

## Securing The Electric Grid of The Future

Smart Grid Info Sharing Call/Webcast  
November 29<sup>th</sup> 2010

Erfan Ibrahim, PhD  
Technical Executive  
Power Delivery & Utilization

# Electric Power Research Institute

Collaboration.....Technical Expertise....Thought Leader



- Not for profit, collaborative electricity research organization with more than 450 participants in over 40 countries
- US utilities that are members of EPRI produce over 90% of the electricity generated in the nation
- Independent electricity research in:
  - Generation
  - Environment
  - Power Delivery & Energy Utilization
  - Nuclear
- 1600+ R&D projects annually, ~\$400M R&D funding, more than 400 engineers and scientists

# IntelliGrid: R&D to Develop the Foundation of Smart Grid

- Smart Grid Requirements gathering methodology
- Standards assessment and contribution
- Information model to facilitate systems integration
- Communication technology assessment
- Security Policy for smart grid applications



# Intelligrid Structure

**PS 161A – Tech transfer, Technology Watch, Industry Coordination**

**PS 161B – Infrastructure for Smart Transmission Systems**

**PS 161C – Infrastructure for Smart Distribution Systems**

**PS 161D – Infrastructure for Smart Customer Interface**

**PS 161E – Infrastructure Security**

# EPRI's IntelliGrid R&D Program

## Largest Funded Collaborative R&D Program in Smart Grid

### U.S. Utilities

- 2010 Membership includes over 35 utilities in North America

### International Utilities

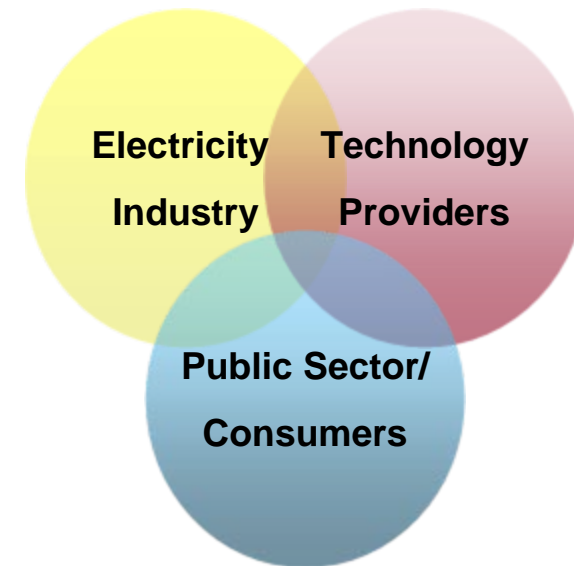
- Electricite de France
- Polish Power Grid Company
- Iberdrola

