GIAN Short course

Cyber-Physical Security for the Smart Grid

Indian Institute of Technology, Bombay, India

Coordinator: Prof. R. K. Shyamasundar

Manimaran Govindarasu

Dept. of Electrical and Computer Engineering

Iowa State University

Email: gmani@iastate.edu

http://powercyber.ece.iastate.edu

March 5-16, 2018

Course Agenda

Day 01	• Module 1: Cyber Threats, Attacks, and Security concepts
Day 02	• Module 2: Risk Assessment and Mitigation & • Overview of Indian Power Grid
Day 03	• Module 3: Attack-resilient Wide-Monitoring, Protection, Control
Day 04	• Module 4: SCADA, Synchrophasor, and AMI Networks & Security
Day 05	• Module 5: Attack Surface Analysis and Reduction Techniques
Day 06	• Module 6: CPS Security Testbeds & Case Studies
Day 07	• Module 7: Cybersecurity Standards & Industry Best Practices
Day 08	• Module 8: Cybersecurity Tools & Vulnerability Disclosure
Day 09	• Module 9 : Review of materials, revisit case studies, assessments
Day 10	• Module 10: Research directions, education and training

Module 4:
SCADA, Syhchrophasor, and AMI Networks and Security

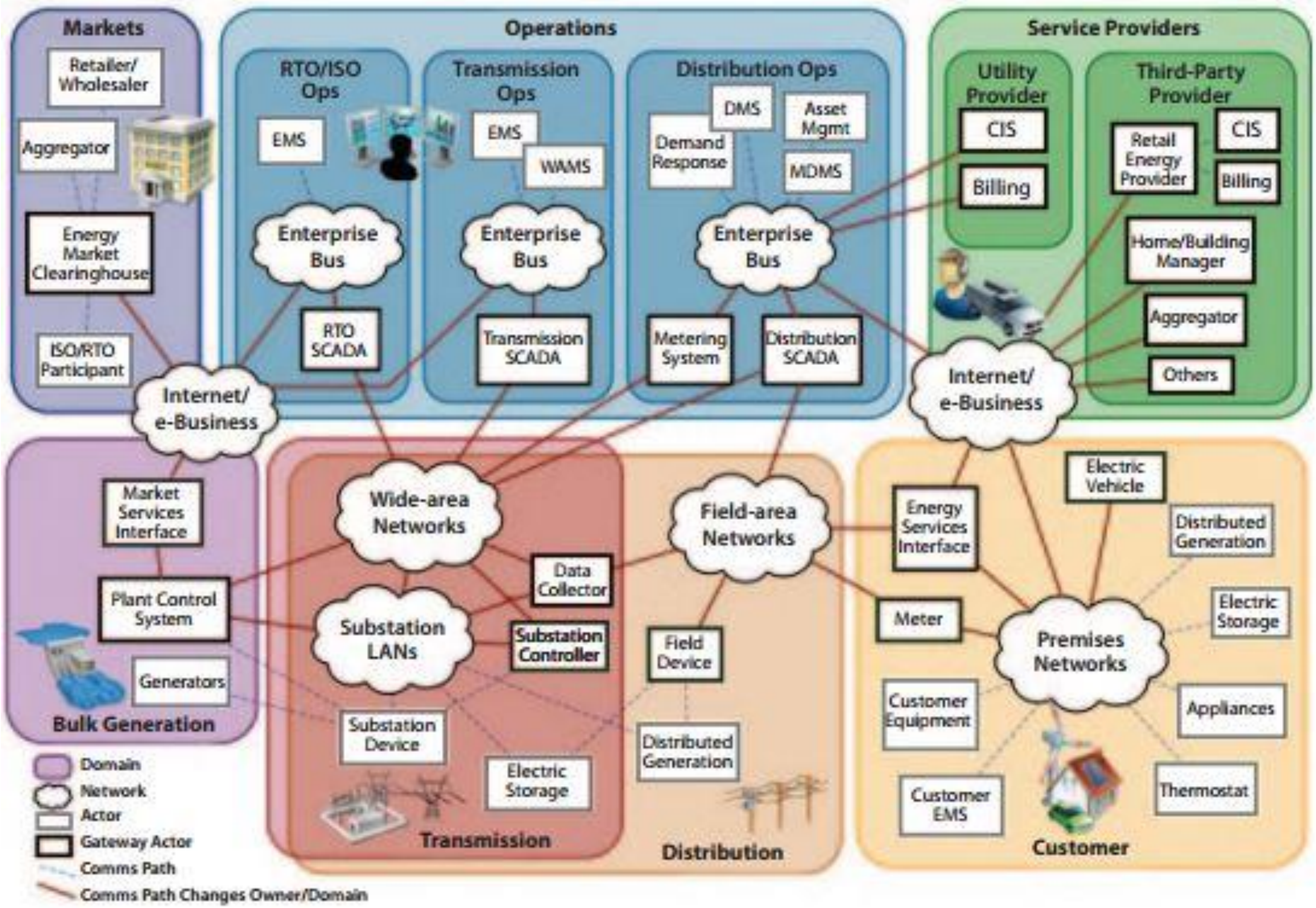
- SCADA Protocols – DNP3, ICCP, IEC 61850
- Synchrophasor (PMU) network, NASPInet and security
- AMI Security and Privacy

SCADA Protocols:

DNP3, ICCP, IEC 61850

NIST SGIP Smart Grid schematic

"The Future of the Electric Grid" MIT Report



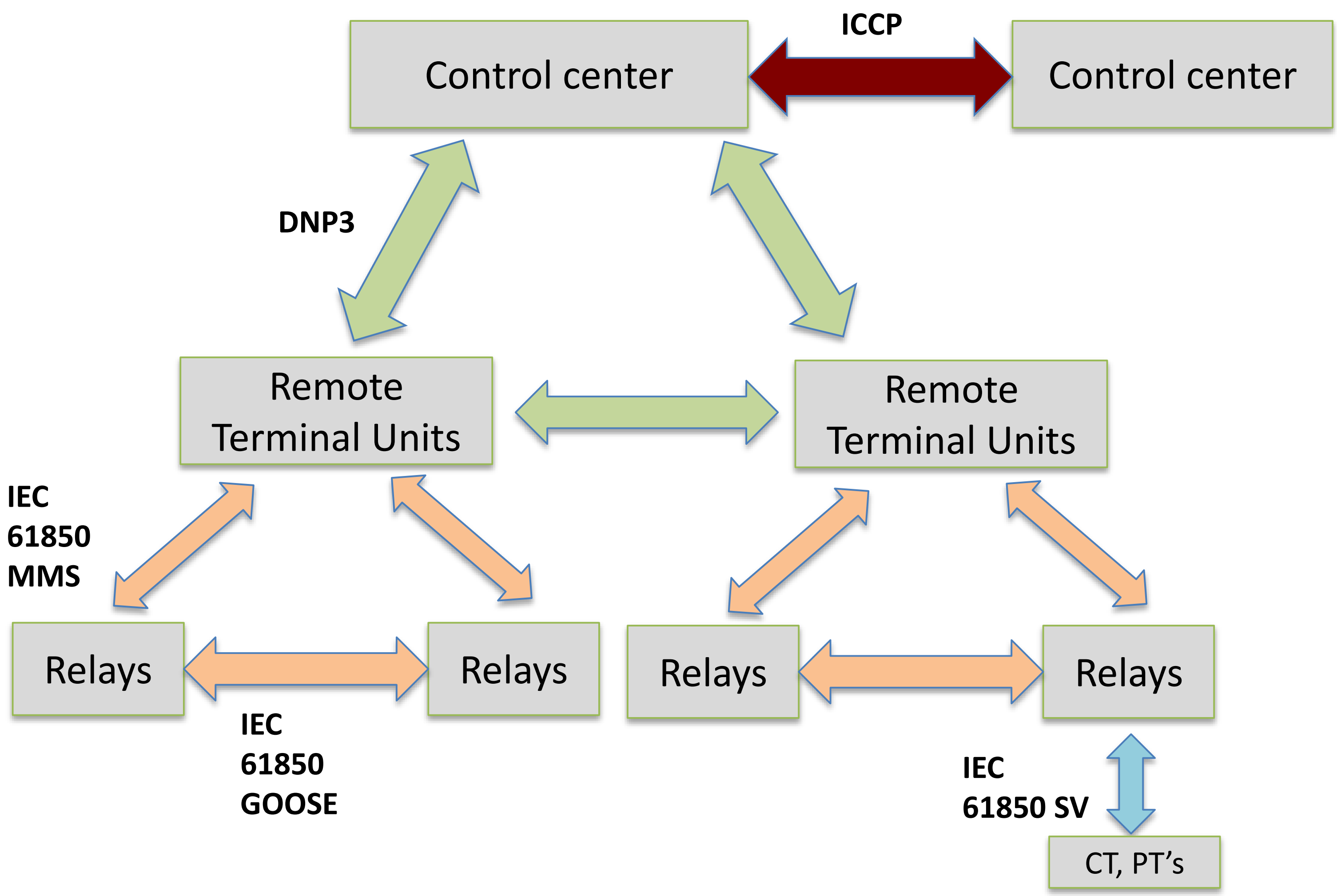
Changes to Current Grid

- Blurring the distinctions between the generator and the consumer
- Point-to-point and one-way communication networks is being replaced by two-way communication networks
- Network capacity is being increased
- High data rate and storage capacity
- Efficiency and reliability of the network must increase (reduced latency)
- Advanced monitoring systems

Potential Protocols
(source: “The Future of the Electric Grid” MIT)

Application	Media	Standard/ Protocol	Network Requirements: Expected Data Rate/Bandwidth[a]	Acceptable Latency[a]	Frequency of Use[b]	Reliability Need[a]	Security Need[a]	Backup Power[a]
Home-area Network	Power line communications,[c] wireless	HomePlug, ZigBee, IP						
Advanced Metering Infrastructure (AMI)*	Power line communications,[c,d] wireless radio frequency,[e,f] T1, microwave, broadband (via fiber, cable, digital subscriber line), commercial wireless[g]	For backhaul: WiMAX, LTE For appliance to meter: IEEE 802.15.4,[h] ZigBee[g]	10–100 kilobytes/ second (kbps)/ node, 500 kbps for backhaul	2–15 seconds	5–15 minutes/ node	99–99.99%	High	Not necessary
Demand Response (Part of AMI)	Same as AMI	Same as AMI	14 kbps–100 kbps/ node or device	500 milliseconds (ms)– several minutes	35 days/ year	99–99.99%	High	Not necessary
Electric Transportation	Power line communications[i] wireless[h]	ZigBee, IEEE 802.15.4[h]	9.6–56 kbps, 100 kbps is a good target	2 seconds– 5 minutes	Daily	99–99.99%	Relatively high	Not necessary
Distribution Grid Management	Fiber, wireless,[j] satellite, cellular[g]	DNP3 (IEEE 1815), IEC 61850/ GOOSE,[k] WiMAX, LTE,[j] IP,[g] IEEE 802.15.4[h]	9.6–100 kbps	100 ms– 2 seconds	Continuous	99–99.999%	High	24–72 hours
Distributed Energy Resources and Storage	Fiber, wireless,[j] microwave, satellite[g]	DNP3, IEC 61850/ GOOSE[k] WiMAX, LTE,[j] ZigBee,[g] IEEE 802.15.4[h]	9.6–56 kbps	20 ms– 15 seconds	Continuous	99–99.99%	High	1 hour
Wide-area Situational Awareness (synchro-phasors[#])	SONET, ATM, Frame Relay, MPLS,[f,g] fiber, microwave, broadband over power line[g]	C37.118, IEC 61850/ GOOSE,[k] IP[h,l]	600–1,500 kbps	20 ms–200 ms	Continuous	99.999– 99.9999%	High	24-hour supply
Interutility communications (Southern California Edison)	Fiber, microwave, wired	ICCP[k]	> 45 megabytes/ second (mbps)	<50 ms (DS-3)	Continuous	99.999– 99.9999%	High	24-hour supply
Interregional data communications (ISO New England)	Standard telco T1 circuits with copper endpoints (NERCNet)	IP	256 kbps	20–200 ms	Continuous	99.999%	High	24-hour supply
Market data communications (ISO New England)	Wired	IP	18 mbps + 45 mbps connections	20–200 ms	Continuous	99.999%	Relatively high	24-hour supply

SCADA communication Protocols - An overview



ICCP

ICCP– Inter-Control Center Communications Protocol – used primarily for communications between the control centers, power plants to exchange real-time data.

•Originally developed by Utility Communications Specification Working Group

•ICCP uses the client/server model.

•Maximizes use of existing standard protocols in all layers of OSI 7 layer reference model.

