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
| 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, Synchrophasor, 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)

<table>
<thead>
<tr>
<th>Application</th>
<th>Media</th>
<th>Standard/Protocol</th>
<th>Network Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>Expected Data Rate/Bandwidth&lt;sup&gt;a&lt;/sup&gt;</td>
</tr>
<tr>
<td>Home-area Network</td>
<td>Power line communications,&lt;sup&gt;c&lt;/sup&gt; wireless</td>
<td>HomePlug, ZigBee, IP</td>
<td></td>
</tr>
<tr>
<td>Advanced Metering Infrastructure</td>
<td>Power line communications,&lt;sup&gt;c&lt;/sup&gt; wireless radio frequency,&lt;sup&gt;e&lt;/sup&gt; T1, microwave, broadband (via fiber, cable, digital subscriber line), commercial wireless&lt;br&gt;(AMI)&lt;sup&gt;a&lt;/sup&gt;</td>
<td>For backhaul: WiMAX, LTE For appliance to meter: IEEE 802.15.4,&lt;sup&gt;h&lt;/sup&gt; ZigBee&lt;sup&gt;g&lt;/sup&gt;</td>
<td>10–100 kilobytes/second (kbps)/node, 500 kbps for backhaul</td>
</tr>
<tr>
<td>Demand Response (Part of AMI)</td>
<td>Same as AMI</td>
<td>Same as AMI</td>
<td>2–15 seconds</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>5–15 minutes/node</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>99–99.99% high</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Not necessary</td>
</tr>
<tr>
<td>Electric Transportation</td>
<td>Power line communications,&lt;sup&gt;l&lt;/sup&gt; wireless&lt;sup&gt;m&lt;/sup&gt;</td>
<td>ZigBee, IEEE 802.15.4&lt;sup&gt;n&lt;/sup&gt;</td>
<td>9.6–56 kbps, 100 kbps is a good target</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2 seconds–5 minutes</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Daily 99–99.99% relatively high</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Not necessary</td>
</tr>
<tr>
<td>Distribution Grid Management</td>
<td>Fiber, wireless,&lt;sup&gt;c&lt;/sup&gt; satellite, cellular&lt;sup&gt;n&lt;/sup&gt;</td>
<td>DNP3 (IEEE 1815), IEC 61850/GOOSE&lt;sup&gt;k&lt;/sup&gt; WiMAX, LTE&lt;sup&gt;l&lt;/sup&gt; IP&lt;sup&gt;m&lt;/sup&gt; IEEE 802.15.4&lt;sup&gt;n&lt;/sup&gt;</td>
<td>9.6–100 kbps</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>100 ms–2 seconds</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Continuous 99–99.999% high</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>24–72 hours</td>
</tr>
<tr>
<td>Distributed Energy Resources and</td>
<td>Fiber, wireless,&lt;sup&gt;c&lt;/sup&gt; satellite&lt;sup&gt;n&lt;/sup&gt;</td>
<td>DNP3, IEC 61850/GOOSE&lt;sup&gt;k&lt;/sup&gt; WiMAX, LTE/&lt;sup&gt;l&lt;/sup&gt; IP&lt;sup&gt;m&lt;/sup&gt; IEEE 802.15.4&lt;sup&gt;n&lt;/sup&gt;</td>
<td>9.6–56 kbps</td>
</tr>
<tr>
<td>Storage</td>
<td></td>
<td></td>
<td>20 ms–15 seconds</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Continuous 99–99.99% high</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>1 hour</td>
</tr>
<tr>
<td>Wide-area Situational Awareness</td>
<td>SONET, ATM, Frame Relay, MPLS,&lt;sup&gt;g&lt;/sup&gt; fiber, microwave, broadband over power line&lt;sup&gt;h&lt;/sup&gt;</td>
<td>C37.118, IEC 61850/GOOSE&lt;sup&gt;k&lt;/sup&gt; IP&lt;sup&gt;n&lt;/sup&gt;</td>
<td>600–1,500 kbps</td>
</tr>
<tr>
<td>(synchrophasors&lt;sup&gt;e&lt;/sup&gt;)</td>
<td></td>
<td></td>
<td>20 ms–200 ms</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Continuous 99–999–99.999% high</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>24-hour supply</td>
</tr>
<tr>
<td>Interutility communications</td>
<td>Fiber, microwave, wired</td>
<td>ICCP&lt;sup&gt;k&lt;/sup&gt;</td>
<td>&gt; 45 megabytes/second (mbps)</td>
</tr>
<tr>
<td>(Southern California Edition)</td>
<td></td>
<td></td>
<td>&lt;50 ms (DS-3)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Continuous 99:999–99.999% high</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>24-hour supply</td>
</tr>
<tr>
<td>Interregional data communications</td>
<td>Standard telco T1 circuits with copper endpoints (NERCNet)</td>
<td>IP&lt;sup&gt;n&lt;/sup&gt;</td>
<td>256 kbps</td>
</tr>
<tr>
<td>(ISO New England)</td>
<td></td>
<td></td>
<td>20–200 ms</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Continuous 99:999% high</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>24-hour supply</td>
</tr>
<tr>
<td>Market data communications</td>
<td>Wired</td>
<td>IP&lt;sup&gt;n&lt;/sup&gt;</td>
<td>18 mbps + 45 mbps connections</td>
</tr>
<tr>
<td>(ISO New England)</td>
<td></td>
<td></td>
<td>20–200 ms</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Continuous 99:999% high</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Relatively high</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>24-hour supply</td>
</tr>
</tbody>
</table>
SCADA communication Protocols - An overview