### Manufacturers

- ABB
- Siemens
- Cisco
- Symantec

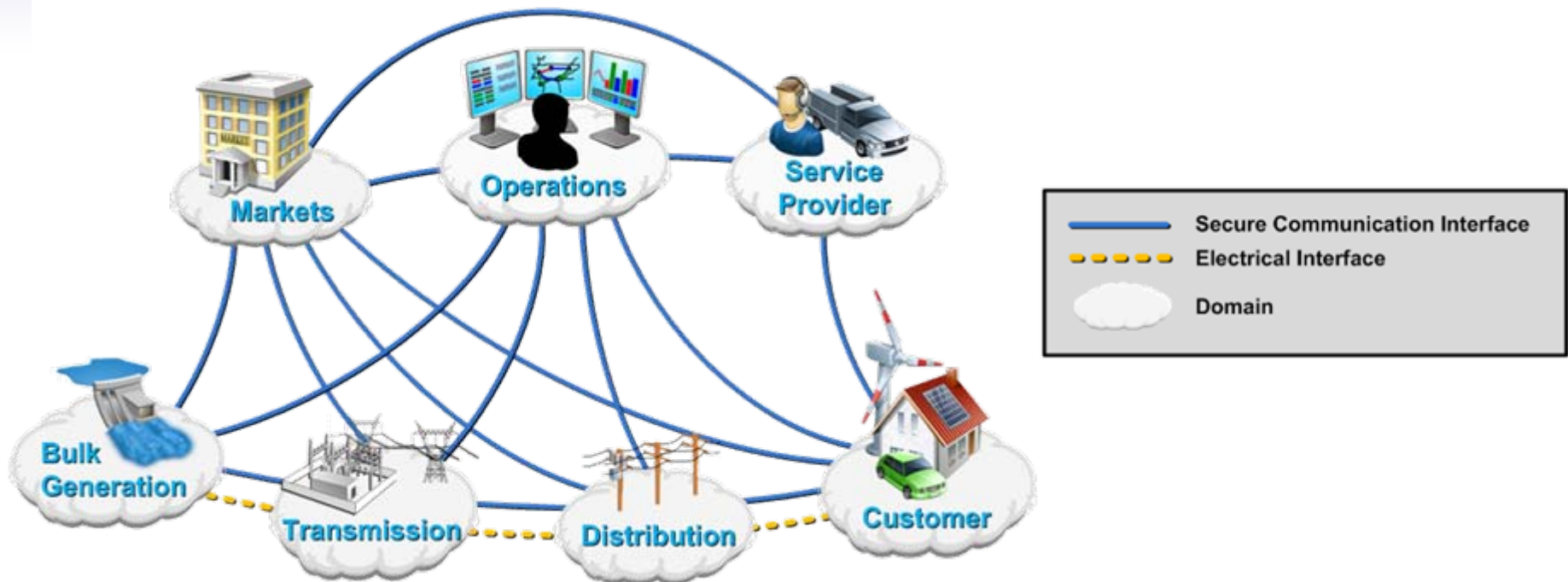
### Public Agencies

- Association of State Energy Research and Technology Transfer Institutions
- International Brotherhood of Electrical Workers
- National Association of Regulatory Utility Commissioners
- National Association of State Energy Officials
- National Conference of State Legislatures
- National Governors Association
- State Energy Offices and Research Programs
- Department of Energy
- NIST
- DHS
- NERC



# Securing the Electric Grid of the Future

## Sensors....Two Way Communications....Intelligence



### Acting on this Information Will:

Enable active participation by consumers

Anticipate & respond to system disturbances (self-heal)

Accommodate all generation and storage options

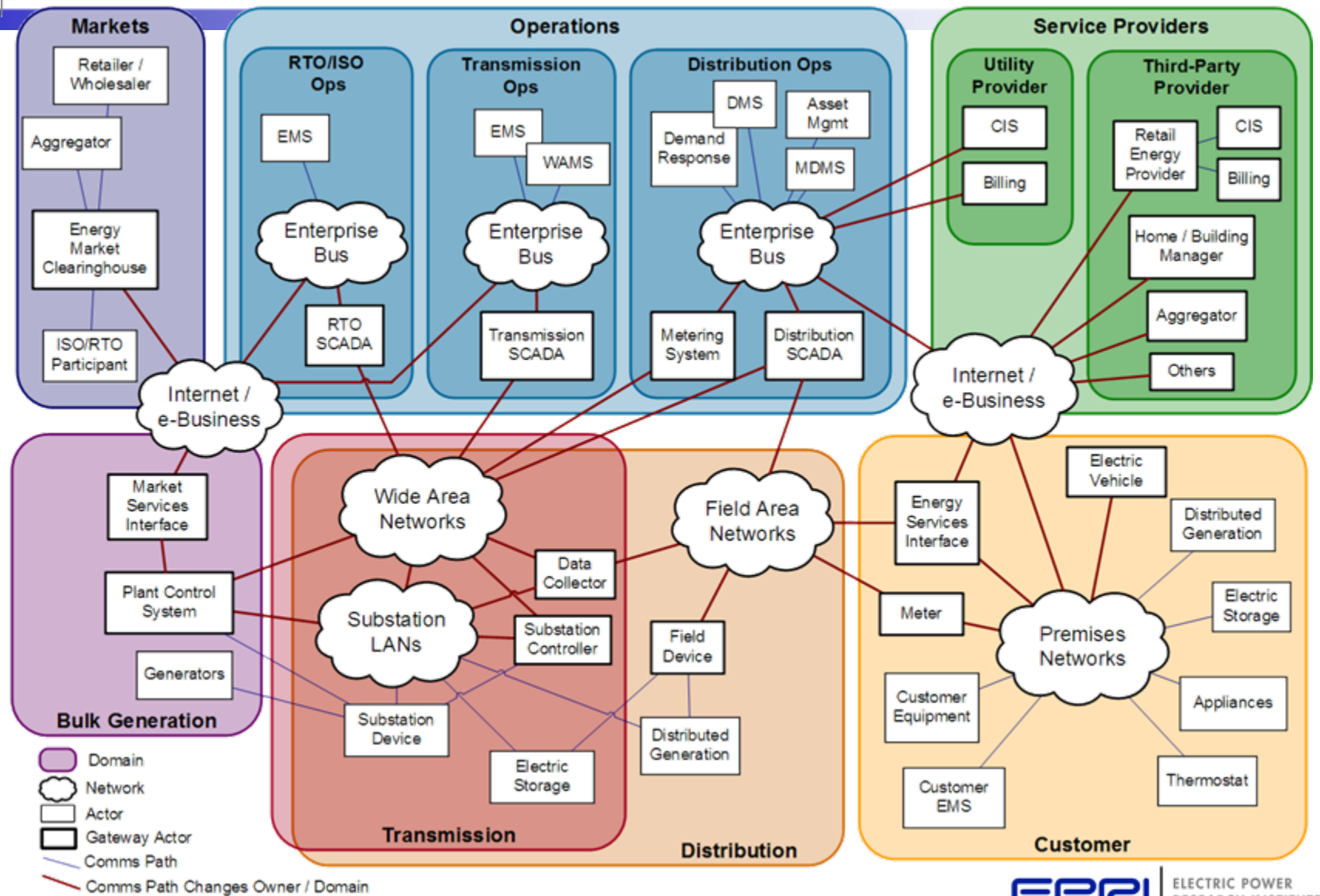
Operate resiliently against attack and natural disaster