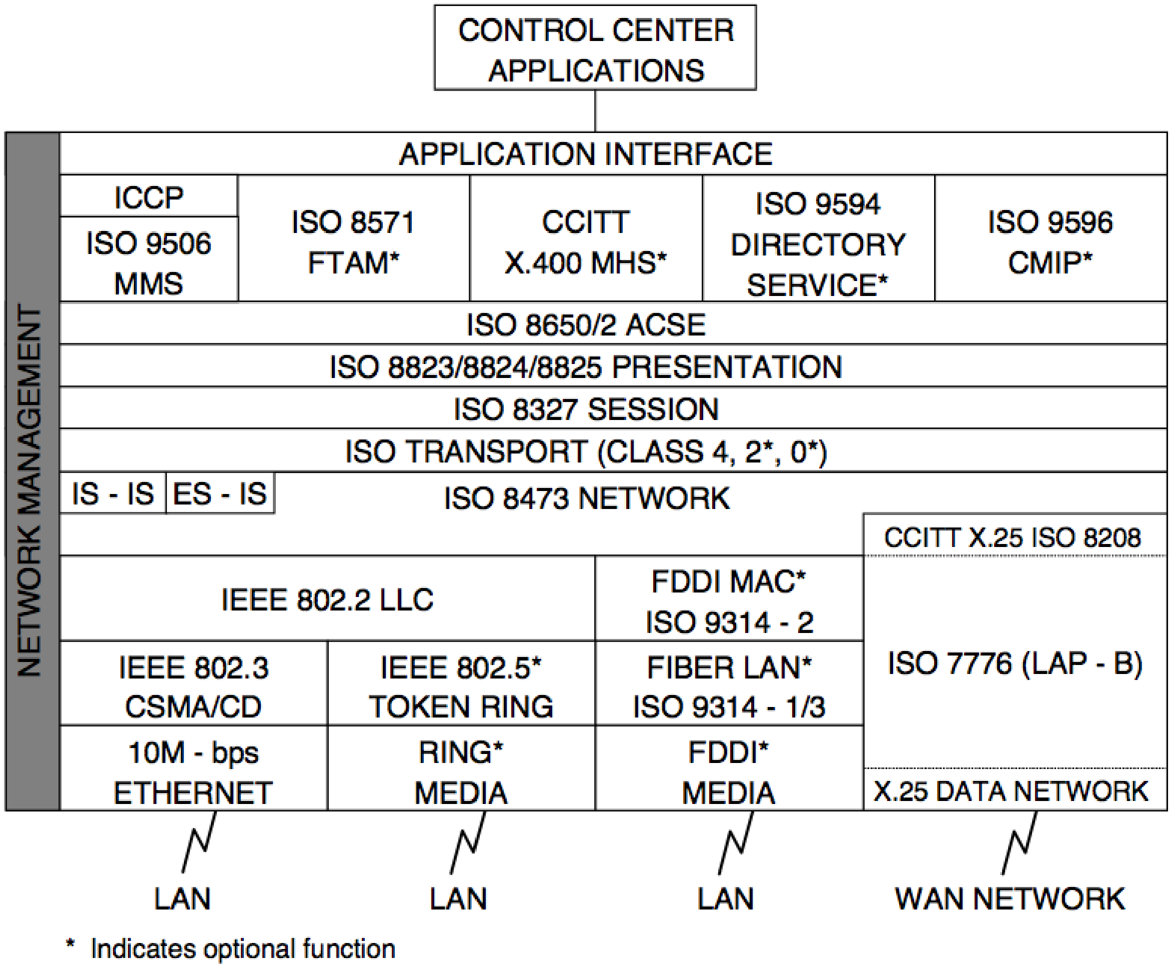
•ICCP uses *Manufacturing Message Specification* (MMS) for messaging services.

•Control center applications use an *Application Programming Interface* (API) to exchange real-time data in ICCP.

Source: ICCP User Guide, Prepared by Electric Power Research Institute (EPRI), February 1996.

ICCP

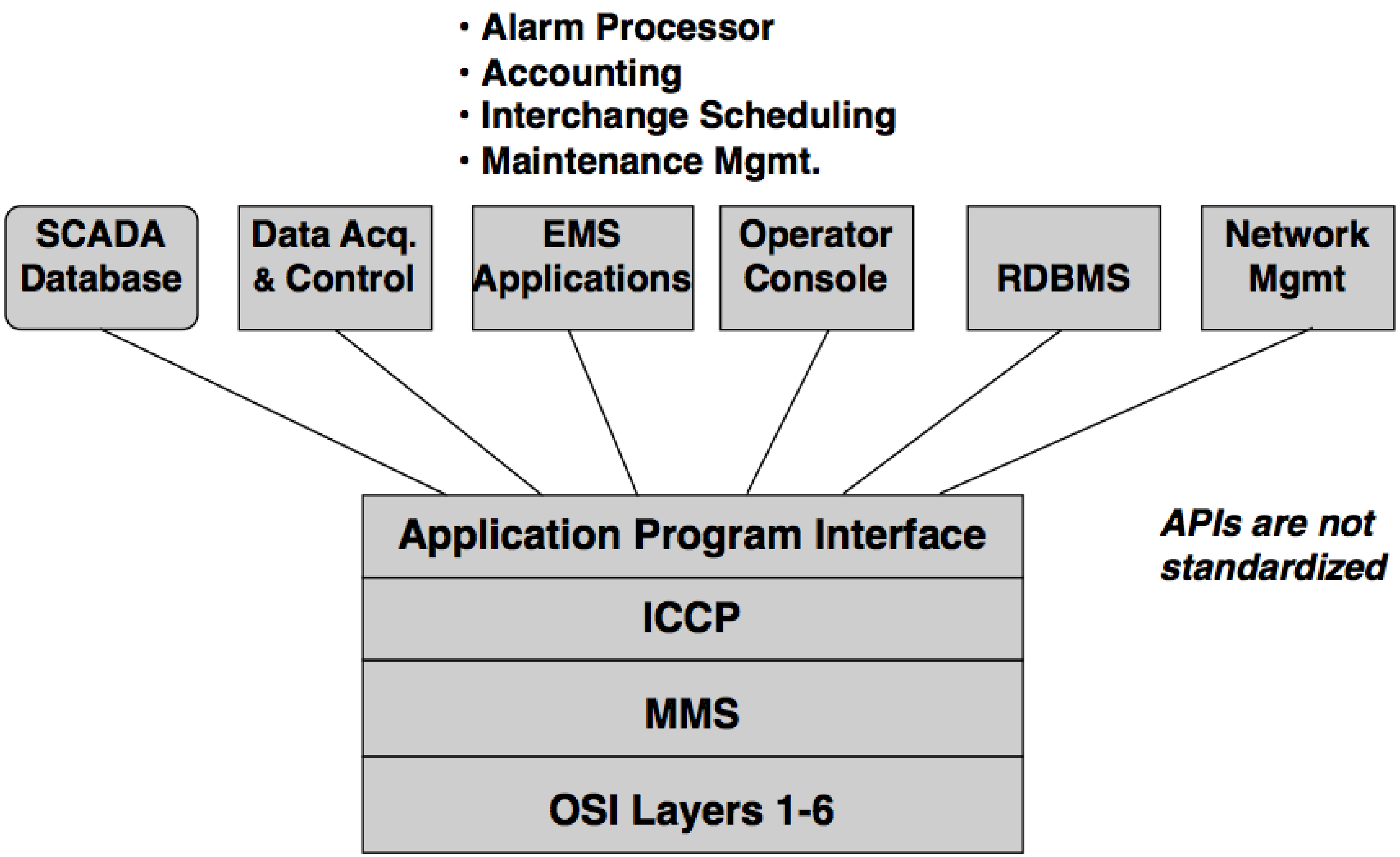
Protocol Architecture



Source: ICCP User Guide, Prepared by Electric Power Research Institute (EPRI), February 1996.

ICCP

Application Programming Interface (API)



Source: ICCP User Guide, Prepared by Electric Power Research Institute (EPRI), February 1996.

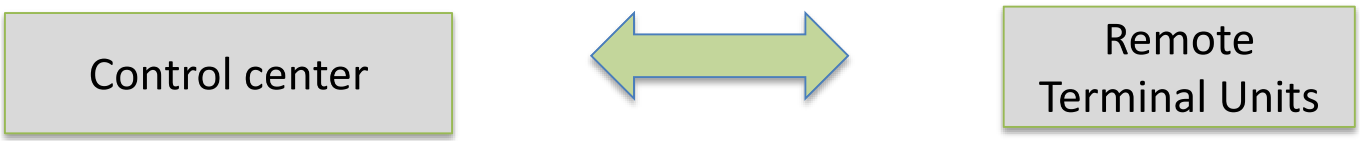
DNP3

DNP3 – Distributed Network Protocol 3.0 – used primarily for communications between the control center and Remote Terminal Units in substations.

Master/slave protocol (client/server model)

Originally developed as a serial protocol and extended to work over IP, encapsulated in TCP/UDP.

DNP3 Master (client) **DNP3 Slave (master)**



DNP3 application layer uses *requests* and *response* messages.

Application Control	Function Code	Internal Indications	
		LSB	MSB

DNP3 Application header

Secure DNP3 protocol was introduced in 2007.
Security related function code and authentication added to application layer.

Source: http://www.digitalbond.com/scadapedia/protocols/dnp3/

IEC 61850

IEC 61850–Communications for power system automation – Developed by the IEC working group TC 57– used primarily for communications between field devices like relays, and between relays and substation RTU's.

Developed for interoperability and standardization.

Based on client/server model and uses Ethernet and TCP/IP networking.

Object oriented substation automation standard that includes

- Standardized names
- Standardized meaning of data
- Standardized abstract services
- Standardized behavior models

Mapping of these abstract services and models to specific protocols for

- Control and Monitoring (MMS)
- Protection (GOOSE)
- Transducers (SV)

Source: IEC 61850 Tutorial, IEC 61850 users group, November 15, 2011, UCAlug Summit Meeting, Austin, TX.

IEC 61850

IEC 61850–6 describes *Substation Configuration Language* (SCL) – a standardized method of describing Substation topologies and protection device configurations.

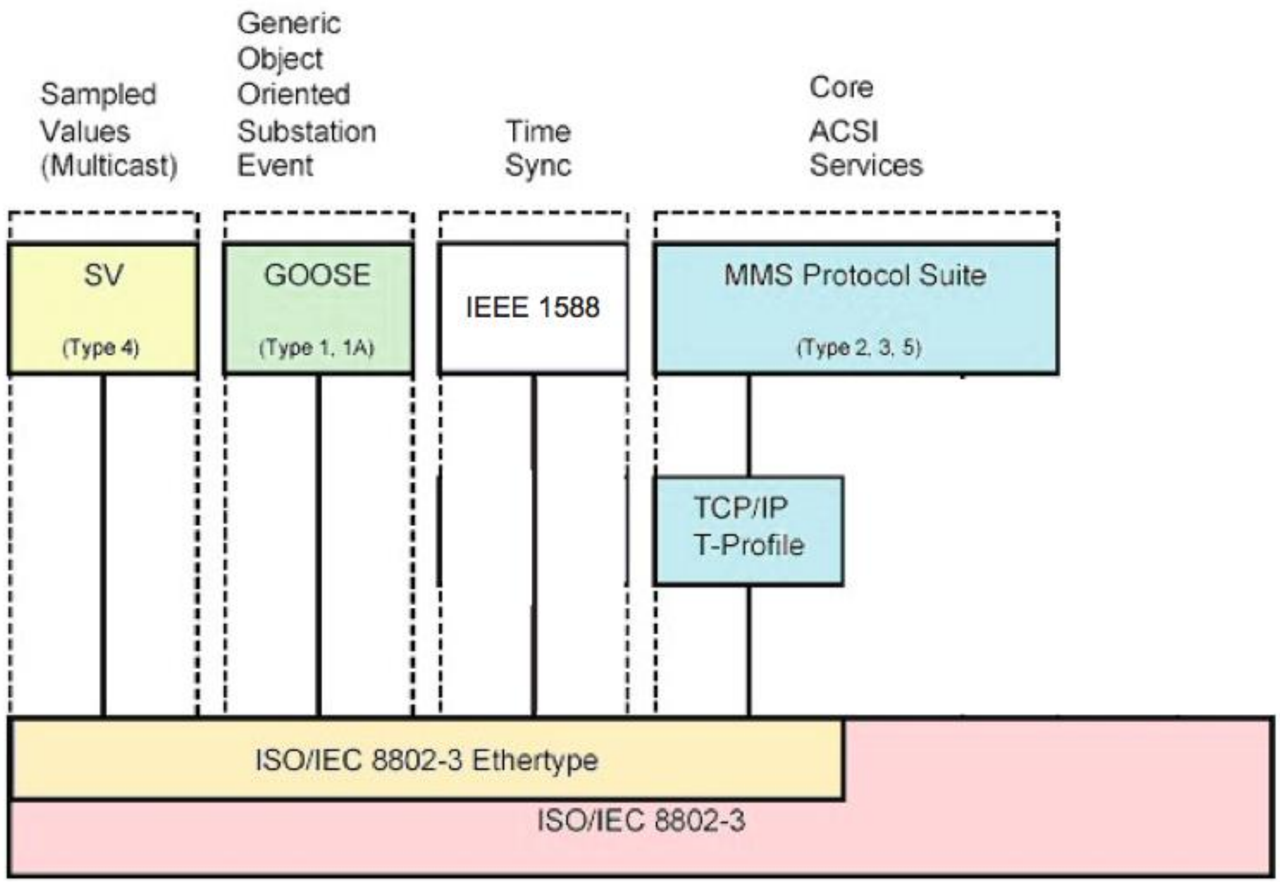
IEC 61850-7-1 & 8-1 describes *Generic Object Oriented Substation Events* (GOOSE) –a mechanism of transferring event data over substation networks using multicasts or broadcasts for performing protection functions.

IEC 61850-9-2 describes *Sampled Values* (SV) – a mechanism that supports distribution of time sampled data such as measurements, status, and other I/O signals over a separate “process bus”.

Source: IEC 61850 Tutorial, IEC 61850 users group, November 15, 2011, UCAlug Summit Meeting, Austin, TX.

