COMMUNICATION AND SECURITY IN SMART GRID

Tricha Anjali
School of Computing & Electrical Engineering
Indian Institute of Technology, Mandi

CONTENTS

- Introduction to smart grid
- Communication in Smart Grid
- Security Problems and Solutions

TEXTBOOK DEFINITION

- "an automated, widely distributed energy delivery network characterized by a two-way flow of electricity and information, capable of monitoring and responding to changes in everything from power plants to customer preferences to individual appliances"

- "the electricity delivery system (from point of generation to point of consumption) integrated with communications and information technology for enhanced grid operations, customer services, and environmental benefits"

PRACTICAL DEFINITION

- a new **digital meter** to replace the traditional analog meter?
- a **wireless network** that accesses those meters remotely or the data management system that processes the information?
- some **solar panels** on the roof or **wind mills** on farm?
- a **load-controller** on the user premises?
- **Smart Grid is the inclusion of all of these things**

WHAT CAN IT DO?

- Identify and resolve faults in electricity grid
- Automatically self-heal the grid
- Monitor power quality and manage voltage
- Identify devices or subsystems that require maintenance
- Help consumers optimize their individual electricity consumption (minimize their bills)
- Enable the use of smart appliances that can be programmed to run on off-peak power

ENABLERS

- Intelligent sensors and actuators
- Extended data management system
- Expanded two way communication between utility operation system facilities and customers
- Network security

IED EXPLOSION

- Protection relay
- Auxiliary relay
- Remote terminal units
- Circuit breaker monitor
- Revenue meters
- Power quality monitors
- Phasor measurement units
- Communication alarm etc

SMART GRID COMMUNICATION NETWORK (SGCN)

- Communication Network to support these functionalities
    - Advanced Metering Infrastructure(AMI),
    - Demand Response (DR),
    - Electric Vehicles (EVs),
    - Wide-Area Situational Awareness (WASA),
    - distributed energy resources and storage,
    - distribution grid management, etc.

AMI

- Systems that measure, collect and analyze energy usage, from advanced devices such as electricity meters, gas meters, and water meters through various communication media.
  - Smart meters at the consumer's location
  - Fixed communication networks between consumers and service providers
  - Data reception and management systems that make the info available to the service provider (meter data management system or "MDMS")

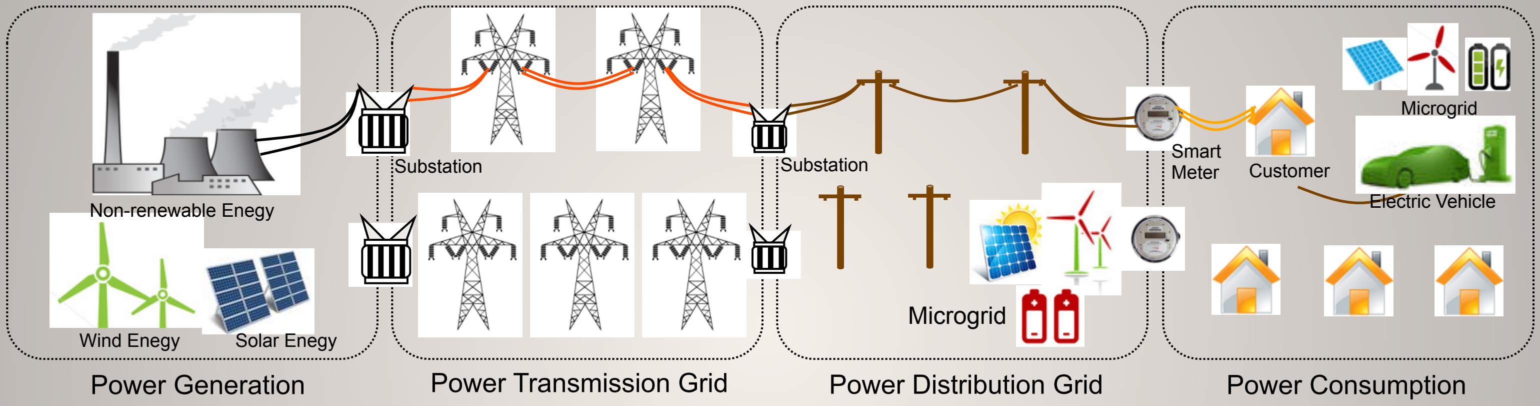
DEMAND RESPONSE

- Smart grid allows customers to shift load and to generate and store energy based on near real-time prices and other economic incentives.
- Customers can also sell extra stored energy back to the grid when the price is high.
- Such demand-response mechanisms help the grid balance power supply and demand, thus enhancing the efficiency of power usage.

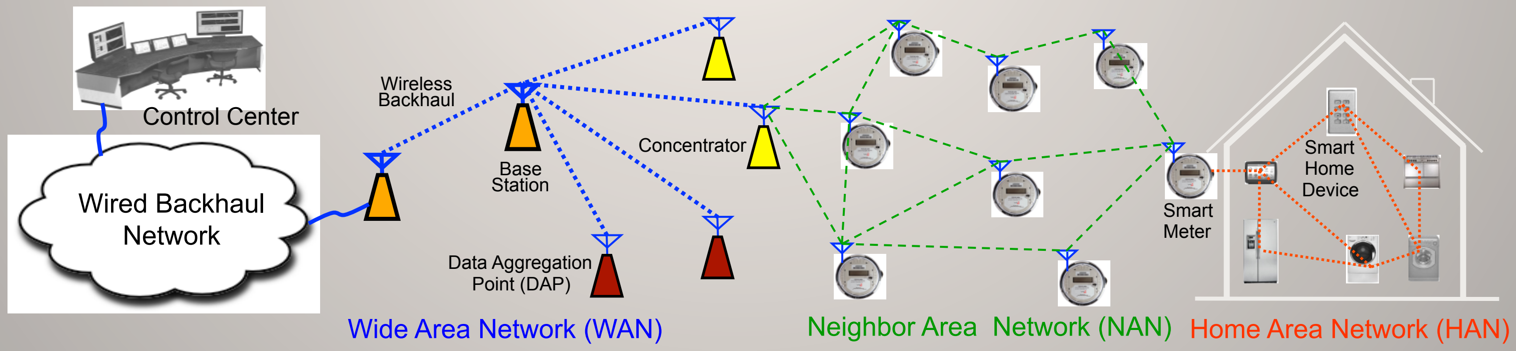
WASA

- Monitoring of the power system across large geographic areas
- Broad and dynamic picture of the functioning of the grid
- Optimize the management of power-network components, behavior, and performance
- Anticipate, prevent, or respond to problems before disruptions can arise