Enable new products, services and markets

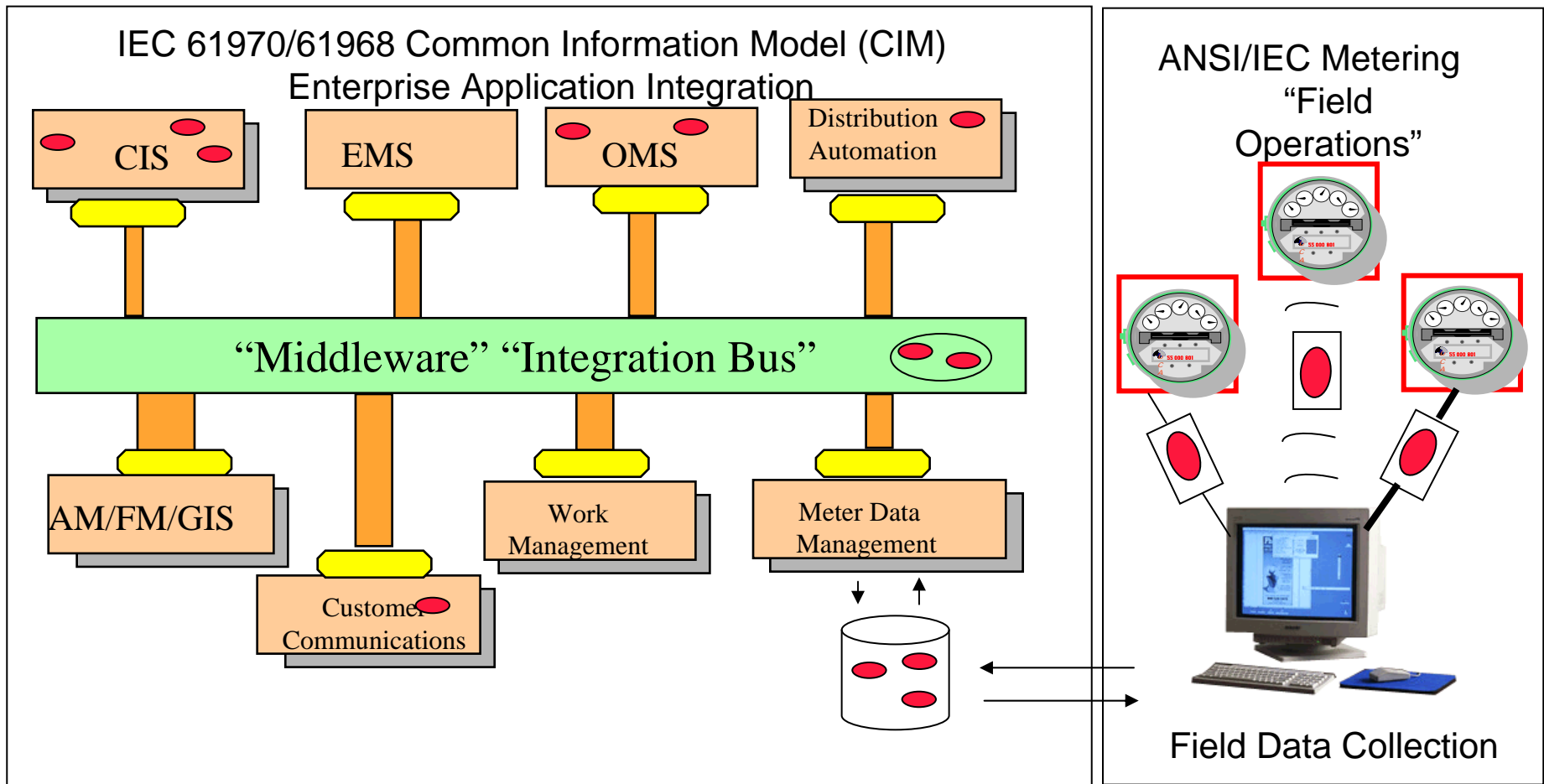
Optimize asset utilization and operate efficiently