IEC 61850

IEC 61850 profiles mapping to OSI model



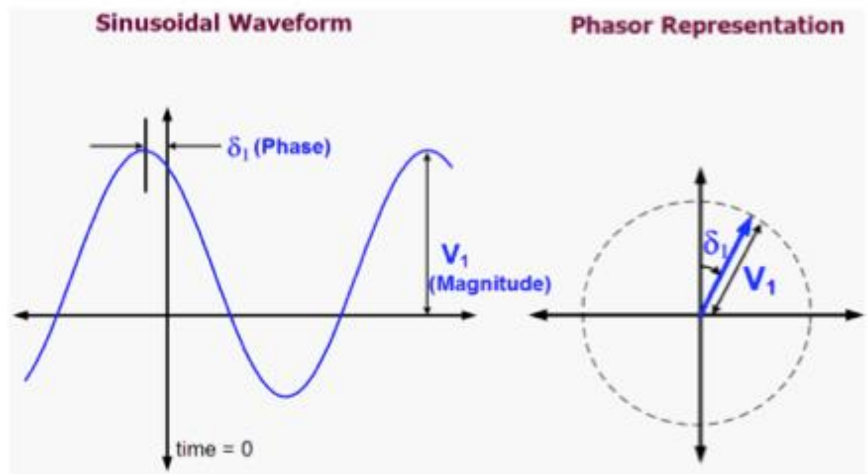
Source: IEC 61850 Tutorial, IEC 61850 users group, November 15, 2011, UCAlug Summit Meeting, Austin, TX.

Synchrophasor Network, NAPSInet & Security

Synchrophasors

Phasors:

- Magnitude
- Angle



Synchrophasors:

- Common measurement time-stamp using GPS

SCADA vs. PMU data

SCADA data:

- **Voltage & Current Magnitudes**
- **Frequency**
- **Every 2-4 seconds**

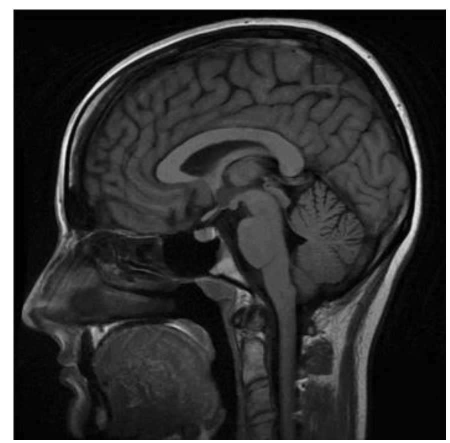
PMU data:

- **Voltage & Current phase angles**
- **Rate of change of frequency**
- **Time synchronized (using GPS) and**
- **Every 30 -120 times per second**

SCADA vs. PMU data

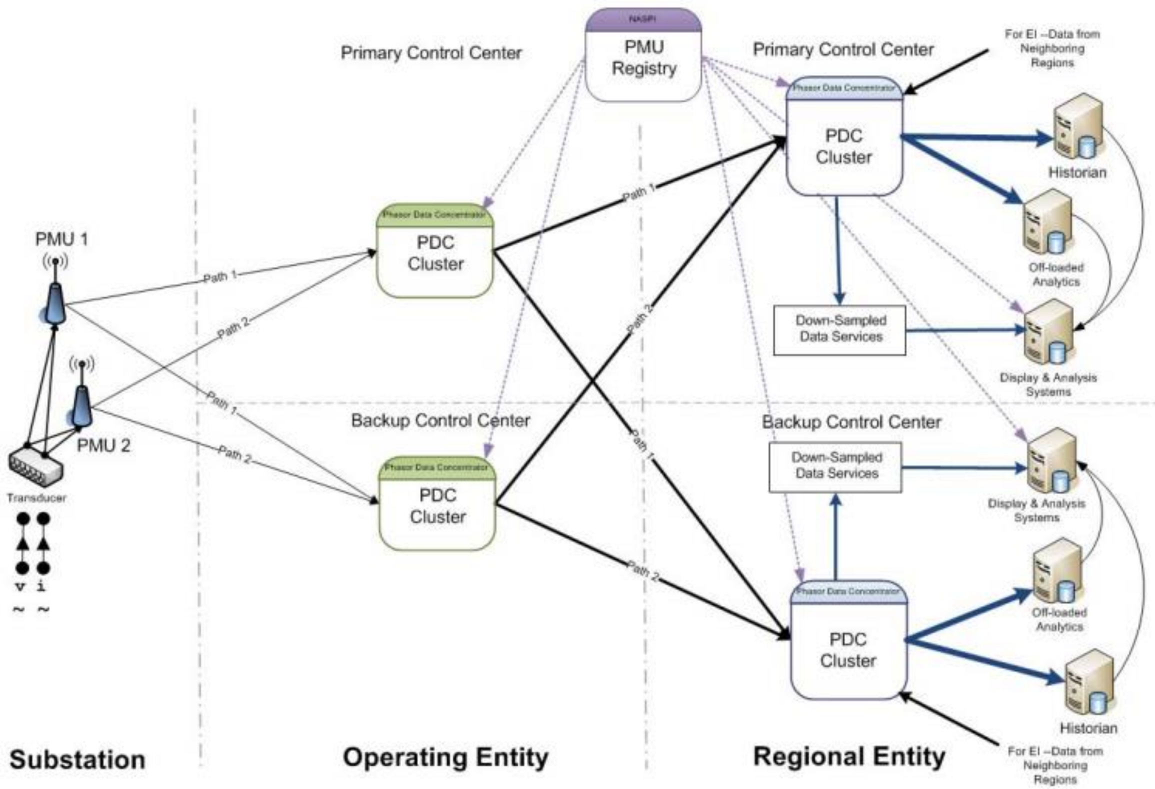
- SCADA data:
  - Voltage & Current
    - **Magnitudes**
  - Data rate
    - **Every 2-4 seconds (per sample)**
- PMU data:
  - Voltage & Current
    - Magnitudes
    - Phase angles
  - Frequency
  - Rate of change of frequency
  - Time synchronized (using GPS Satellite)
  - Data rate
    - **30 -120 samples per second**

SCADA DATA



PMU DATA

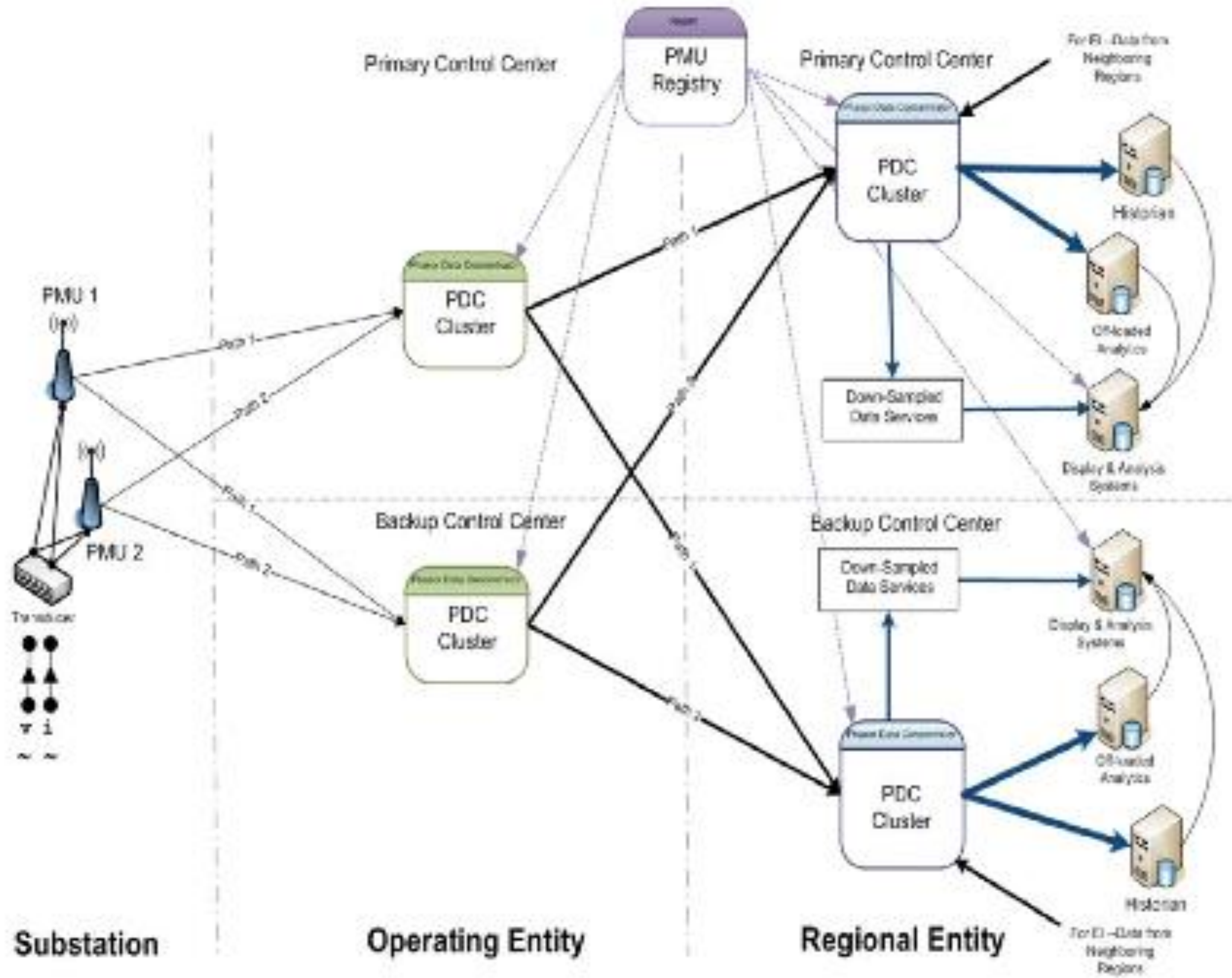
Synchrophasor Network Architecture



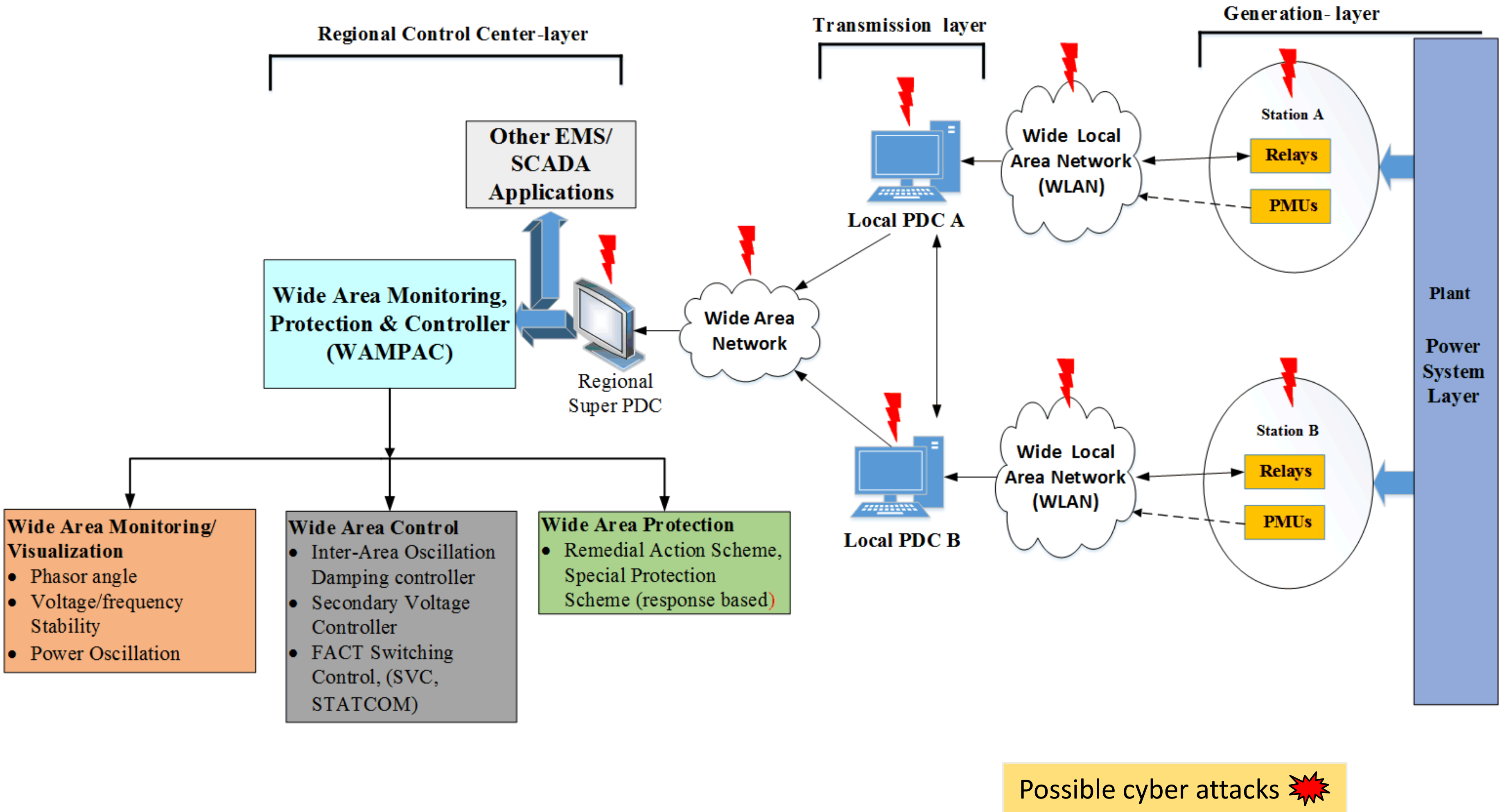
A Generic Architecture of a Synchrophasor Network

PMU measurement infrastructure

- PMUs to local PDC
- PDCs to control center
- PDC clusters to control center for data processing & archiving