LAYERS

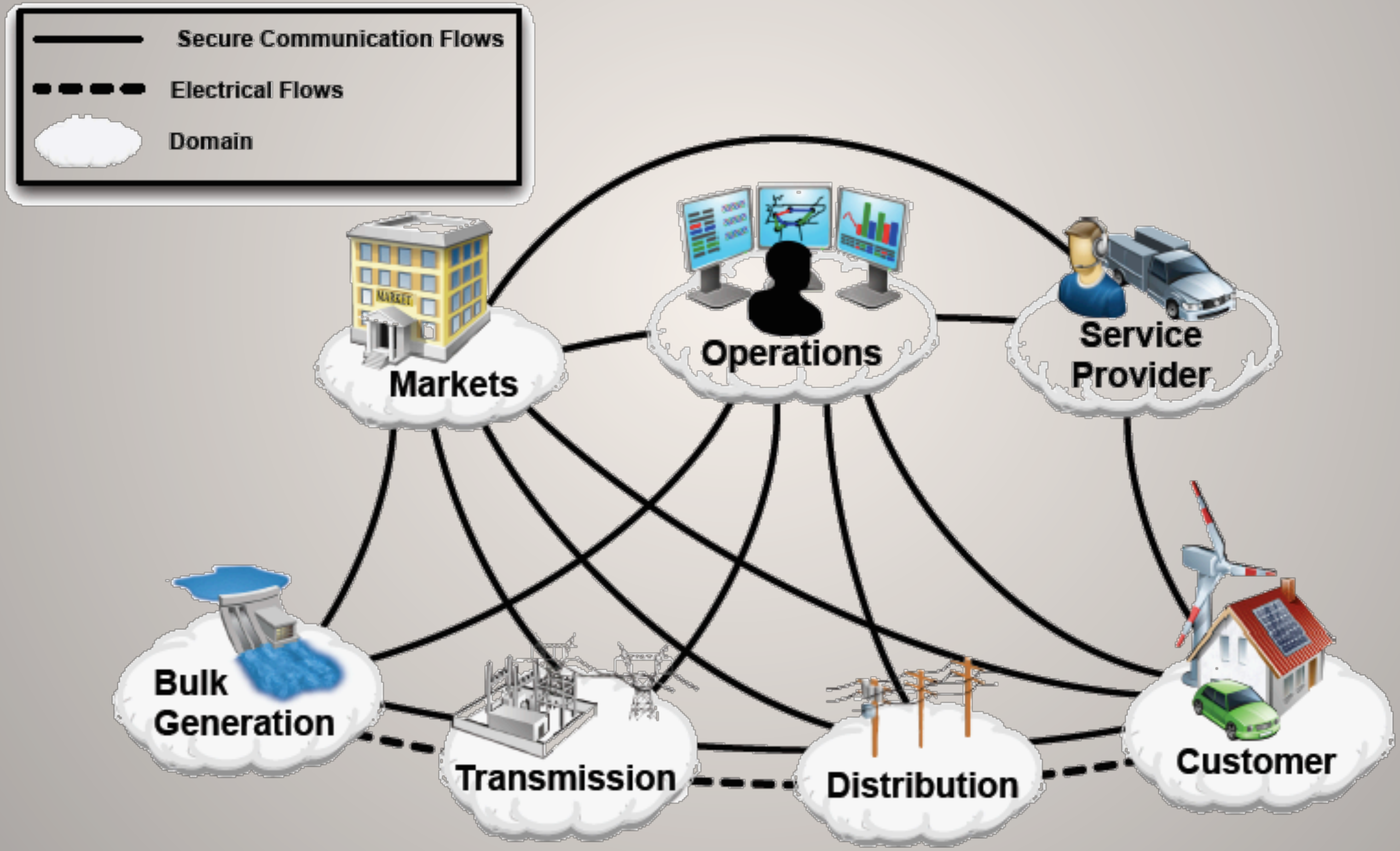


(a) Power System Layer



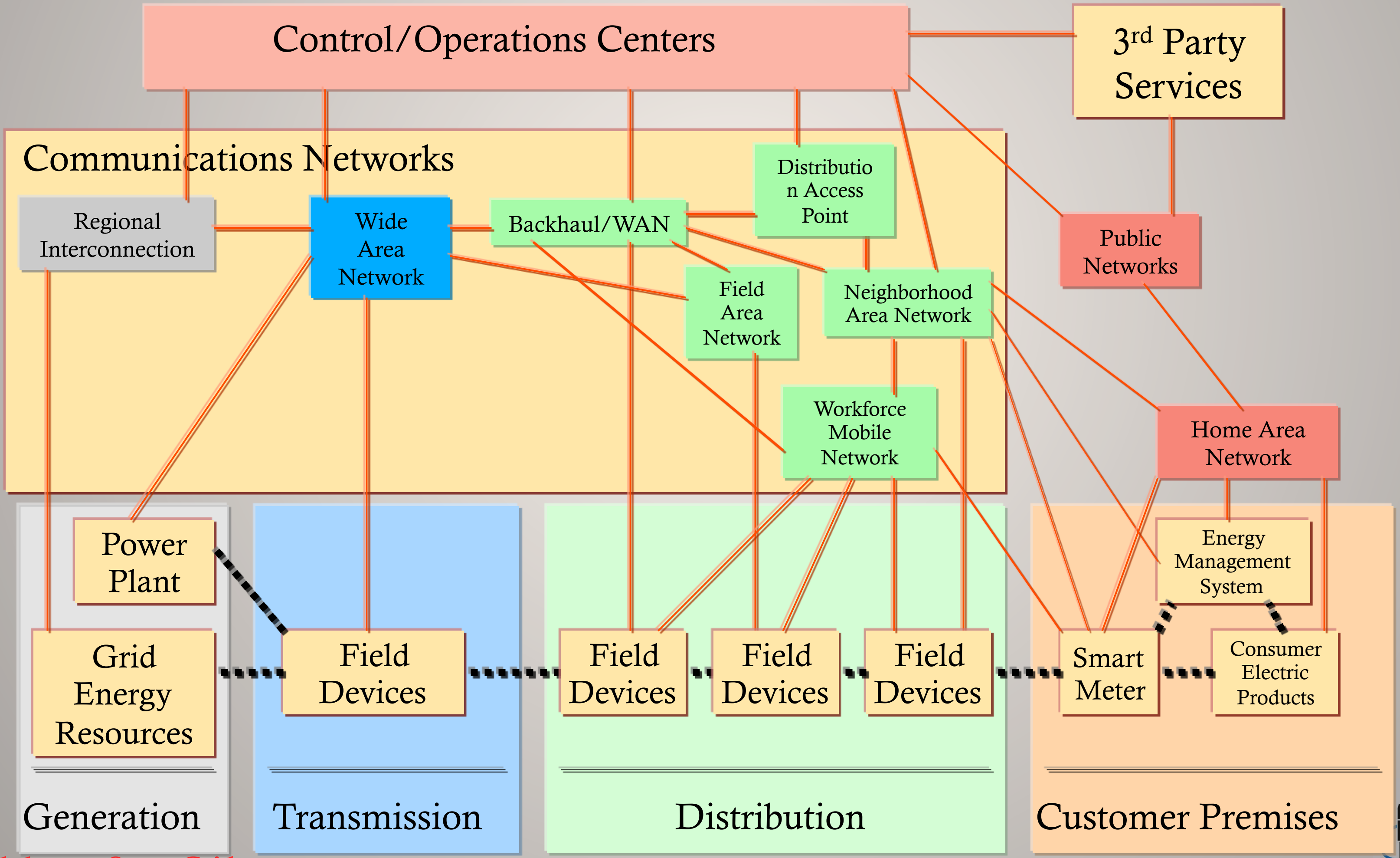
(b) Communications Layer

ARCHITECTURE



NIST Smart Grid Framework 1.0 January 2010

ARCHITECTURE



SCADA: COMPONENT OF OPERATIONS

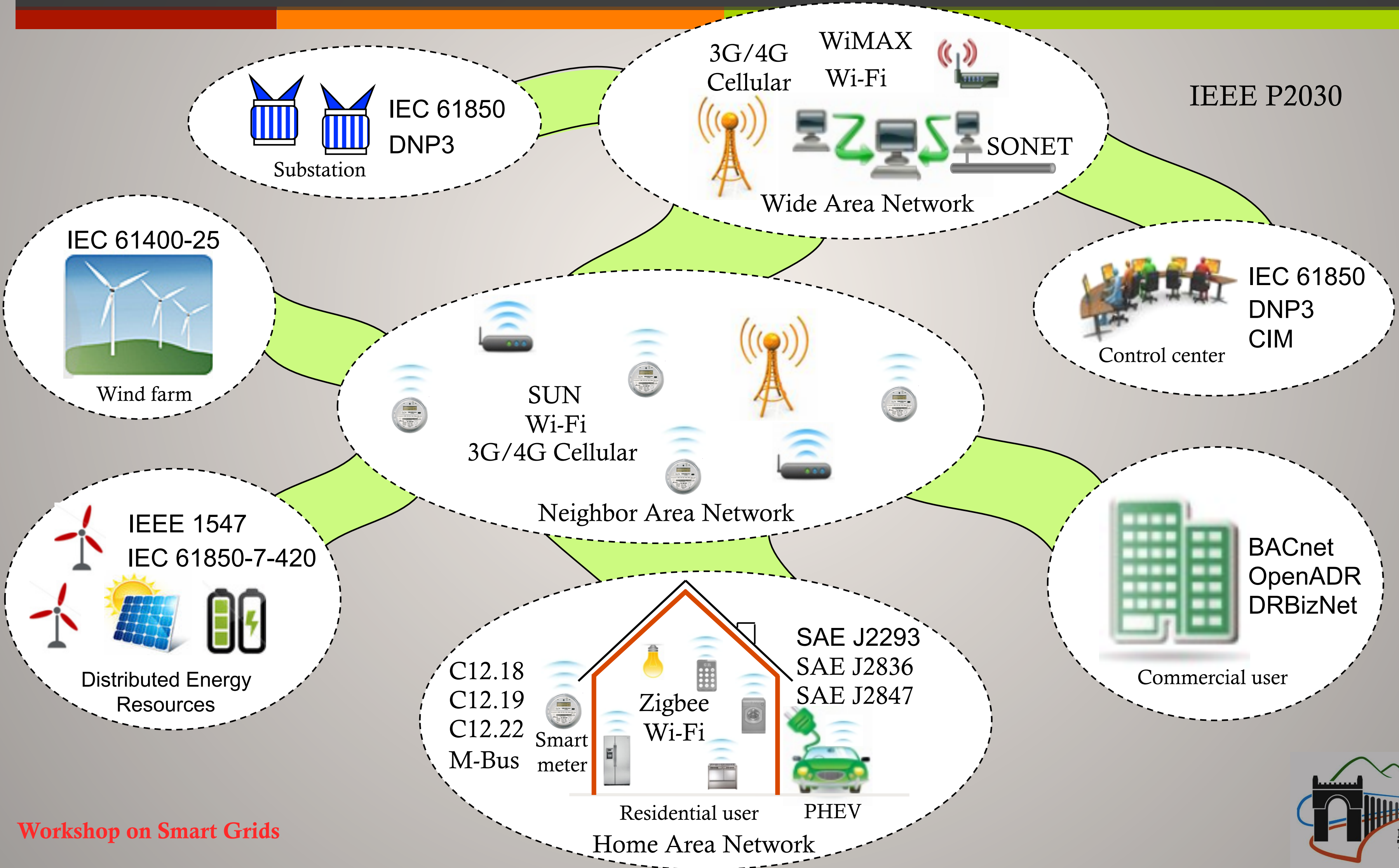
- SCADA (Distribution Supervisory Control and Data Acquisition)
  - A type of control system that transmits individual device status, manages energy consumption by controlling the devices.
  - Allows operators to directly control power system equipment.

Main Goal: Helping the grid reduce operation and maintenance costs and ensure reliability of power supply.

STANDARDS

- Standards Development Organizations (SDOs):
  - National Institute of Standards and Technology (NIST),
  - American National Standards Institute (ANSI),
  - International Electrotechnical Commission (IEC),
  - Institute of Electrical and Electronics Engineers (IEEE),
  - International Organization for Standardization (ISO),
  - International Telecommunication Union (ITU),
- Alliances:
  - ZigBee Alliance, Wi-Fi Alliance, HomePlug Powerline Alliance, Z-Wave Alliance, etc.

MAIN STANDARDS



NAN

- Huge number of devices
- Scalable and self-configurable
- Heterogeneous and location-aware
- Time-varying link conditions
- Reliability
- QoS
- Privacy and security

Open Issues in NAN

- Downlink Communications
- QoS Differentiation and Provisioning
- Network Self-healing
- Multicasting
- Cluster-based Routing
- Optimal Network Design

COMMUNICATION MEDIA

- PLC
- Wired
- Wireless
- Fiber
- Microwave

WIRELESS COMMUNICATION

Technology	Advantage	Disadvantage	Application
Zigbee (IEEE 802.15.4, ZigBee Alliance) Low-cost, low power, wireless mesh standard for wireless home area networks (WHANs) or wireless personal area networks (WPANs)	Very low cost - inexpensive consumer devices; Low power consumption - years of battery life; Self-organizing, secure, and reliable mesh network; Network can support a large number of users; Smart energy profile for HANs is available	Very short range; Does not penetrate structures well; Low data rates; Developers must join ZigBee Alliance	HANs for energy management and monitoring; Unlikely to be used in NANs