Provide power quality for the digital economy

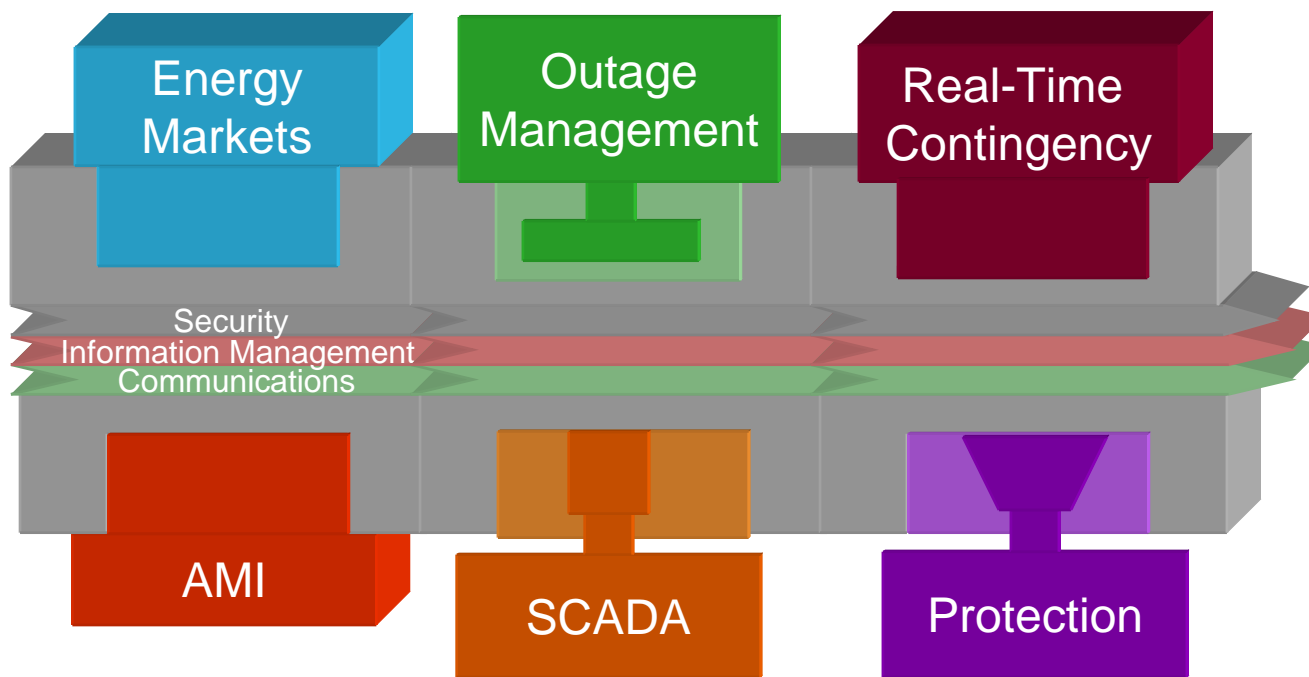
# Future Grid Example Architecture (Defense in Depth)