Attack Surface in Synchrophasor WAMPAC

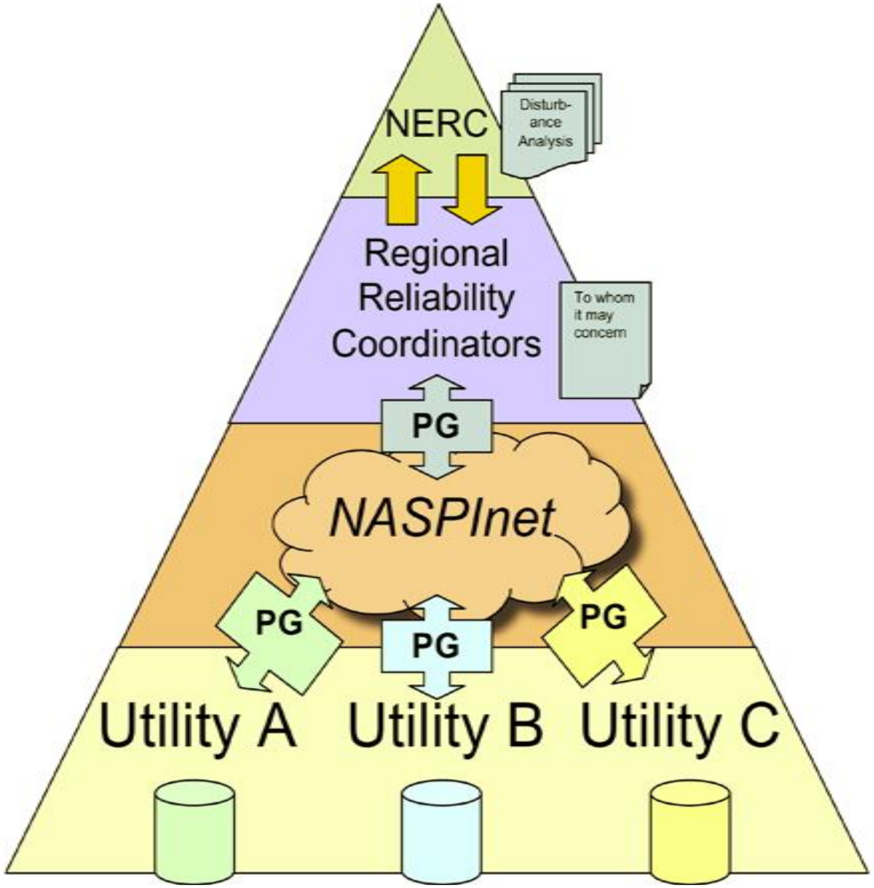


Wide Area Monitoring - NASPI

- *NASPI:* North American Synchrophasor Initiative

- *NASPI Network (NASPInet) is an effort* ***to develop an "industrial grade," secure, standardized, distributed, and expandable data communications infrastructure to support synchrophasor applications in North America.***

https://www.naspi.org

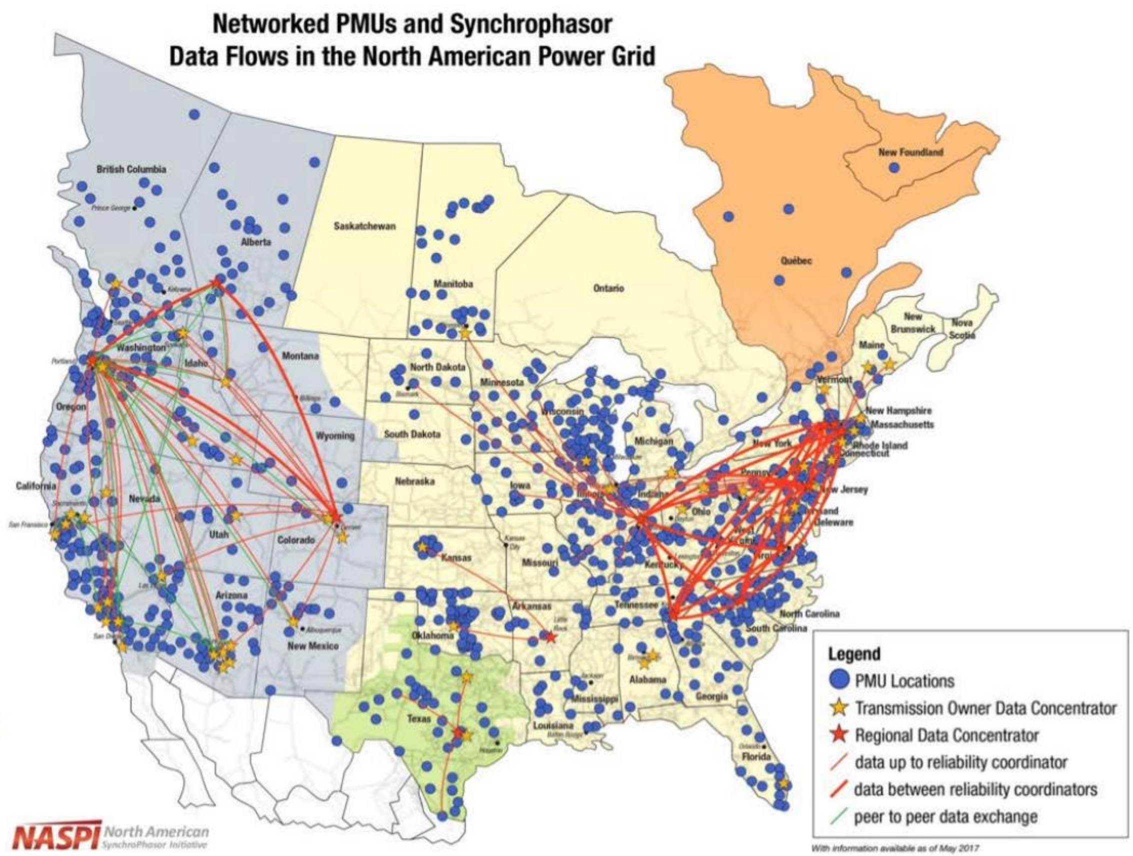


Synchrophasor Deployment in the US

~1200 in India (2018)

2017 North America Synchrophasor networks

- Over 2,500 networked PMUS
- Most RCs are receiving and sharing PMU data for real-time wide-area situational awareness

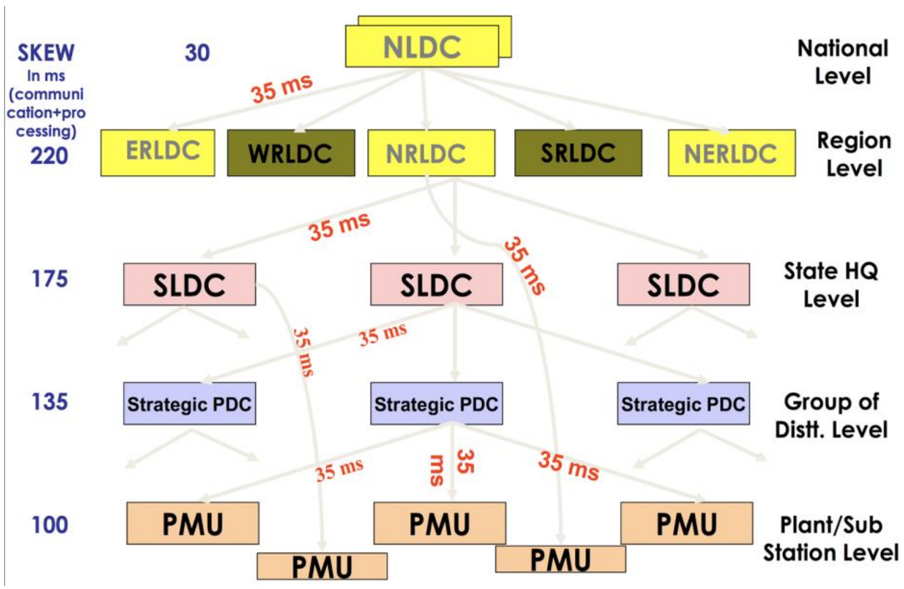


NASPI PMU locations in North America, May 2017

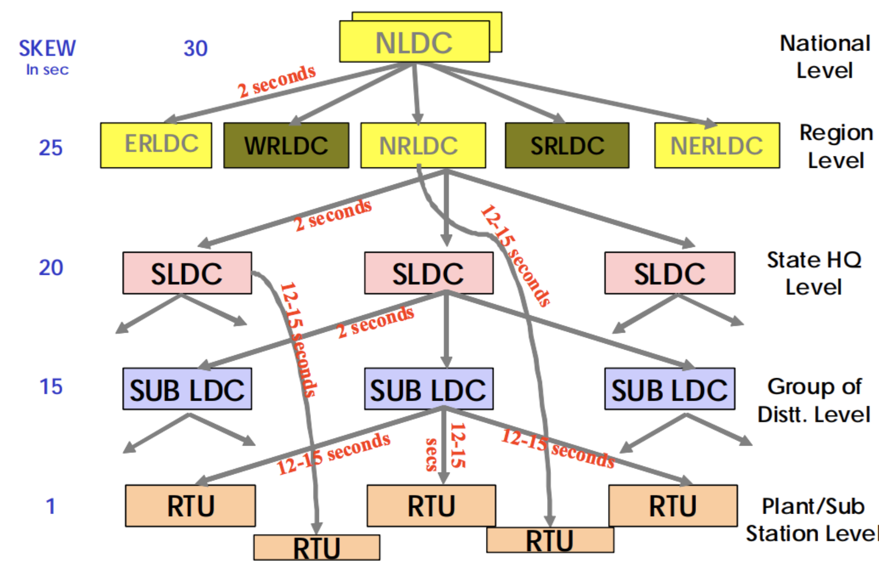
***Source**: "NASPI NARUC Summer Meeting 2017, Synchropahsors and the Grid, https://www.naspi.org/sites/default/files/reference_documents/naspi_naruc_silverstein_20170714.pdf

PMU network hierarchy and latency requirements (Indian power grid)

Latency in WAMS (PMUs)



Latency in SCADA (RTUs)



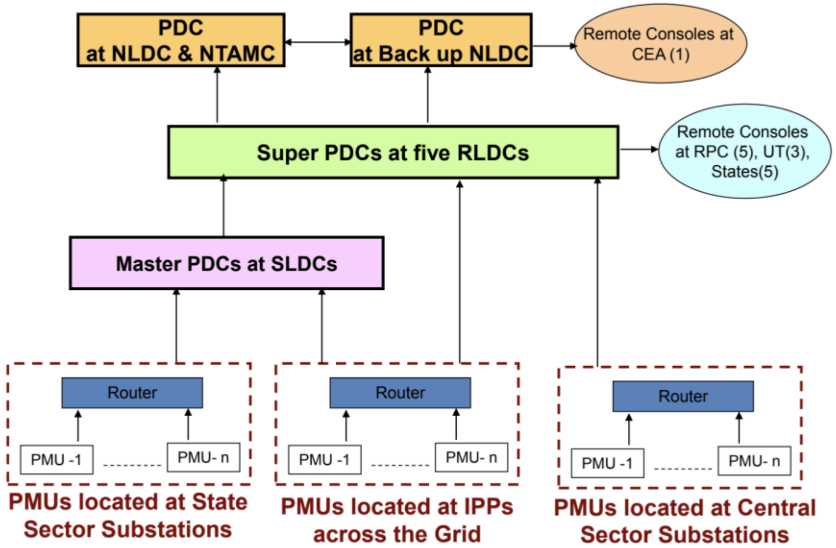
A sample PMU App deployment in India

Unified Real time Dynamic Measurement System (URTDSM)