- Control center
- Remote Terminal Units
- Relays

Protocols:
- DNP3
- ICCP
- IEC 61850
- MMS
- GOOSE
- IEC 61850 SV

Cyber-Physical Security for the Smart Grid, GIAN Course, IIT Bombay (Manimaran Govindarasu)
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.

ICCP Protocol Architecture

ICCP

Application Programming Interface (API)

- Alarm Processor
- Accounting
- Interchange Scheduling
- Maintenance Mgmt.

SCADA Database  Data Acq. & Control  EMS Applications  Operator Console  RDBMS  Network Mgmt

Application Program Interface

- ICCP
- MMS
- OSI Layers 1-6

*APIs are not standardized*

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.

Secure DNP3 protocol was introduced in 2007.

Security related function code and authentication added to application layer.

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 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 profiles mapping to OSI model

Source: IEC 61850 Tutorial, IEC 61850 users group, November 15, 2011, UCAIug 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
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

Possible cyber attacks

Regional Control Center-layer

Other EMS/SCADA Applications

Wide Area Monitoring, Protection & Controller (WAMPAC)

Transmission layer

Regional Super PDC

Wide Area Network

Wide Local Area Network (WLAN)

Local PDC A

Station A

Relays

PMUs

Station B

Relays

PMUs

Generation-layer

Plant

Power System Layer

Wide Area Monitoring/Visualization
- Phasor angle
- Voltage/frequency Stability
- Power Oscillation

Wide Area Control
- Inter-Area Oscillation Damping controller
- Secondary Voltage Controller
- FACT Switching Control, (SVC, STATCOM)

Wide Area Protection
- Remedial Action Scheme, Special Protection Scheme (response based)
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

PMU network hierarchy and latency requirements (Indian power grid)

Latency in WAMS (PMUs)

- SKEW in ms (communication processing) 220
- ERLDC 30
- WRLDC
- NRLDC
- SRLDC
- NERLDC

Latency in SCADA (RTUs)

- SKEW in sec 30
- ERLDC 2 seconds
- WRLDC
- NRLDC
- SRLDC
- NERLDC

- SKEW in sec 25
- ERLDC
- WRLDC
- NRLDC
- SRLDC
- NERLDC

- SKEW in sec 20
- SLDC
- SLDC
- SLDC

- SKEW in sec 15
- SLDC
- SLDC
- SLDC

- SKEW in sec 1
- RTU
- RTU
- RTU
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**

- Master PDCs at SLDCs
- Super PDCs at five RLDCs
- PDC at NLDC & NTAMC
- PDC at Backup NLDC
- Remote Consoles at CEA (1)
- Remote Consoles at RPC (5), UT(3), States(5)
NASPInet - Conceptual architecture

Source: http://rtcmagazine.com/articles/view/101843
Synchrophasor Real-Time Applications

