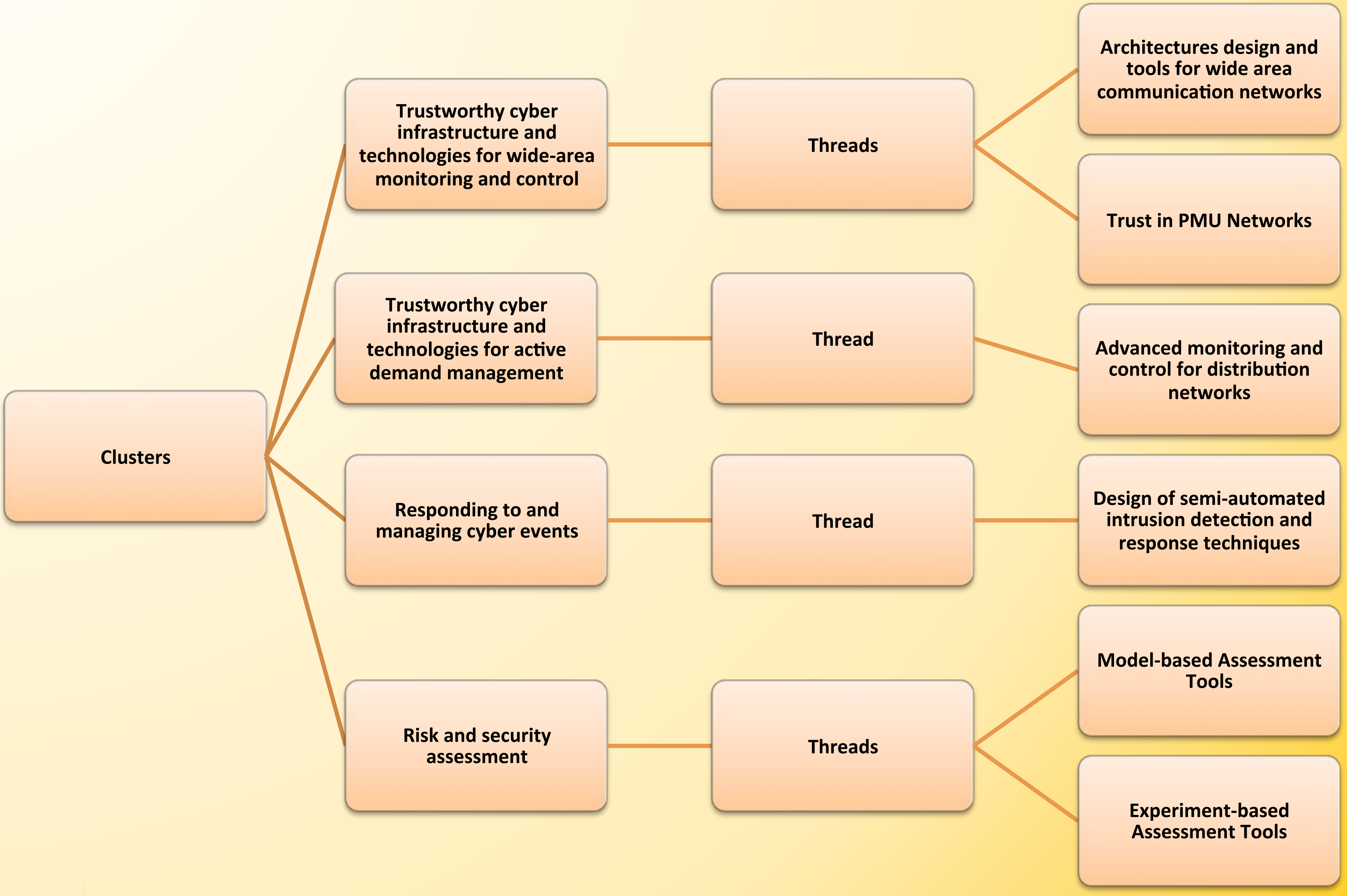
TCIPG Industry Interaction Board



TCIPG Clusters and Cross-Cutting Efforts

- Clusters integrate work in specific technical areas over the life of the project:
  - Trustworthy cyber infrastructure and technologies for wide-area monitoring and control
  - Trustworthy cyber infrastructure and technologies for active demand management
  - Responding to and managing cyber events
  - Risk and security assessment
- Cross-Cutting Efforts address issues that cross technical clusters:
  - Education and workforce development
  - Testbed and evaluation methodologies
  - Industry interactions and technology transition