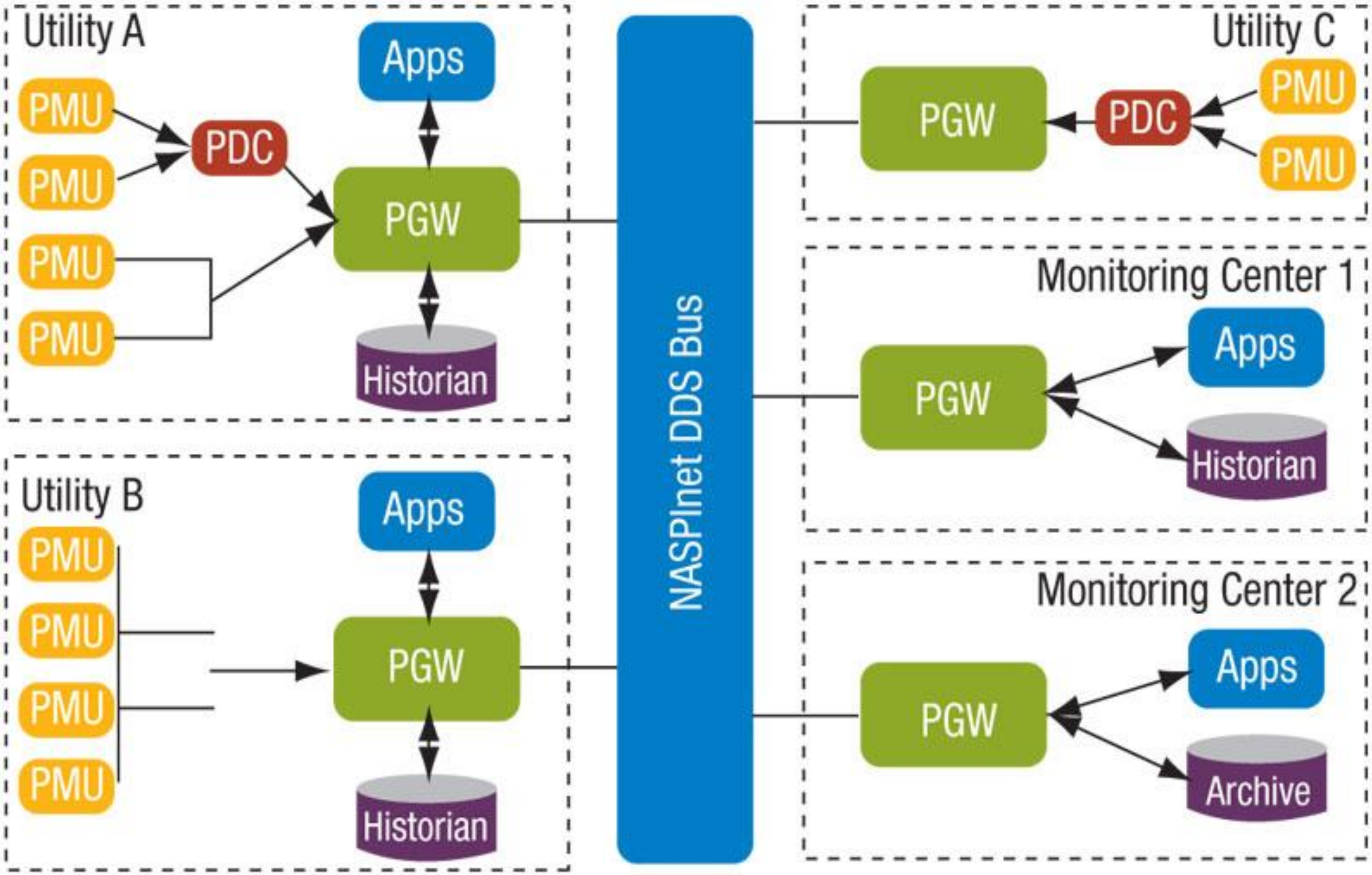
Project Details

- Phase-1
  - LOA: 15.01.2014 to M/s Alstom
    - Completion Schedule: -24 Months (Jan 2016)
    - Scope: Installation of PDCs at 34 Control Centres
    - Installation of 1186 PMUs across 354 Substations
      - PMUs at substations/generating stations of ISTS/STU connected through OPGW network.
      - PDCs at SLDCs/RLDCs/NLDC/NTAMC (34 nos.)
  - Package-I: (NR, ER, NER, NTAMC & NLDC)
    - Supply: - Rs. 158.22 Crore;
    - Services: - Rs.72.82Crore
    - Total: - Rs. 231.04 Cr
  - Package-II: (SR, WR)
    - Supply: - Rs. 82.61 Crore Services: - Rs.43.75Crore
    - Total: - Rs. 126.36 Cr
- Phase-II
  - Installation of approximately 554 PMUs at Substations and Power Plants
  - Installation of 11530 Km of OPGW and associated items mainly on state/ other utilities lines
  - Installation of 326 SDH equipments and associated items at substations and Power Plants
  - Installation of 215 Auxiliary Power Supply Equipments at substations and Power Plants

URTDSM System Hierarchy



NASPInet - Conceptual architecture



Source: http://rtcmagazine.com/articles/view/101843

Synchrophasor Real-Time Applications

Applications 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

(NASPI Summer Meeting 2017)

What's next for synchrophasor technology

- Advanced machine learning using PMU data to identify anomalous events and develop operator decision support tools
- Automated, autonomous system protection schemes, including wide-area damping
- Distribution-level uses for synchronized grid-level measurements (e.g., for two-way grid monitoring and analysis)
- Advance PMU deployment and applications use and data-sharing across TOs and RCs

[Synchrophasor deployment and applications in Industries/Entities]

Industry/ Entity	New PMUs Deployed	Application
Western Electric Coordinating Council	>250	**WAMPAC**, Congestion Management
PJM interconnection	>80	**WAMPAC**, Model Validation, Post-event analysis
Midwest ISO	>150	**WAMPAC,** EMS alarms
Duke Energy California	102	**WAMS**
ISO New England	30	**WAMS**, Congestion Management

***Source**: NERC: Real-Time Applications for Improving Reliability, October 2010, https://www.naspi.org/sites/default/files/reference_documents/rapir_final_20101017.pdf

Synchrophasor Applications

Current applications

- Monitoring & Visualization
  - Angle differences
  - Voltage Stability
  - Frequency
  - Trending analysis
- Alarms and Alerts for Situational Awareness
- State Estimation
- Fault Location
- Post mortem forensic analysis
- Model validations
- Special protection schemes (SPS) & Islanding

Potential future applications

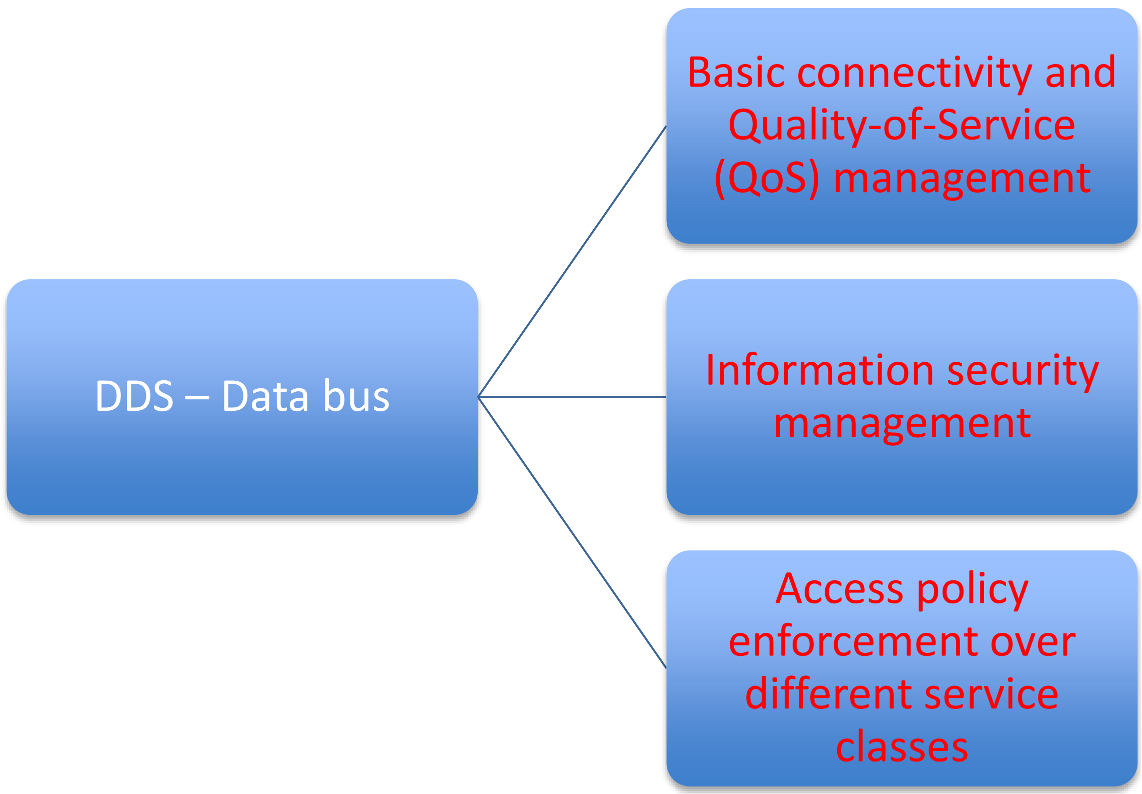
- Dynamic State Estimation
- Real-time automated controls
- Wide-Area Adaptive Protection
- Dynamic Line Rating
- System Integrity Protection Schemes

NASPInet - Phasor Data Concentrators

- PDC- Phasor Data Concentrators
  - Time align multiple phasors
  - Construct single data packet from several PMU data

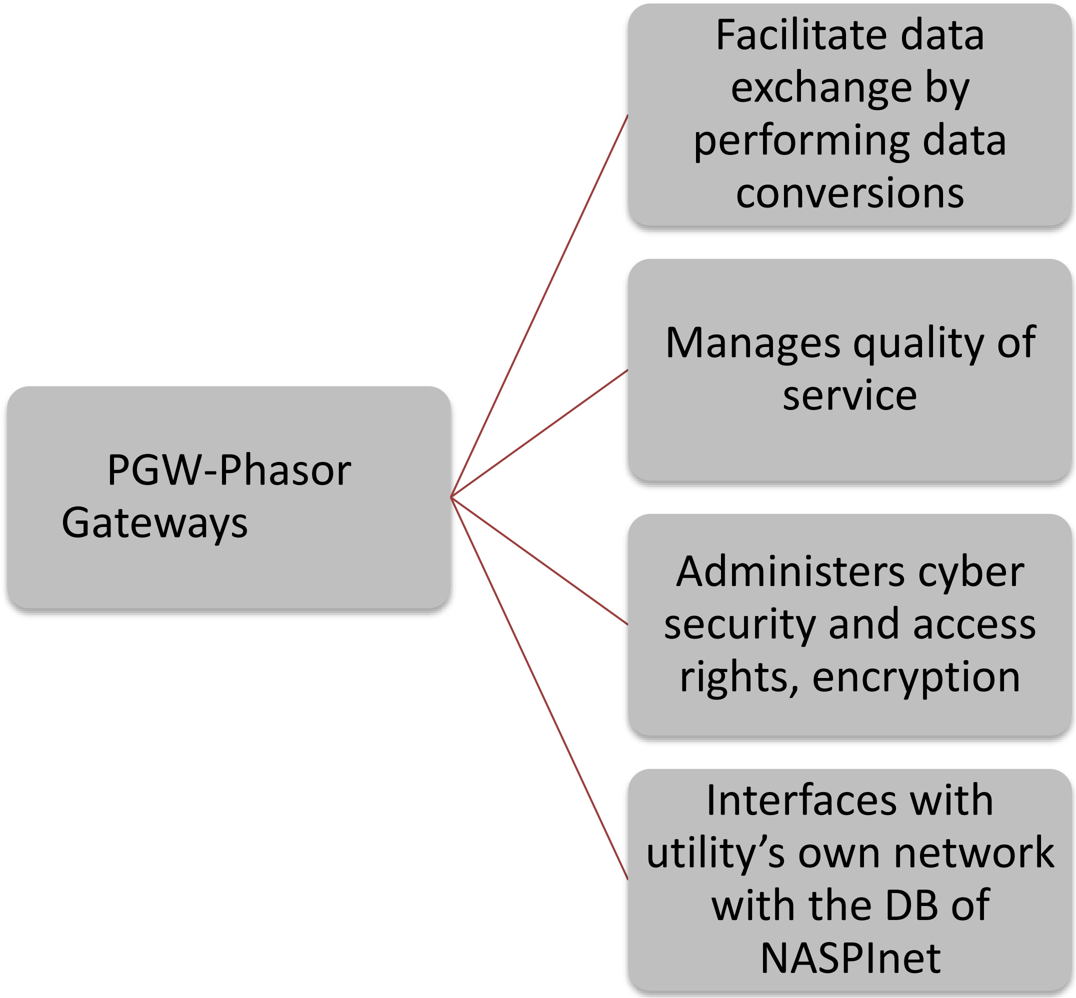
Source: http://rtcmagazine.com/articles/view/101843

NASPInet – Data Bus



Source: http://rtcmagazine.com/articles/view/101843

NASPInet - Phasor Gateways



Source: http://rtcmagazine.com/articles/view/101843

NASPInet Phasor Data Services

NASPInet has five different classes of phasor data services to facilitate real-time and historical synchrophasor data exchange among entities

- Class A data service for Feedback Control
  - Small signal stability, wide-area voltage and reactive power control
- Class B data service for Feed-forward Control
  - State estimator enhancement
- Class C data service for Visualization Applications
  - Increased operator visibility beyond own territory
- Class D data service for Post Event Analysis
  - Analysis of past disturbances
- Class E data service for Research and Development
  - Archived historical events data for R&D

NASPInet Phasor Data Services

Attribute	Data Service Classes				
	Class A	Class B	Class C	Class D	Class E
Low latency	4	3	2	1	1
High availability	4	2	1	3	1
High accuracy	4	2	1	4	1
Time alignment	4	4	2	1	1
High Sampling rate	4	2	2	4	1
Path redundancy	4	4	2	1	1

PHASOR DATA SERVICES: DATA CLASS ATTRIBUTES

4 – critically important; 3 – Important; 2 – Somewhat important; and 1 – Not very important.

Source: NASPInet Specification- An Important Step toward Its Implementation, Proceedings of the 43rd Hawaii International Conference on System Sciences, 2010