Applications Taxonomy

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

<table>
<thead>
<tr>
<th>Industry/Entity</th>
<th>New PMUs Deployed</th>
<th>Application</th>
</tr>
</thead>
<tbody>
<tr>
<td>Western Electric</td>
<td>&gt;250</td>
<td>WAMPAC, Congestion Management</td>
</tr>
<tr>
<td>Coordinating Council</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PJM interconnection</td>
<td>&gt;80</td>
<td>WAMPAC, Model Validation, Post-event analysis</td>
</tr>
<tr>
<td>Midwest ISO</td>
<td>&gt;150</td>
<td>WAMPAC, EMS alarms</td>
</tr>
<tr>
<td>Duke Energy California</td>
<td>102</td>
<td>WAMS</td>
</tr>
<tr>
<td>ISO New England</td>
<td>30</td>
<td>WAMS, Congestion Management</td>
</tr>
</tbody>
</table>


March 2018

Cyber-Physical Security for the Smart Grid, GIAN Course, IIT Bombay (Manimaran Govindarasu)
## 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
NASPIInet - Phasor Gateways

- Facilitate data exchange by performing data conversions
- Manages quality of service
- Administers cyber security and access rights, encryption
- Interfaces with utility’s own network with the DB of NASPIInet

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

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Data Service Classes</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Class A</td>
</tr>
<tr>
<td>Low latency</td>
<td>4</td>
</tr>
<tr>
<td>High availability</td>
<td>4</td>
</tr>
<tr>
<td>High accuracy</td>
<td>4</td>
</tr>
<tr>
<td>Time alignment</td>
<td>4</td>
</tr>
<tr>
<td>High Sampling rate</td>
<td>4</td>
</tr>
<tr>
<td>Path redundancy</td>
<td>4</td>
</tr>
</tbody>
</table>

### PHASOR DATA SERVICES: DATA CLASS ATTRIBUTES

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

# NASPInet Phasor Data Services

<table>
<thead>
<tr>
<th>Data Class</th>
<th>Reporting Rate</th>
<th>Availability</th>
<th>Maximum Interruption</th>
<th>Latency</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>30, 60, 120</td>
<td>99.9999</td>
<td>&lt;5</td>
<td>&lt;50</td>
</tr>
<tr>
<td>B</td>
<td>20, 30, 60</td>
<td>99.999</td>
<td>&lt;25</td>
<td>&lt;100</td>
</tr>
<tr>
<td>C</td>
<td>10, 15, 20, 30</td>
<td>99.99</td>
<td>&lt;100</td>
<td>&lt;1000</td>
</tr>
<tr>
<td>D</td>
<td>30, 60, 120</td>
<td>99.99</td>
<td>-</td>
<td>&lt;2</td>
</tr>
<tr>
<td>E</td>
<td>30, 60, 120</td>
<td>99.99</td>
<td>-</td>
<td>&lt;2</td>
</tr>
</tbody>
</table>

**PHASOR DATA SERVICES: PERFORMANCE REQUIREMENTS**

PMU data usage in critical applications

- Non-mission critical
  - Situational awareness
  - Current

- Mission critical
  - Real-Time Control
  - Future

PMU data usage

Cyber-Physical Security for the Smart Grid, GIAN Course, IIT Bombay (Manimaran Govindarasu)
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:**

- 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

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
NASPIInet 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)

- **Control Center**
- **Corporate network**

Electronic Security Perimeter

- **HMI**
- **Data Concentrator**
- **Substation Network**
- **IED**
- **PMU**

March 2018
NERC CIP and Synchrophasors – Evolving state ...

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

Cyber-Physical Security for the Smart Grid, GIAN Course, IIT Bombay (Manimaran Govindarasu)
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

- Motivates and includes the consumer
- Accommodates all generation and storage options
- Enables markets
- Provides power quality for 21st century needs
- Resists attack
- Self Heals
- Optimizes assets and operates efficiently

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

Customer Data Collection

Communication Network

Utility/ Third Party Data Reception and Management

Data Transmission Network (BPL, PLC, RF, Public Networks)

AMI Host server

Meter Data Management System (MDMS)

Electricity Meter

Gas Meter

Water Meter

ADVANCED METERING INFRASTRUCTURE (AMI)

- Two-way communication between producer and consumers

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

AMI Cyber Threats

- Connection-based threats:
  - RF jamming
  - Wireless scrambling
  - Eavesdropping
  - Message modification and injection
  - Protocol failures
  - Physical attacks and natural disasters

- Device-based threats:
  - Physical attacks and natural disasters
  - Rogue access points
  - Man-in-the-middle attacks
  - DoS attacks
  - Replay attacks
  - Illegitimate use of services
  - Masquerading
  - Wardriving
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