Wi-Fi (IEEE 802.11b/g/n) Indoor wireless local area networks (WLANs), wireless mesh networks	Low-cost chip sets - inexpensive consumer devices; Widespread use and expertise; Low-cost application development; Stable and mature standards	Does not penetrate cement buildings or basements; Small coverage and short distances limit wide spread use; Security issues with multiple networks operating in same locations	Could be used for HANs, MGANs, and NANs
3G Cellular (UMTS, CDMA2000, EV-DO, EDGE) Wide-area wireless networks for voice, video, and data services in a mobile environment	Expensive infrastructure already widely deployed, stable and mature; Well standardized; Equipment prices keep dropping; Readily available expertise in deployments; Cellular chipset very inexpensive; Large selection of vendors and service providers	Utility must rent the infrastructure from a cellular carrier for a monthly access fee; Utility does not own infrastructure; Technology is in the transition phase to LTE deployment; Public cellular networks not sufficiently stable/secure for mission critical/utility applications; Not well-suited for large data/high bandwidth applications	AMI Backhaul, Field Area Network (FAN)
LTE Enhancements to 3G Universal Mobile Telecommunications System (UMTS) mobile networking, providing for enhanced multimedia services	Low latency, high capacity; Fully integrated with 3GGP, compatible with earlier 3GPP releases; Full mobility for enhanced multimedia services; Carrier preferred protocol; Low power consumption	Utility must rent the infrastructure from a cellular carrier for a monthly access fee; Utility does not own infrastructure; Not readily available in many markets/ still in testing phases in others; Equipment cost high; Vendor differentiation still unclear; Lack of expertise in designing LTE networks; Utilities’ access to spectrum	AMI Backhaul, SCADA Backhaul, Demand Response, FAN, Video Surveillance
WiMAX (IEEE 802.16) Wireless metropolitan area network (MAN) providing high-speed fixed/mobile Internet access	Efficient backhaul of data – aggregating 100’s access points; QoS supports service assurance; Battery-backup improves reliability and security; Simple, scalable network rollout and customer-premises equipment (CPE) attachment; Faster speeds than 3G cellular; Large variety of CPE and gateway/ base station designs	Limited access to spectrum licenses in the US; Trade off between higher bit rates over longer distances; Asymmetrical up and down link speeds; User shared bandwidth; Competing against future 4G cellular	AMI Backhaul, SCADA Backhaul, Demand Response, FAN, Video Surveillance