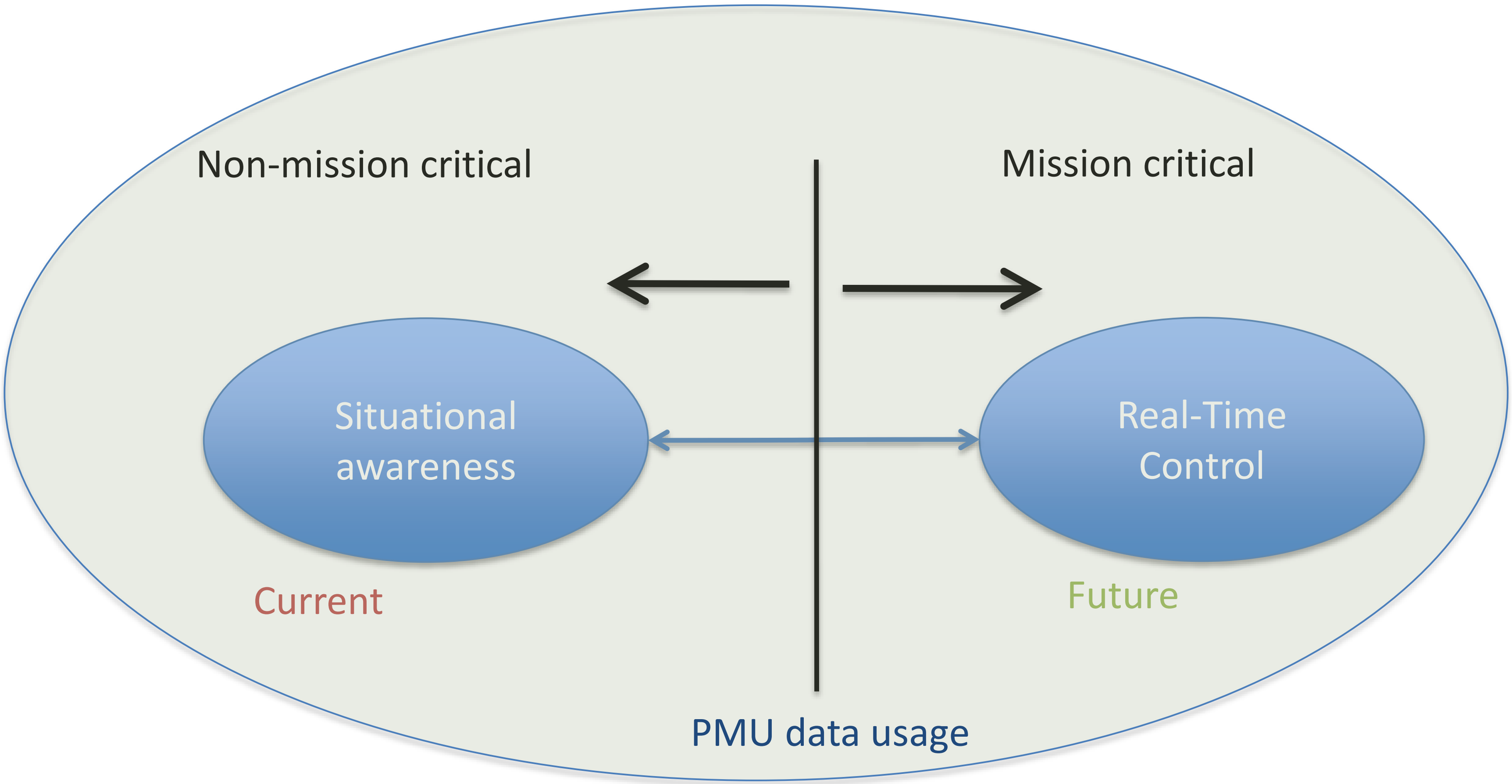
NASPInet Phasor Data Services

Data Class	Reporting Rate	Availability	Maximum Interruption	Latency
	Frames/s	**%**	**ms**	**ms**
A	30, 60, 120	99.9999	<5	<50
B	20, 30, 60	99.999	<25	<100
C	10, 15, 20, 30	99.99	<100	<1000
D	30, 60, 120	99.99	-	<2
E	30, 60, 120	99.99	-	<2

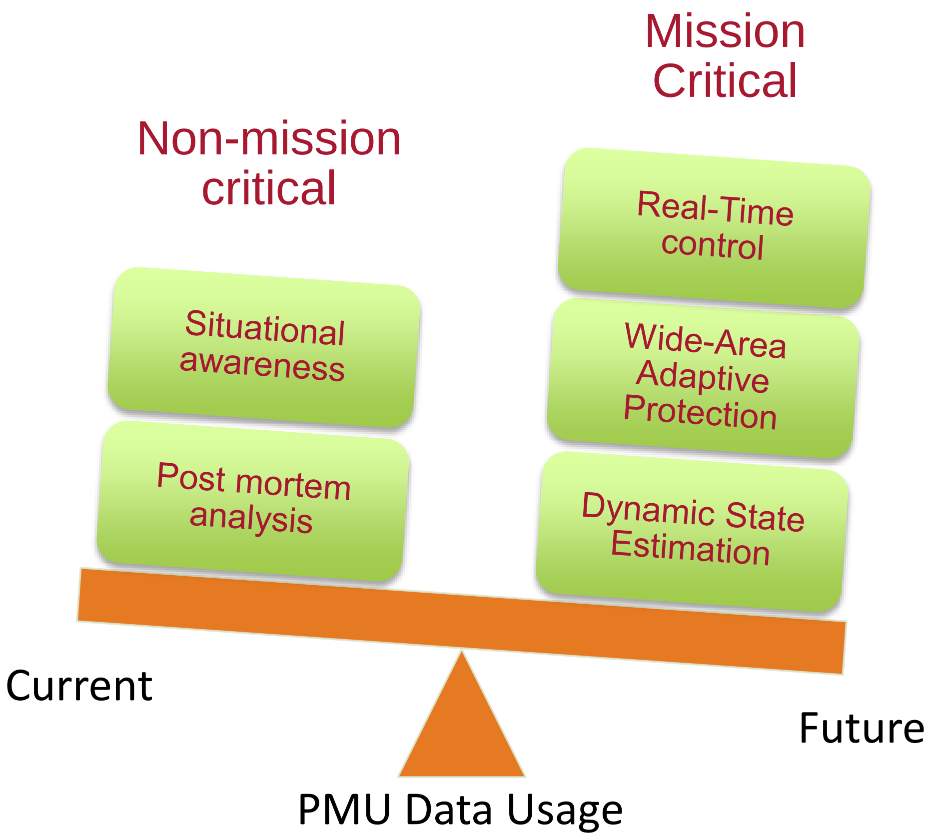
PHASOR DATA SERVICES: PERFORMANCE REQUIREMENTS

Source: NASPInet Specification- An Important Step toward Its Implementation, Proceedings of the 43rd Hawaii International Conference on System Sciences, 2010

PMU data usage in critical applications



Synchrophasor applications evolving …



NASPInet and Cyber Security issues

Use of PMU data

NERC CIP not applicable for Phasor systems today

Cyber-security practices and technologies are still evolving

Future versions of NERC CIP expected to include requirements for Phasor data Systems in detail

US SGIG funded projects: Cyber-security approach

- Identification of cyber-security risks and risk mitigation
- Cyber-security criteria utilized for vendor and device selection
- Relevant cyber-security standards to be followed
- Planning for how the project will support emerging smart grid cyber-security standards

NASPInet Cybersecurity Requirements and Challenges

- Authentication, Authorization and Access Control
  - Prevent unauthorized access of PMU data and also verifying the authenticity of PMU data sending entity
  - Examples: Kerberos type service, digital certificates, access control lists
- Integrity and Confidentiality of Measurement Data
  - Prevent confidentiality and integrity by symmetric-key-based cryptographic message authentication codes, source authentication methods
  - Since multiple entities may subscribe to multicast synchrophasor data group key based message authentication codes and source authentication methods need to be developed
    - E.g.: Digital signatures which use Asymmetric keys

Bobba, R.B.; Dagle, J.; Heine, E.; Khurana, H.; Sanders, W.H.; Sauer, P.; Yardley, T., "Enhancing Grid Measurements: Wide Area Measurement Systems, NASPInet, and Security," Power and Energy Magazine, IEEE , vol.10, no.1, pp.67,73, Jan.-Feb. 2012

NASPInet Cybersecurity Requirements and Challenges

- **Non-repudiation**
  - Digital signatures are used to provide non-repudiation
  - Digital signatures are expensive in computation and communication with respect to real-time requirements
- **Key Management**
  - Complexity of key management increases as **group keys** need to frequently updated with group composition changes
  - **Real-time latency requirements** further complicates group key management problems

NASPInet Cybersecurity Requirements and Challenges

- **Data and Infrastructure Availability**
  - Design of network should incorporate fault-tolerance to maintain high reliability and availability requirements for real-time control applications
  - Mechanisms to detect and respond to cyber attacks and intrusions in a timely manner
    - Network Access Control
    - Secure Logging

NERC CIP and Synchrophasors

- At present, phasor data is not used for mission critical applications, but will be used in the future

- NERC CIP applies only to critical cyber assets

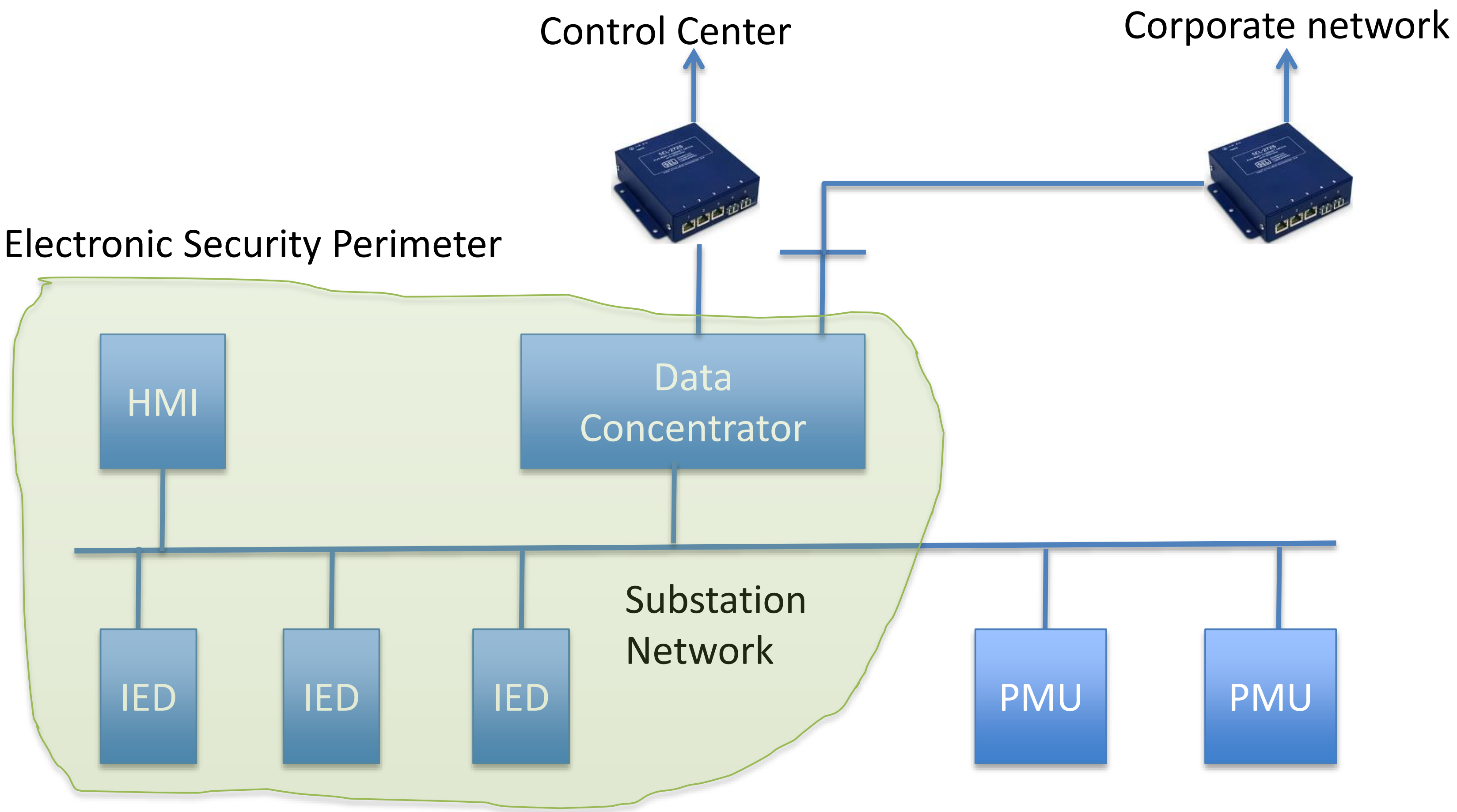
- Critical Cyber Assets
  – "Cyber Assets essential to the reliable operation of Critical Assets"

NERC CIP and Synchrophasors

- Is Synchrophasor a ‘critical cyber asset’?
  - Is it associated with a ‘critical asset’?
  - Is it used in a key control algorithm?
  - Does it support Bulk Electric System reliability?

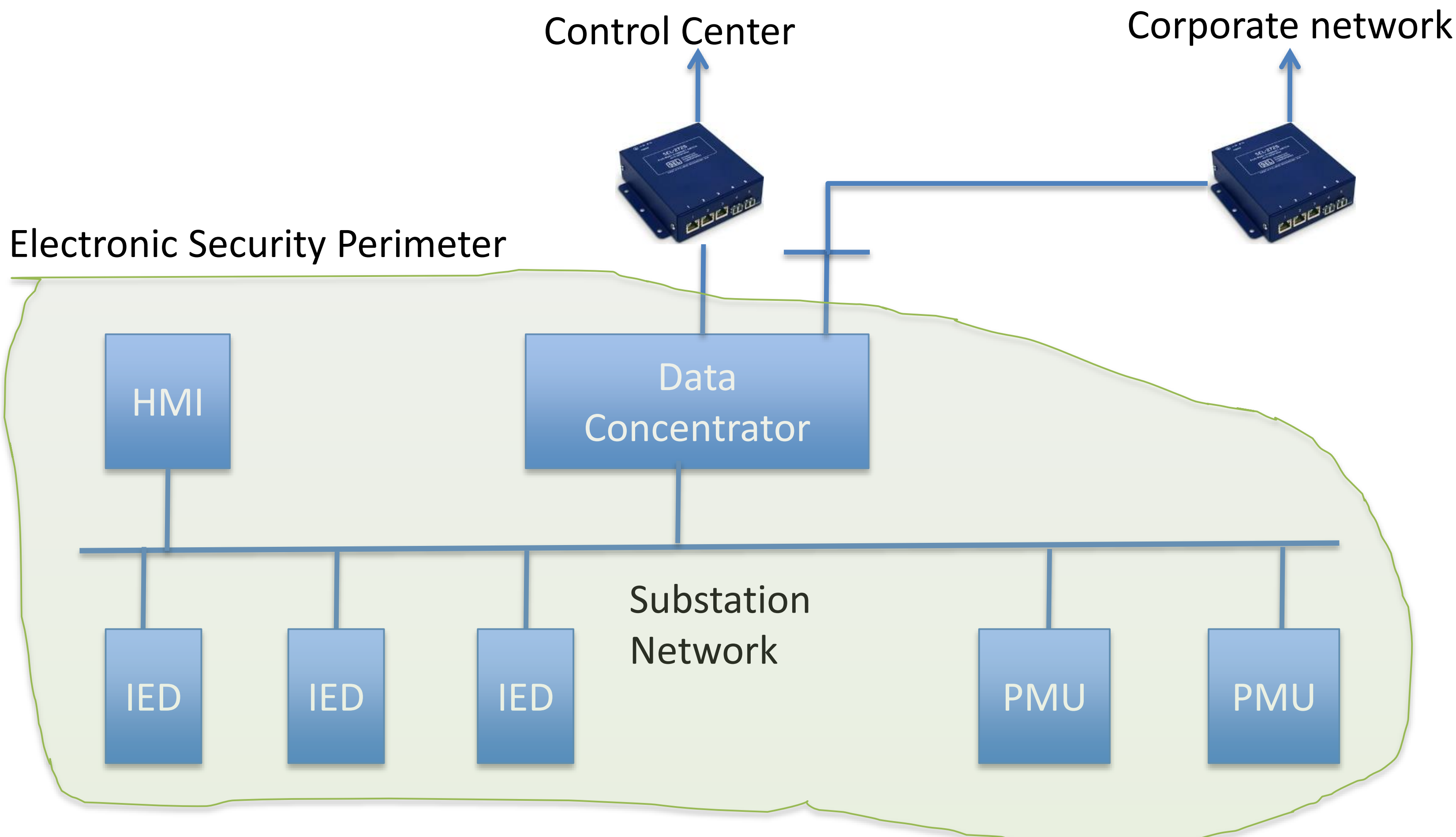
- If a Synchrophasor is associated with ‘Critical Assets’
  – Then, NERC CIP applies

NERC CIP and Synchrophasors –
Electronic Security Perimeter (CIP 005)



NERC CIP and Synchrophasors – Evolving state …

CIP compliance applies based on PMU's classification as BES Cyber Asset or not?