# Developing the Common Information Model (CIM) for Distribution Applications



# Security – Cross Cutting Concept



## *Foundation of the Future Electric Grid*

Security

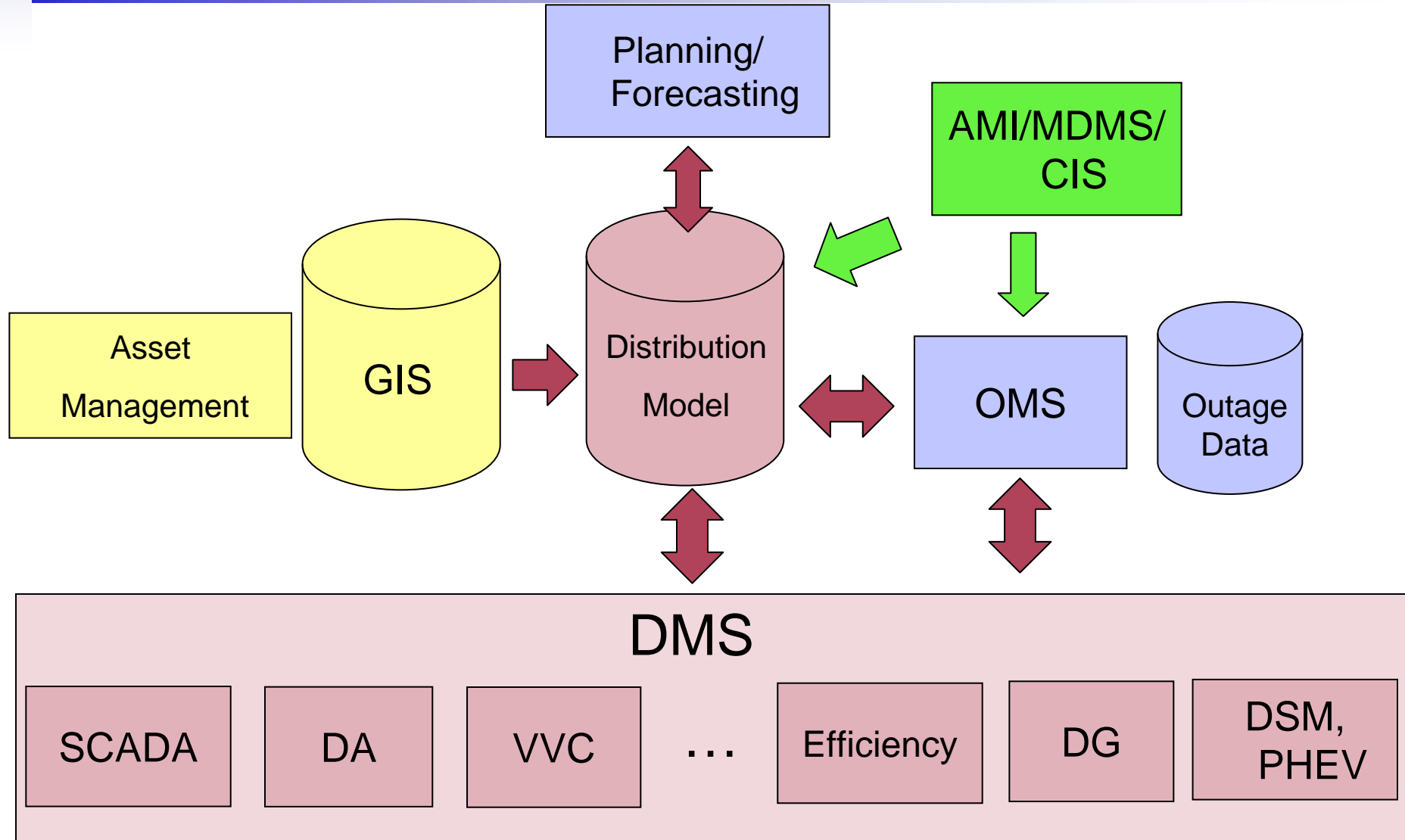