SECURITY

WHY?

- Network security is a priority and not a add on for smart grids
- Protecting control center alone - not enough
- Remote access to devices
- QoS requirement from security system
- Safety (line worker public and equipment)
- Reliability and availability

Unique Challenges

- Scale
- Legacy devices
- Field location
- Culture of security through obscurity
- Evolving standards and regulations

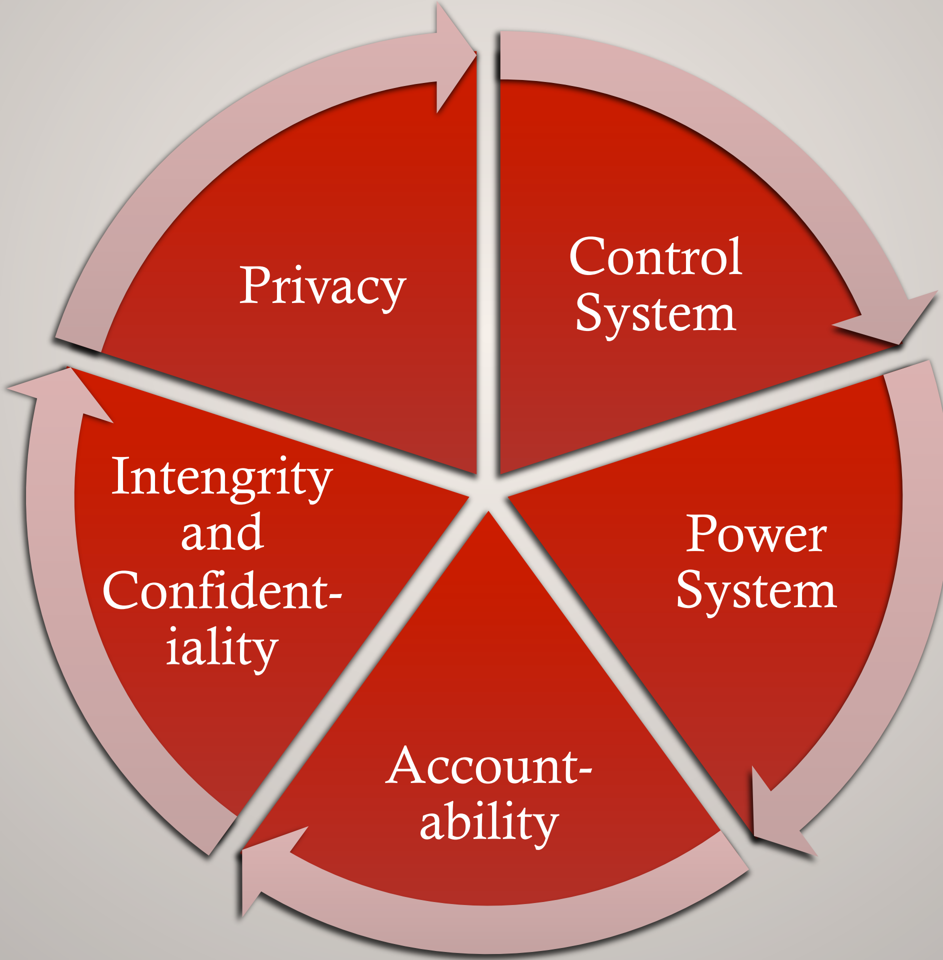
ADVERSARIES

- Nation states
- Hackers
- Terrorist /Cyber terrorists
- Organized crime
- Other criminal elements
- Industrial competitors
- Disgruntled employees
- Careless and poorly trained employees

SOLUTIONS

- Security by obscurity
- Trust no one
- Layered security framework
- Efficient firewall
- Intrusion detection
- Self healing security system