Summary

- Synchrophasor is key technology in the smart grid
- PMU, synchrophasor network, and applications are being deployed
- NAPSInet is being deployed in different regions of the grid in the US
- Synchrophasor applications are being tested in real grid environment
- NERC CIP compliance applies for critical PMUs (used for critical applications)
- In India, PMU deployment and pilot testing of applications is underway

AMI Security and Privacy

Need for Advanced Metering Infrastructure (AMI)

System Operation Benefits
- Reduction in peak loads
- Improved Monitoring and control
- Improved efficiency and reliability
- Cost reduction

Customer Service Benefits
- Billing accuracy and flexible billing cycle
- Time based rate options
- Custom energy profiles for Energy Efficiency
- Demand Response

Financial Benefits
- Reduced equipment and maintenance costs
- Reduced support expenses
- Faster outage restoration
- Improved inventory management

Advanced Metering Infrastructure

Digital hardware and software

+

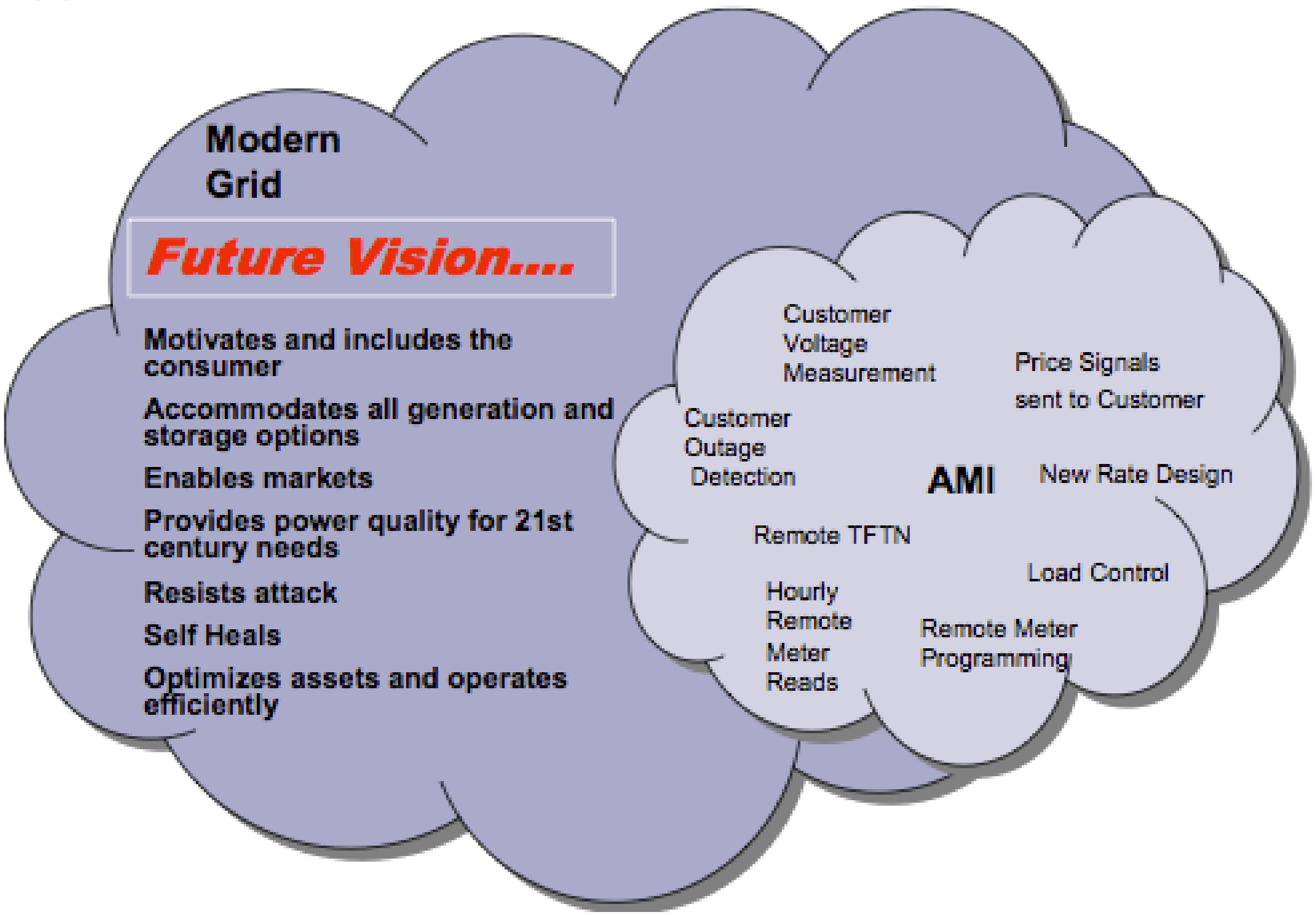
Interval data measurement capability

+

Two-way remote communications

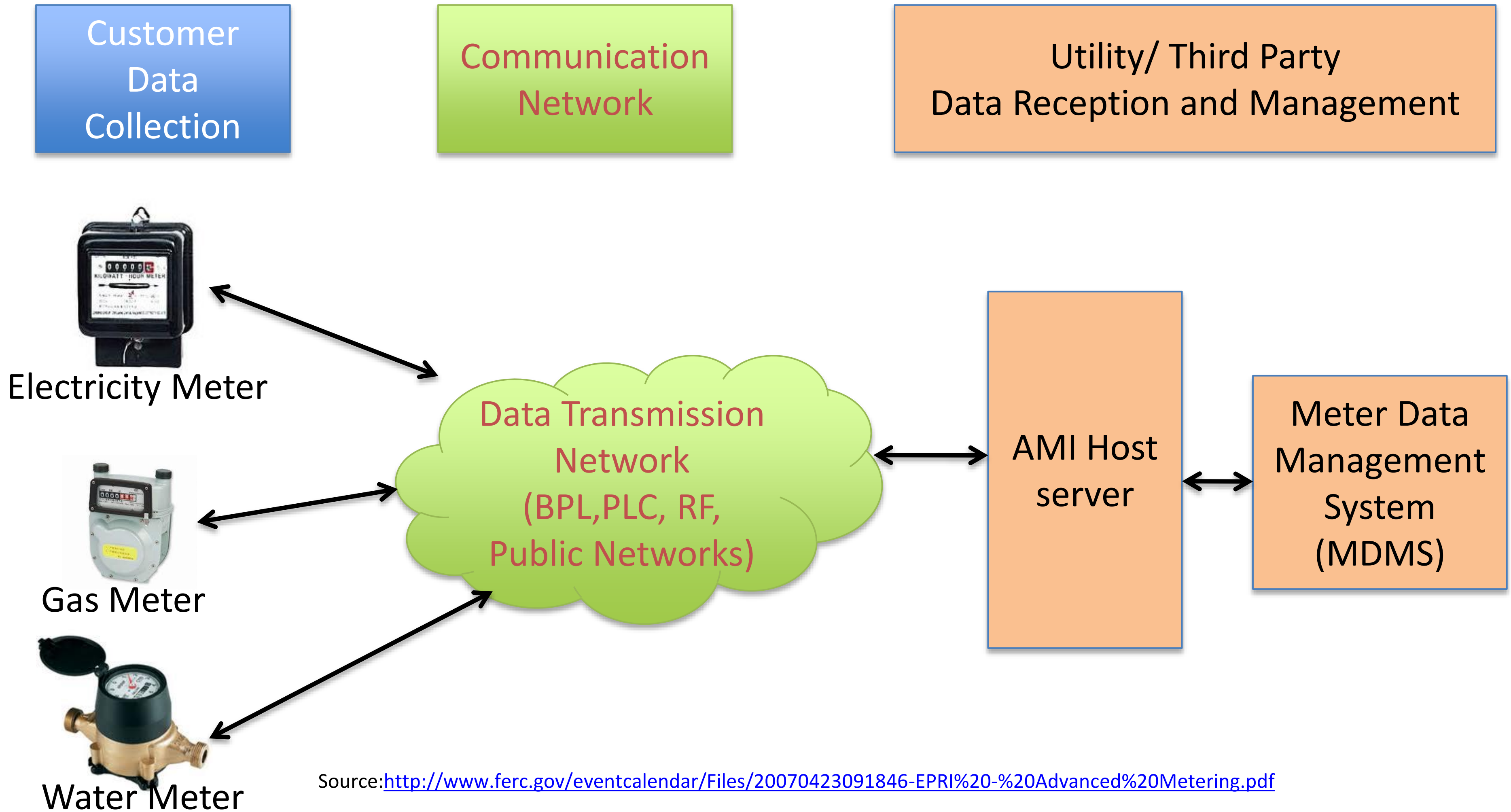
= AMI

AMI in Modern Grid vision



Advanced Metering Infrastructure, National Energy Technology Laboratory, U.S Department of Energy, Office of Electricity Delivery and Energy Reliability, February 2008

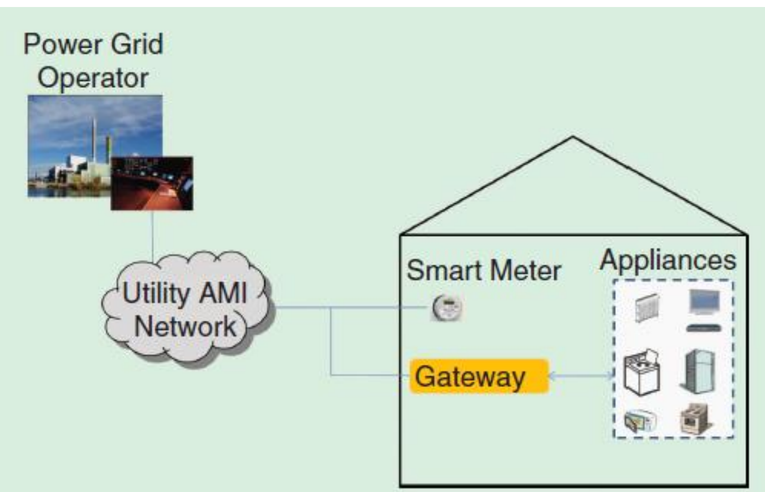
Basic AMI architecture

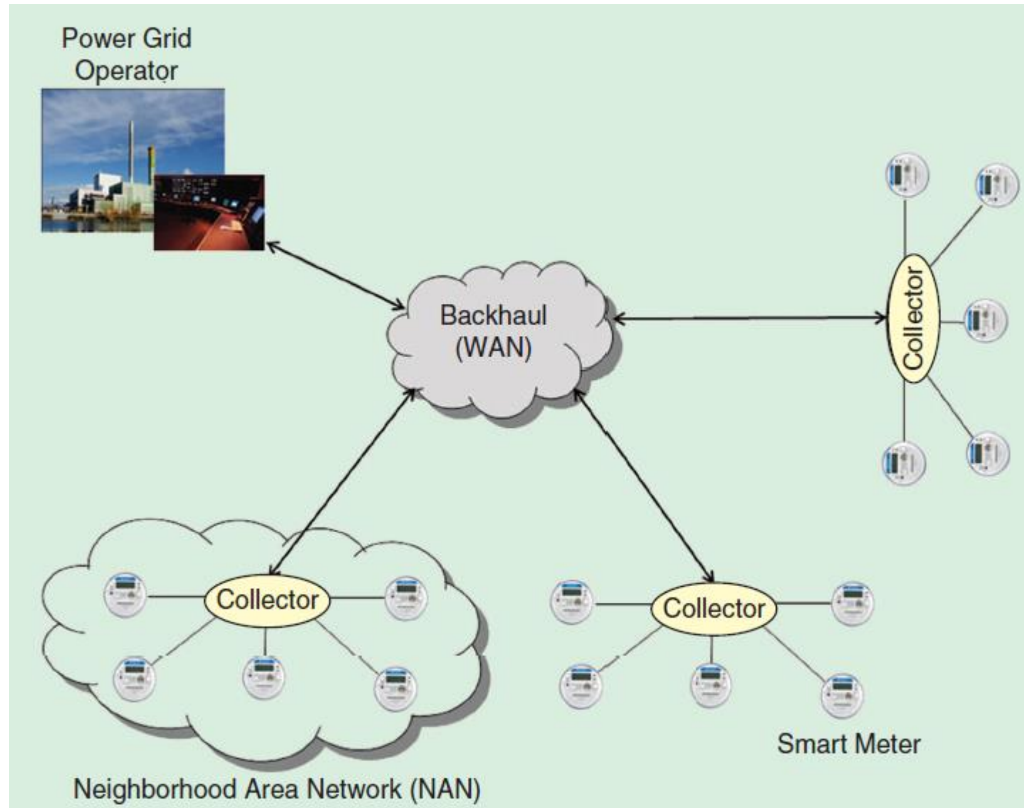


Source:http://www.ferc.gov/eventcalendar/Files/20070423091846-EPRI%20-%20Advanced%20Metering.pdf