Information Management

Communications

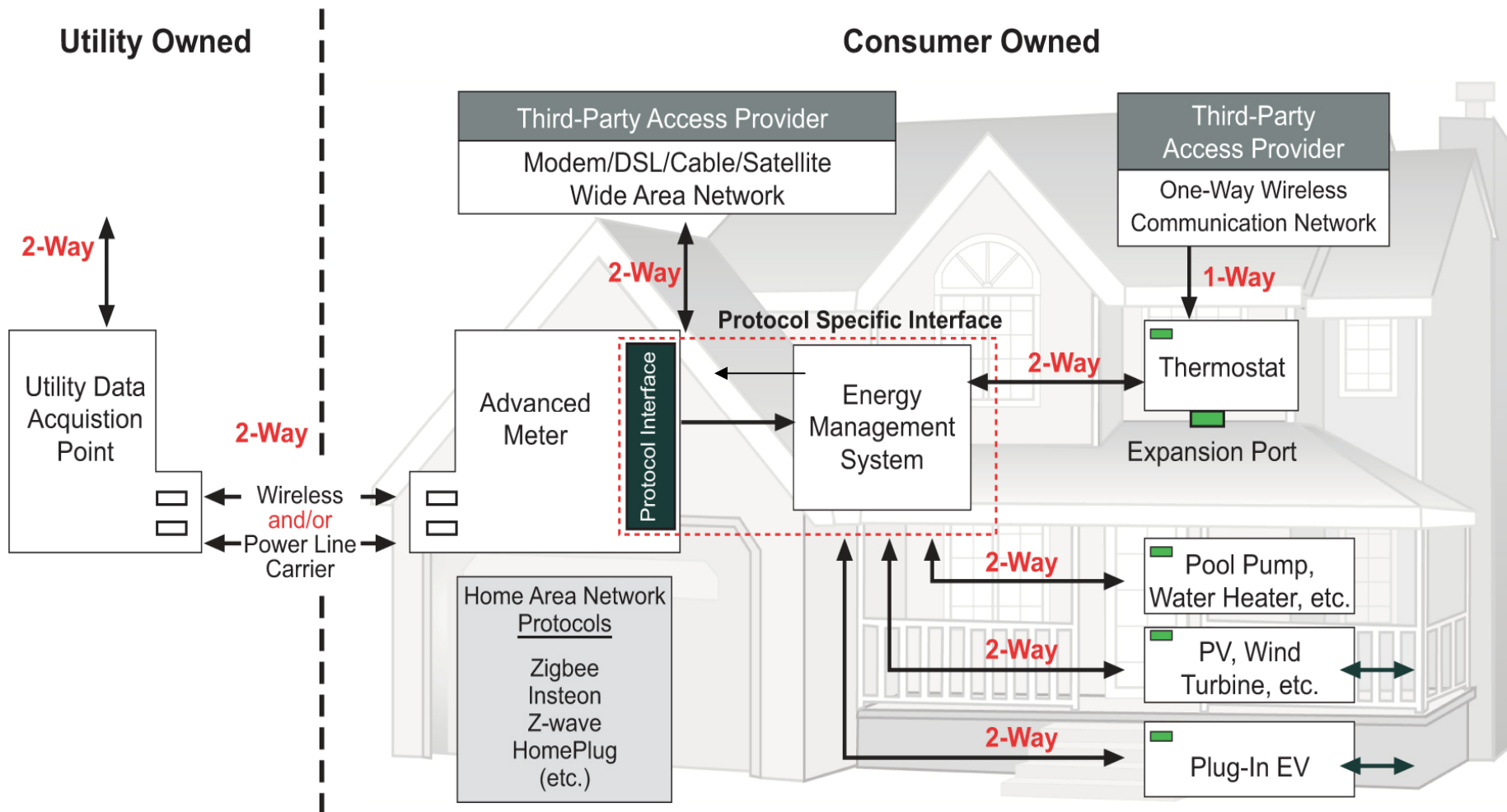
Interoperability

Systems Engineering Methodology

# Vision for Distribution Management System integration with