TCIPG Technical Clusters and Threads


Clusters
Trustworthy cyber infrastructure and technologies for wide-area monitoring and control
Threads
Architectures design and tools for wide area communication networks
Trust in PMU Networks
Trustworthy cyber infrastructure and technologies for active demand management
Thread
Advanced monitoring and control for distribution networks
Responding to and managing cyber events
Thread
Design of semi-automated intrusion detection and response techniques
Risk and security assessment
Threads
Model-based Assessment Tools
Experiment-based Assessment Tools

Breadth of TCIPG Research Activities

Cluster: Trustworthy cyber infrastructure and technologies for wide-area monitoring and control

- Secure Wide-Area Data and Communication Networks for PMU-based Power System Applications
- Real-time, Secure, and Converged Power Grid Cyber Networks
- Cooperative Congestion Avoidance in Power Grid Networks
- Direct Application of PMU Values into Power Flow Software
- GridStat Middleware Communication Framework: Application Requirements, Management Security, and Trust
- Lossless Compression of Syncrhophasor Measurement Data Archives
- Decentralized Sensor Networking Models and Primitives for the Smart Grid

Cluster: Trustworthy cyber infrastructure and technologies for active demand management

- Smart-Grid-Enabled Distributed Voltage Support
- Specification-based IDS for Smart Meters
- Development of the Information Layer for the V2G Framework Implementation
- Non-Intrusive Load Monitoring
- Agent Technologies for Active Control Applications in the Power Grid
- Development of the Information Layer for the V2G Framework Implementation

Breadth of TCIPG Research Activities

Cluster: Responding to and managing cyber events

- RRE: A Game-Theoretic Response and Recovery Engine
- Assessment and Forensics for Large-Scale Smart Grid Networks
- Coordinating Black Start Operations Using Synchrophasors

Cluster: Risk and security assessment

- Trustworthiness Enhancement Tools for SCADA Software and Platforms
- Tools for Assessment and Self-assessment of ZigBee Networks
- Analysis of Impacts of Smart Grid Resources on Economics and Reliability of Electricity Supply
- Vulnerability Assessment Tool Using Model Checking
- Test-bed-Driven Assessment: Experimental Validation of System Security and Reliability
- Modeling Methodologies for Power Grid Control System Evaluation
- Automatic Verification of Network Access Control Policy Implementations
- Quantifying the Impacts on Reliability of Coupling between Power System Cyber and Physical Components
- Towards Robust Power System Applications

TCIPG Testbed Effort

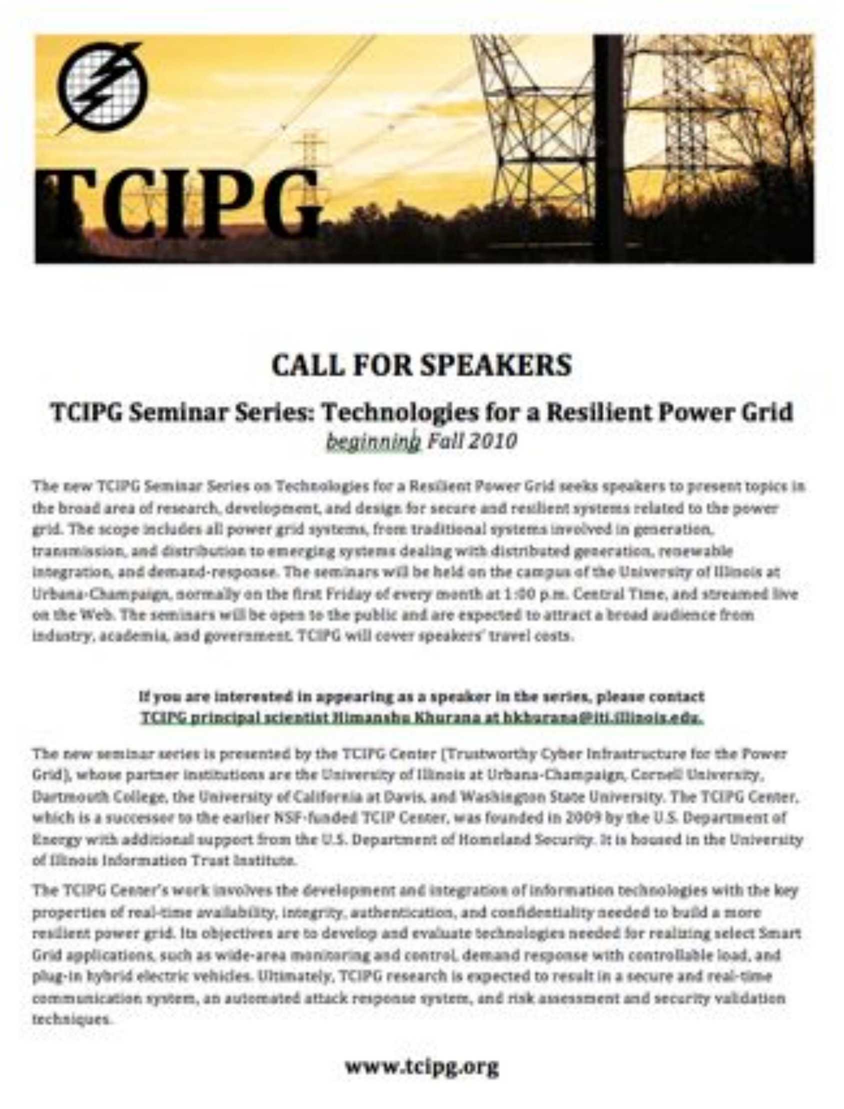
- TCIPG testbed aims to:
  - Provide experimental support and integration of TCIPG projects
  - Serve as national resource for experimental work in analysis of power grid system resiliency
- Testbed capabilities:
  - Equipment
    - Commercial Hardware and Software
    - Transmission, Distribution, Generation, and Home automation/ control
  - Scalable simulation and emulation
    - Simulation of power generation/transmission, simulation/ emulation of computer and communication systems
  - Coupling
    - Integration of simulation of electrical state, real equipment and cyber simulation/emulation of other grid components