ADVANCED METERING INFRASTRUCTURE (AMI)

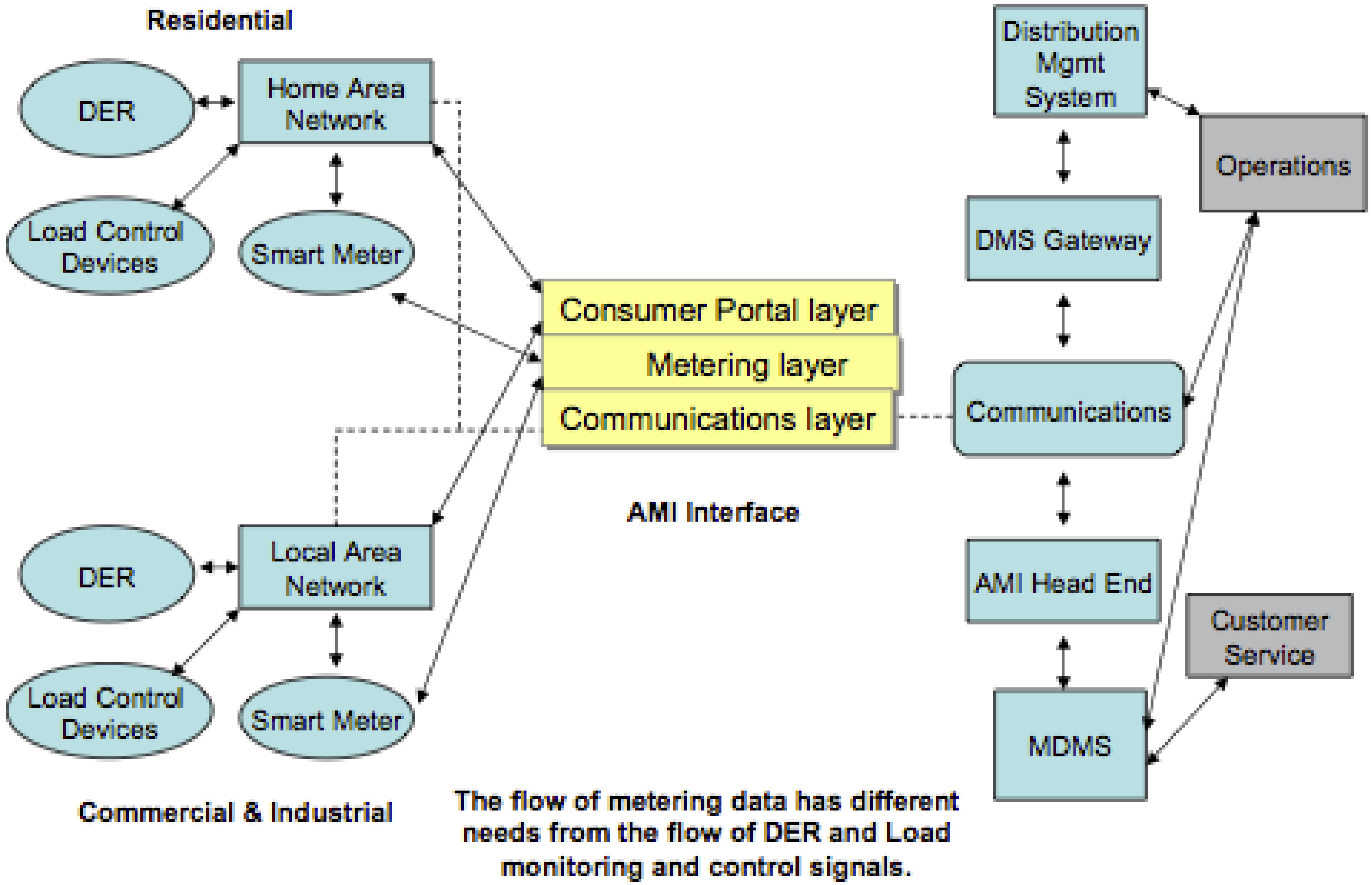
- Two-way communication between producer and consumers





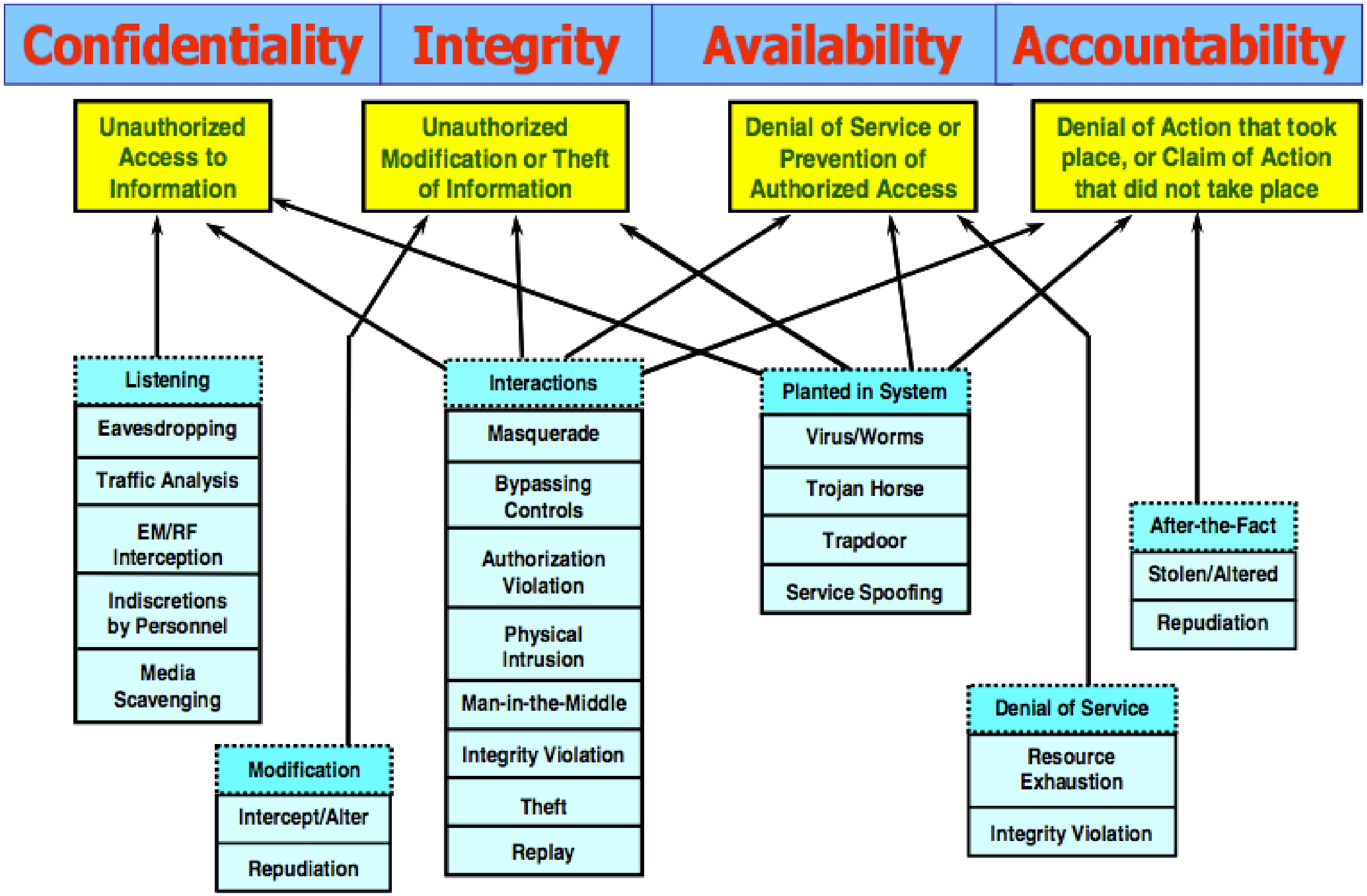
Bouhafs, F. Mackay, M. Merabti, M., "Links to the Future: Communication Requirements and Challenges in the Smart Grid," IEEE Power & Energy magazine, Jan. 2012

Overall AMI architecture



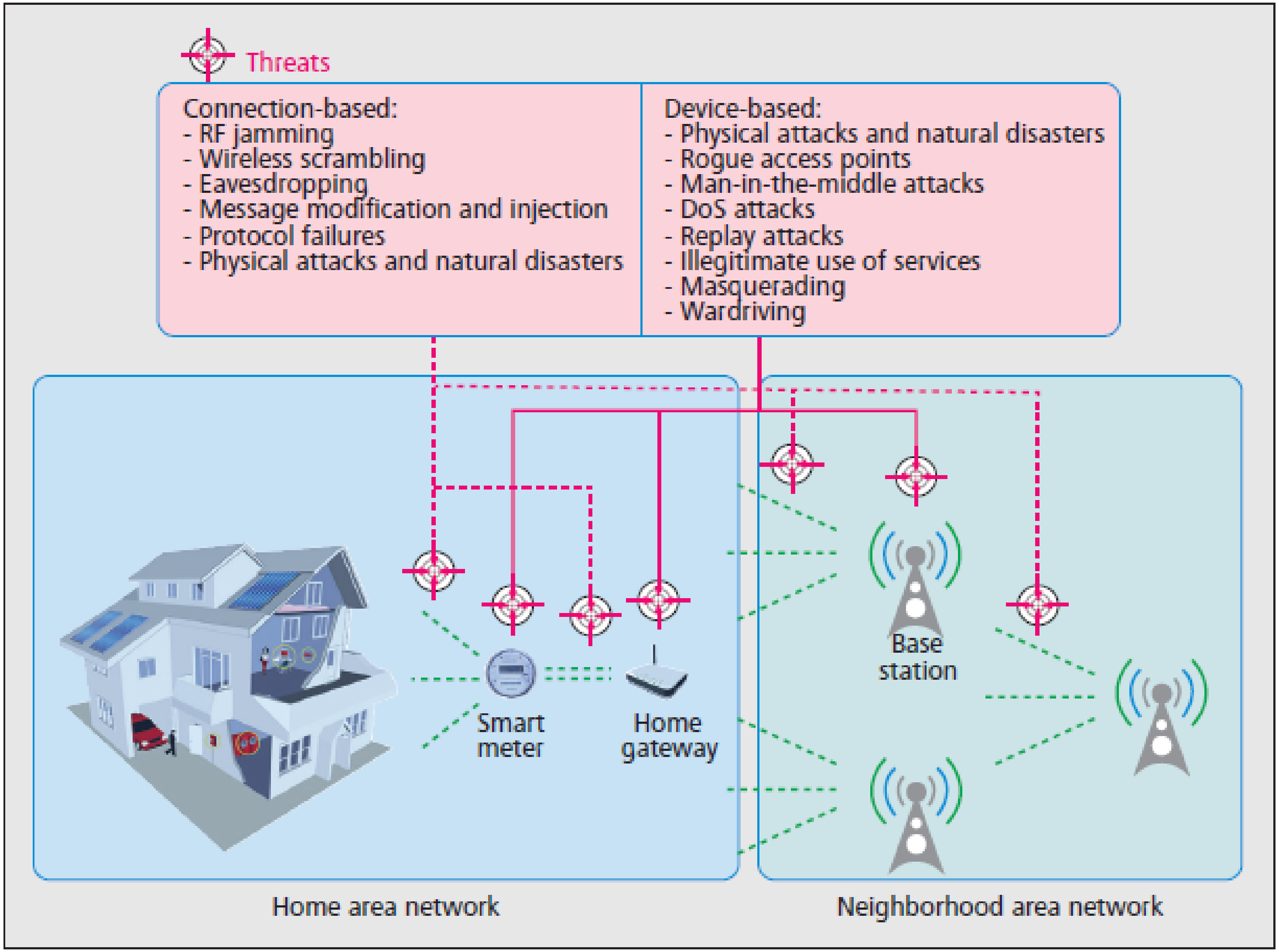
Advanced Metering Infrastructure, National Energy Technology Laboratory, U.S Department of Energy, Office of Electricity Delivery and Energy Reliability, February 2008

AMI security requirements



Cleveland, F.M.; , "Cyber security issues for Advanced Metering Infrastructure (AMI)," Power and Energy Society General Meeting - Conversion and Delivery of Electrical Energy in the 21st Century, 2008 IEEE , vol., no., pp.1-5, 20-24 July 2008.

AMI Cyber Threats



AMI security vs. privacy

- What data?
- How much data to be collected, by whom, when and how?
- How to adequately protect data?
- Two major areas
  - Operational data (Bulk System)
  - Electric Usage data (Consumer data)

Privacy of Operational Data

- Following data needs to be secure
  - Operational procedures
  - System topology
  - Control and monitoring signals
  - Load analysis data

- NERC deals with security and reliability of bulk power system only

Privacy of Customer Data

- Protection of Consumer Electric Usage Data (CEUD)
  - Data collection
  - Data ownership
  - Data integrity
  - Data privacy
- Government has a role in regulating privacy of consumer data

Course module Summary

- Protocol Security
  - DNP3,
  - ICCP,
  - IEC 61850 MMS, GOOSE, SV

- Synchrophasor & NASPInet Security
  - Architecture
  - Security issues
  - Requirements and challenges

- AMI Security
  - Architecture
  - Security and privacy