SECURITY



Privacy

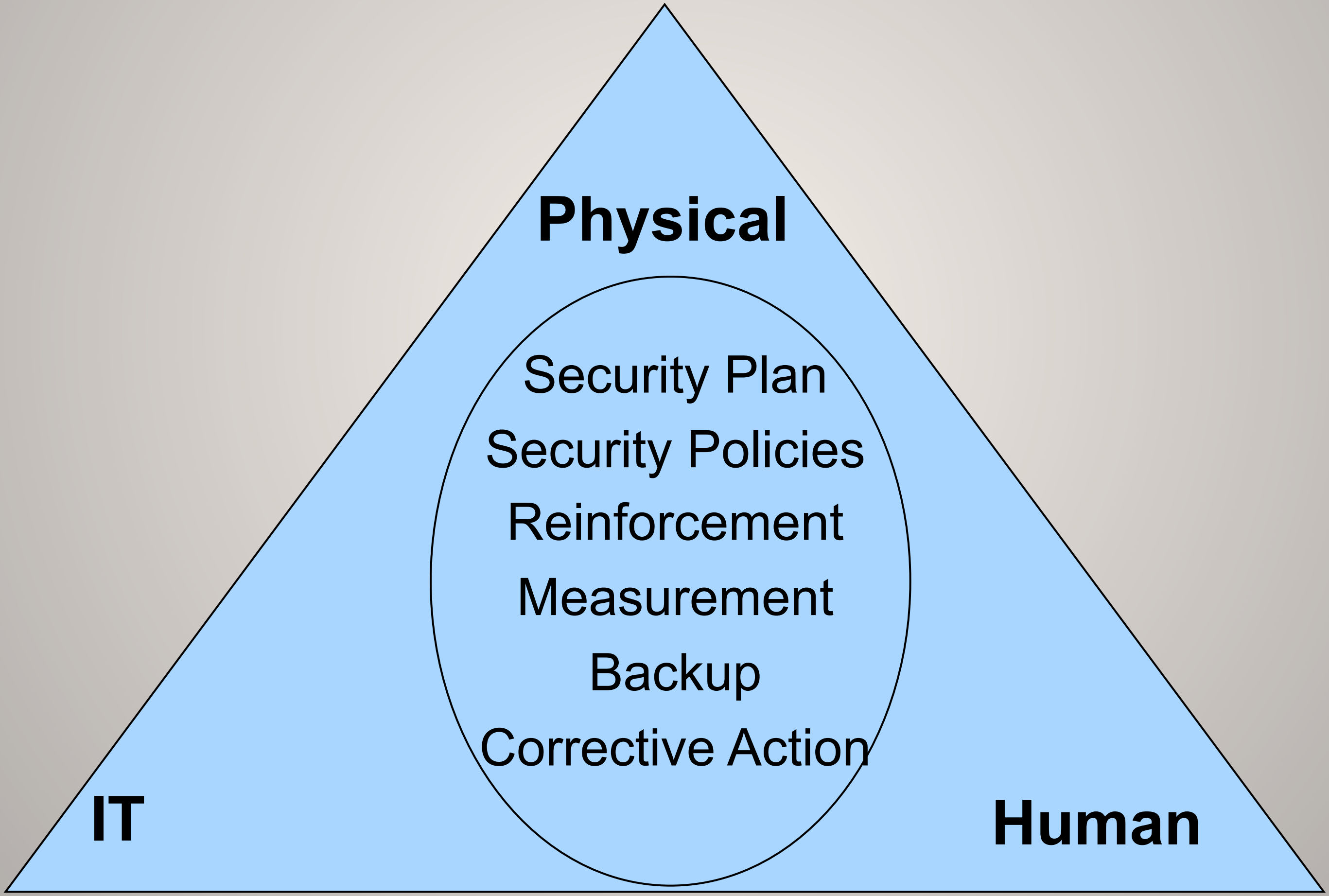
Control System

Power System

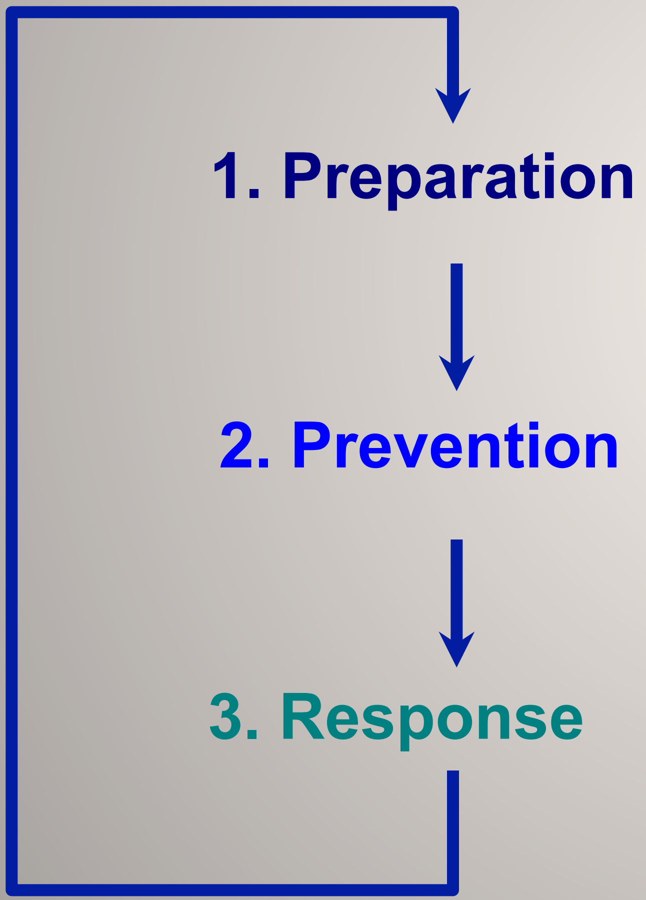
Account-ability

Intengrity and Confident-iality

HOLISTIC APPROACH



SECURITY LIFECYCLE



- Preparation
  - create/review policy statements
  - conduct a risk analysis
  - establish/review security team structure
- Prevention
  - deploy security countermeasures
  - approve security changes
  - monitor security posture
- Response
  - respond to security violations
  - restoration
  - review

DEFENSE IN DEPTH

- Perimeter Protection
  - Firewall, IPS, VPN, AV
  - Host IDS, Host AV
  - DMZ
- Interior Security
  - Firewall, IDS, VPN, AV
  - Host IDS, Host AV
  - IEEE P1711, IEC 62351
  - NAC
  - Scanning
- Monitoring
- Management
- Processes

IDS	Intrusion Detection System
IPS	Intrusion Prevention System
DMZ	DeMilitarized Zone
VPN	Virtual Private Network (encrypted)
AV	Anti-Virus (anti-malware)
NAC	Network Admission Control