TCIPG Summer School June 13-17, 2011

Tom Malec of the U.S. Department of Energy addresses the Summer School attendees.

TCIPG Webcasts: Technologies for a Resilient Power Grid

- Present topics on research, development, and design of a secure and resilient power grid
- Webcasts are open to the public and attract a broad audience from industry, academia, and government
- Webcast first Friday of each month at 1:00 p.m. CT
- Speakers so far:
  - Sept.: Manimaran Govindarasu, Iowa State
  - Oct.: Mathew Luallen, Sph3r3
  - Nov.: Alan Greenberg, Boeing, & Mark Enstrom, Neustar
  - Dec.: Robert Former, ITRON



TCIPG

CALL FOR SPEAKERS

TCIPG Seminar Series: Technologies for a Resilient Power Grid
beginning Fall 2010

The new TCIPG Seminar Series on Technologies for a Resilient Power Grid seeks speakers to present topics in the broad area of research, development, and design for secure and resilient systems related to the power grid. The scope includes all power grid systems, from traditional systems involved in generation, transmission, and distribution to emerging systems dealing with distributed generation, renewable integration, and demand-response. The seminars will be held on the campus of the University of Illinois at Urbana-Champaign, normally on the first Friday of every month at 1:00 p.m. Central Time, and streamed live on the Web. The seminars will be open to the public and are expected to attract a broad audience from industry, academia, and government. TCIPG will cover speakers' travel costs.

If you are interested in appearing as a speaker in the series, please contact TCIPG principal scientist Himanshu Khurana at hkhurana@iti.illinois.edu.

The new seminar series is presented by the TCIPG Center (Trustworthy Cyber Infrastructure for the Power Grid), whose partner institutions are the University of Illinois at Urbana-Champaign, Cornell University, Dartmouth College, the University of California at Davis, and Washington State University. The TCIPG Center, which is a successor to the earlier NSF-funded TCIP Center, was founded in 2009 by the U.S. Department of Energy with additional support from the U.S. Department of Homeland Security. It is housed in the University of Illinois Information Trust Institute.

The TCIPG Center's work involves the development and integration of information technologies with the key properties of real-time availability, integrity, authentication, and confidentiality needed to build a more resilient power grid. Its objectives are to develop and evaluate technologies needed for realizing select Smart Grid applications, such as wide-area monitoring and control, demand response with controllable load, and plug-in hybrid electric vehicles. Ultimately, TCIPG research is expected to result in a secure and real-time communication system, an automated attack response system, and risk assessment and security validation techniques.

www.tcipg.org

Outline

- Background:
  - Overview of Electrical Power System Basics
    - “Big Wire”
    - IT Infrastructure (“Little Wire”)
  - IT Infrastructure Threats
- Research Challenges:
  - Wide Area Measurement Systems
  - Advanced Metering Infrastructures (AMI)
- Research Directions
  - TCIPG Overview