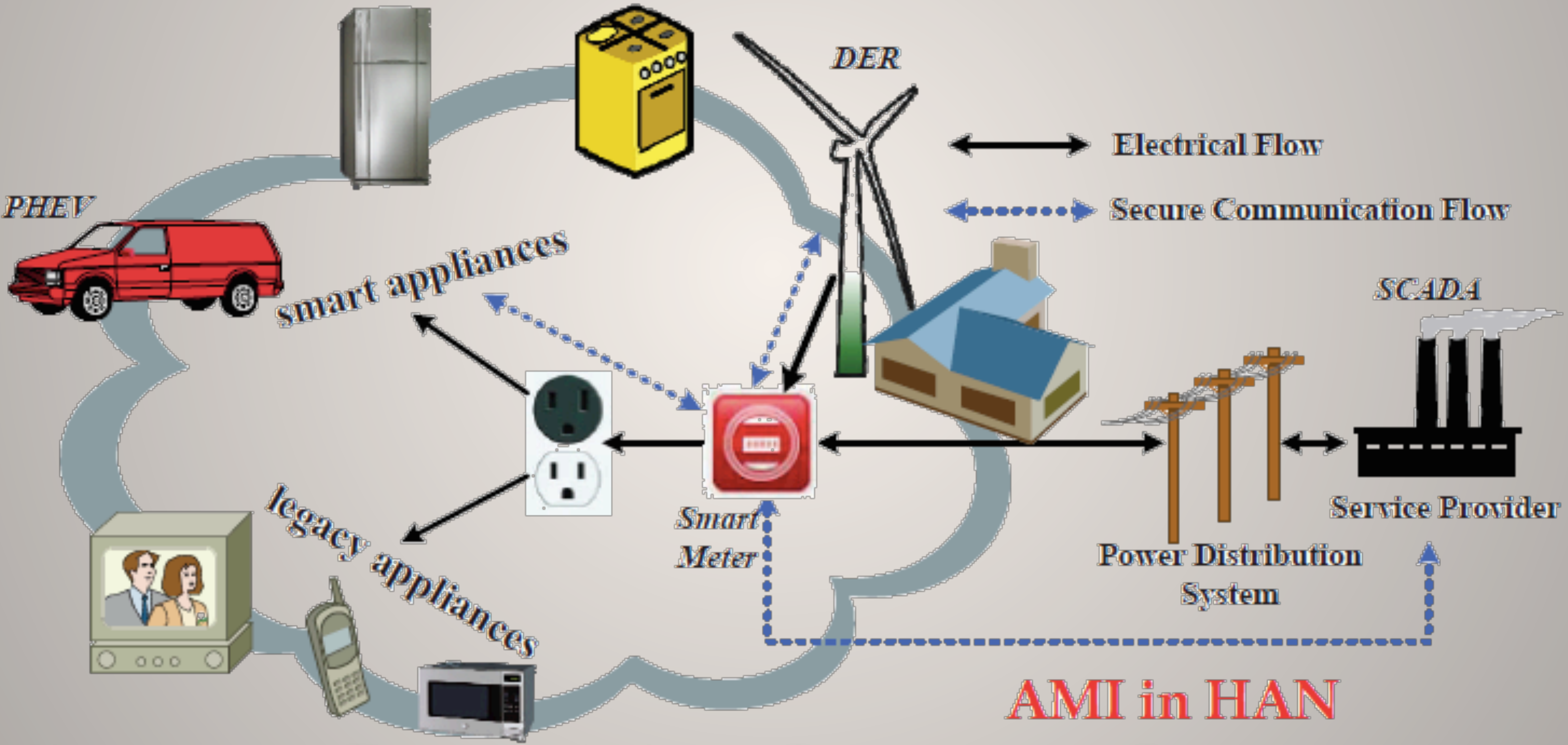
SCADA SECURITY ISSUES

- Distribution control commands and access logs are critical for SCADA systems. Intercepting, tampering, or forging these data damages the grid.
  - Possible solutions: Ensure all commands and log files are accurate and secure.
- Synchronizing time-tagged data in wide areas is essential; without it the safety and reliability of the SCADA system cannot be achieved.
  - Possible solutions: Use a common time reference for time synchronization.

SCADA ISSUES

- Every decision of SCADA comes from the analysis of the raw data based on a reasonable model. Improper models may mislead operator actions. In addition, different vendors using distinct SCADA models will disrupt the consistency of the grid.
  - Possible solutions: So far, none.
- Other security issues ?

AMI IN HAN



PHEV; Plug-in Hybrid Electric Vehicle

DER: Distributed Energy Resource

HAN: Home Area Network

AMI: Advanced Metering Infrastructure

SMART METER SECURITY

- Issues:
  - Physical attacks
  - Remote connect/disconnect
  - Metering database breaches
- Solutions:
  - Ensure integrity of data
  - Detect unauthorized changes on meter
  - Authorized access to AMI

PHEV SECURITY

- Problems:
  - Location aware
  - Inaccurate billing
- Solutions:
  - PHEV standards needed

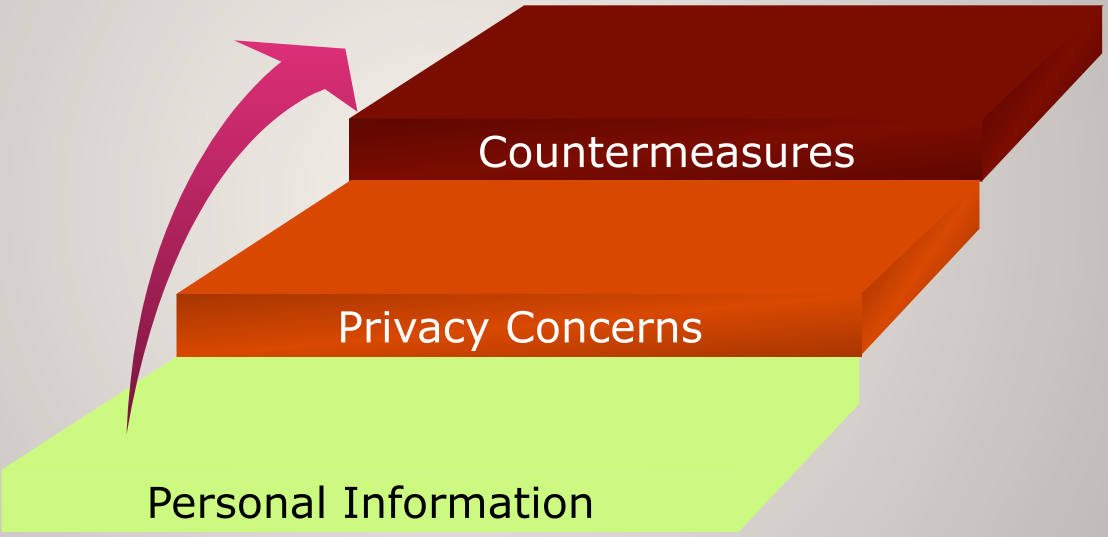
TEMPORAL INFORMATION

- Problems:
  - Replay attacks
  - Timestamps
- Solutions:
  - PMUs
  - Forensic technologies

DATA AND SERVICE

- Problems:
  - The accuracy of transmitted data and the quality of services therefore can not be guaranteed
- Solutions:
  - Fraud detection algorithms and models

PRIVACY



Countermeasures

Privacy Concerns

Personal Information

PERSONAL INFORMATION

- NIST guidelines have provided a list of personal information that may be available through the smart grid as follows:
  - Name: responsible for the account
  - Address: location to which service is being taken
  - Account number: unique identifier for the account
  - Meter IP, Meter reading, current bill, billing history
  - Lifestyle; when the home is occupied and it is unoccupied, when occupants are awake and when they are asleep, how many various appliances are used, etc.
  - DER: the presence of on-site generation and/or storage devices, operational status, net supply to or consumption from the grid, usage patterns.
  - Service Provider: identity of the party supplying this account, relevant only in retail access markets.

PRIVACY CONCERNS

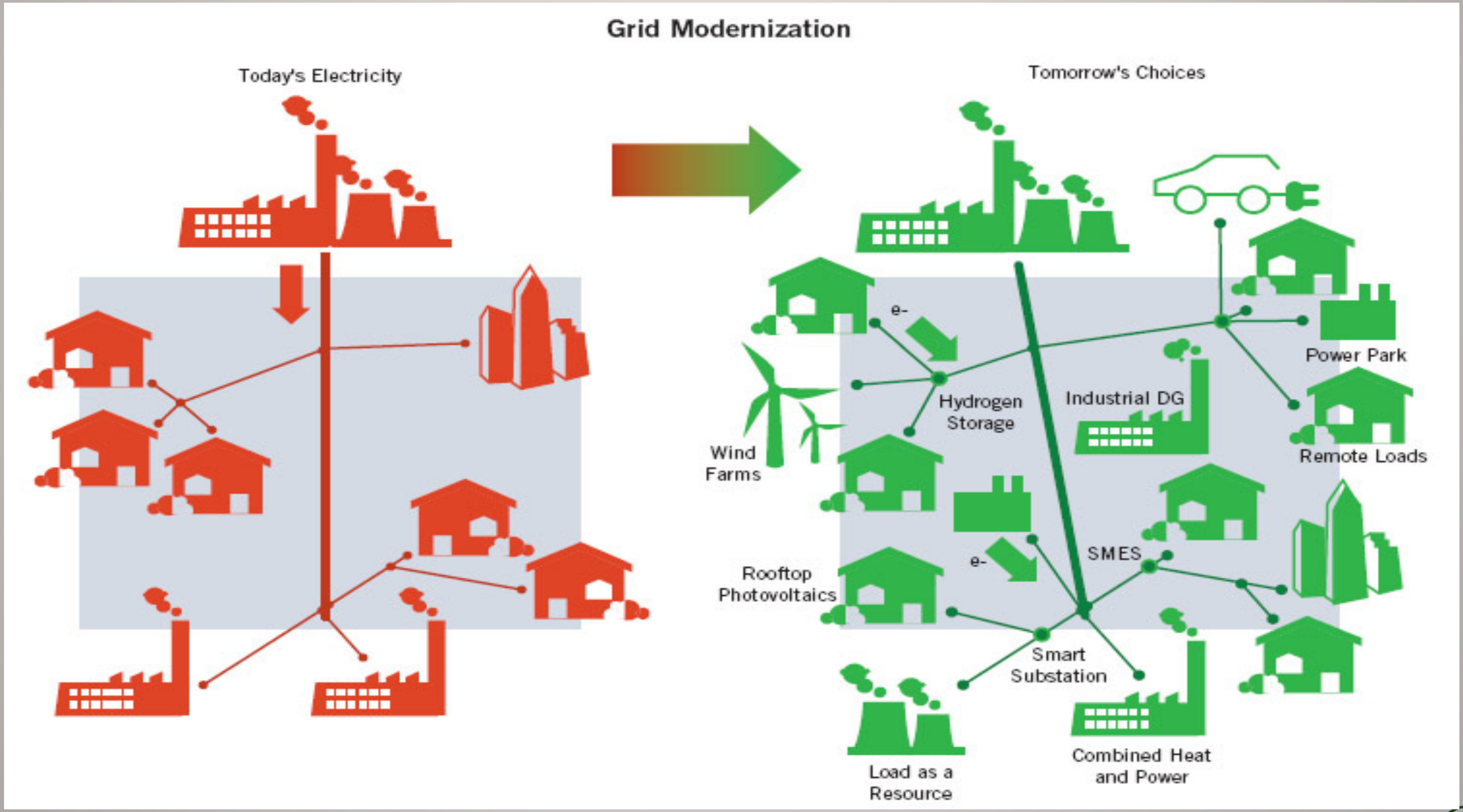
- Energy consumption data obtained by a third party may disclose personal information without one's permission[1].
  - Firstly, data in the smart meter and HAN could reveal certain activities of home smart appliances, e.g., appliance vendors may want this kind of data to know both how and why individuals used their products in certain ways.
  - Secondly, obtaining near real-time data regarding energy consumption may infer whether a residence or facility is occupied, what they are doing, and so on.
  - Thirdly, personal lifestyle information derived from energy use data could be valuable to some vendors or parties, e.g., vendors may use this information for targeted marketing, which could not be welcomed by those targets

COUNTERMEASURES

- An organization should ensure that information security and privacy policies exist and are documented and followed. Audit functions should be present to monitor all data accesses and modifications.
- Before collecting and sharing personal information and energy use data, a clearly-specified notice should be announced.
- Organizations should ensure the data usage information is complete, accurate, and relevant for the purposes identified in the notice.
- Personal information in all forms, should be protected from unauthorized modification, copying, disclosure, access, use, loss, or theft.

TRADING

Diverse Energy Sources



Electricity Market

- Current practice: Fixed market
  - Few producers, less competition
  - Regulated by government
- The future : **Free market**
  - Many producers (wind, solar, …)
  - Less regulation

Goal

- Setup an Electricity market
  - Self interested (producer, buyer, grid owner)
  - Free (no central regulation)
  - Efficient (no overload, no shortage)

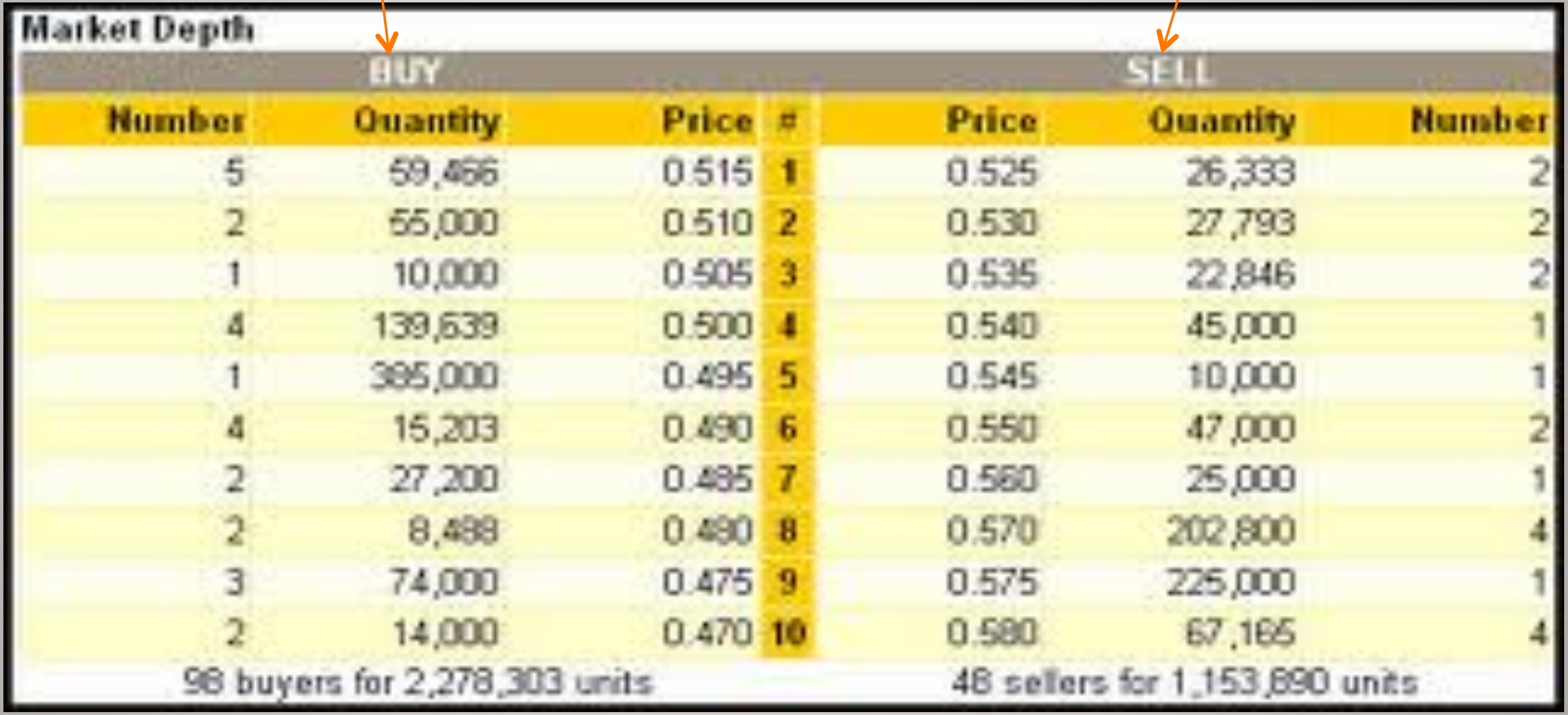
Design

- Trading Mechanism
  - Buy/sell electricity
- Overload Prevention Mechanism
  - Transmission charge
- Online Balancing Mechanism
  - Price for extra demand and supply in real-time

Stock Market

Buy orders

Sell orders



Market Depth

BUY				SELL		
Number	Quantity	Price	#	Price	Quantity	Number
5	59,466	0.515	1	0.525	26,333	2
2	55,000	0.510	2	0.530	27,793	2
1	10,000	0.505	3	0.535	22,846	2
4	139,639	0.500	4	0.540	45,000	1
1	385,000	0.495	5	0.545	10,000	1
4	15,203	0.490	6	0.550	47,000	2
2	27,200	0.485	7	0.560	25,000	1
2	8,488	0.480	8	0.570	202,800	4
3	74,000	0.475	9	0.575	225,000	1
2	14,000	0.470	10	0.580	67,165	4

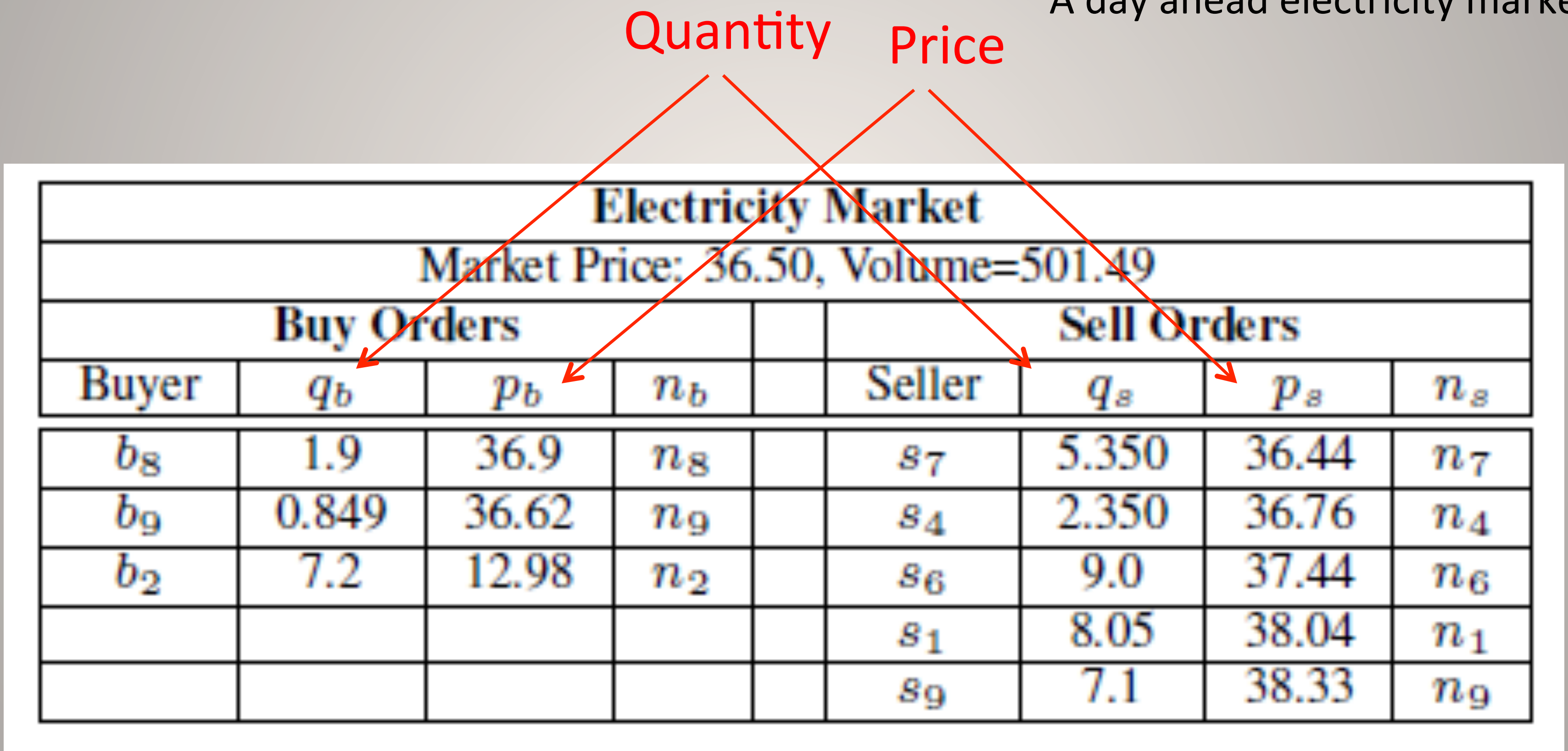
98 buyers for 2,278,303 units

48 sellers for 1,153,890 units

- Market order : buy or sell at market price
- Limit order : specify price to sell or buy

Proposed Electricity Trading

A day ahead electricity market



Quantity

Price

Electricity Market

Market Price: 36.50, Volume=501.49

Buy Orders					Sell Orders			
Buyer	q_b	p_b	n_b		Seller	q_s	p_s	n_s
b_8	1.9	36.9	n_8		s_7	5.350	36.44	n_7
b_9	0.849	36.62	n_9		s_4	2.350	36.76	n_4
b_2	7.2	12.98	n_2		s_6	9.0	37.44	n_6
					s_1	8.05	38.04	n_1
					s_9	7.1	38.33	n_9

- A day ahead market
  - Based on prediction of a day ahead demand/supply

Overload Prevention Mechanism

- Charging transmission (line charge = p_t)
  - Protect **overload** because
    - If p_t is high then demand goes down
    - If p_t is low then demand goes high
  - Line charge is geographically different depending on congestion

Online Balancing Mechanism

- Balancing unpredictable demand/supply on real-time basis
  - + demand
    - need to buy at market price
  - - demand
    - Need to sell at market price
  - - supply
    - Buyer need to buy at market price

Evaluation

- How efficient the market is?
- What's the best trading strategy?

Market Efficiency

- Efficient-market hypothesis (EMH)
  - If all information (buyer's and seller's cost structure) is *publicly available*
  - Market price is determined solely by supply/demand
    - ➔ maximally efficient market
- Cost structure
  - Buyer : minimum and cost sensitive dynamic demand
  - Seller : minimum and quantity proportional production cost
  - Line owner : minimum and quantity proportional cost

Indian Institute of Technology Mandi

Trading Strategy

- Maximum efficiency is not possible
  - Hidden cost information
  - Line charge constraint

CONCLUSIONS

- Communication is an essential part of smart grid
- Security is a crucial concern.

Questions?