Smart Grid

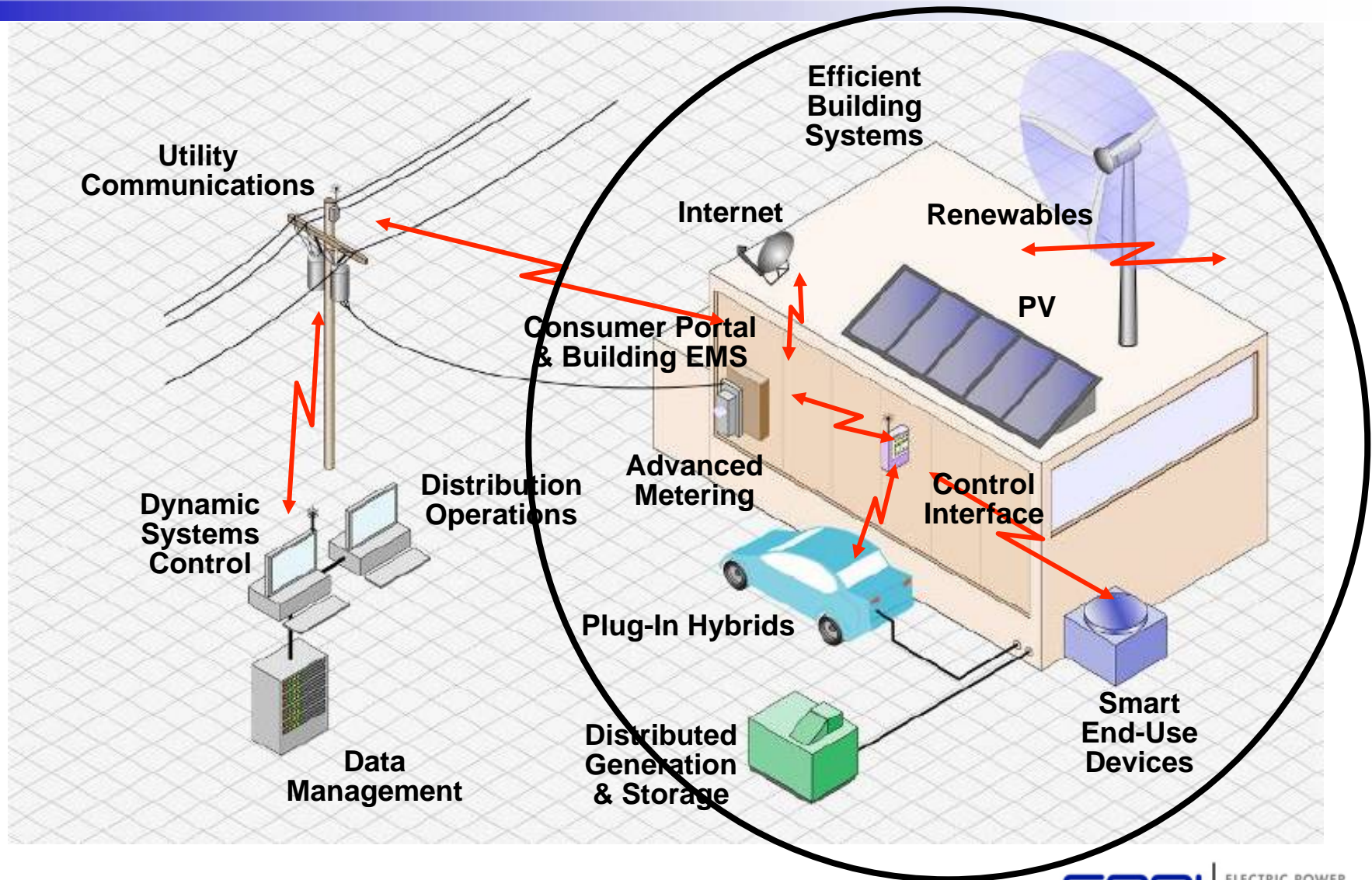


# General HAN Communication Network Architecture & Cyber Security Issues



Courtesy CEC/PIER April 2007

# Smart Grids and Local Energy Networks



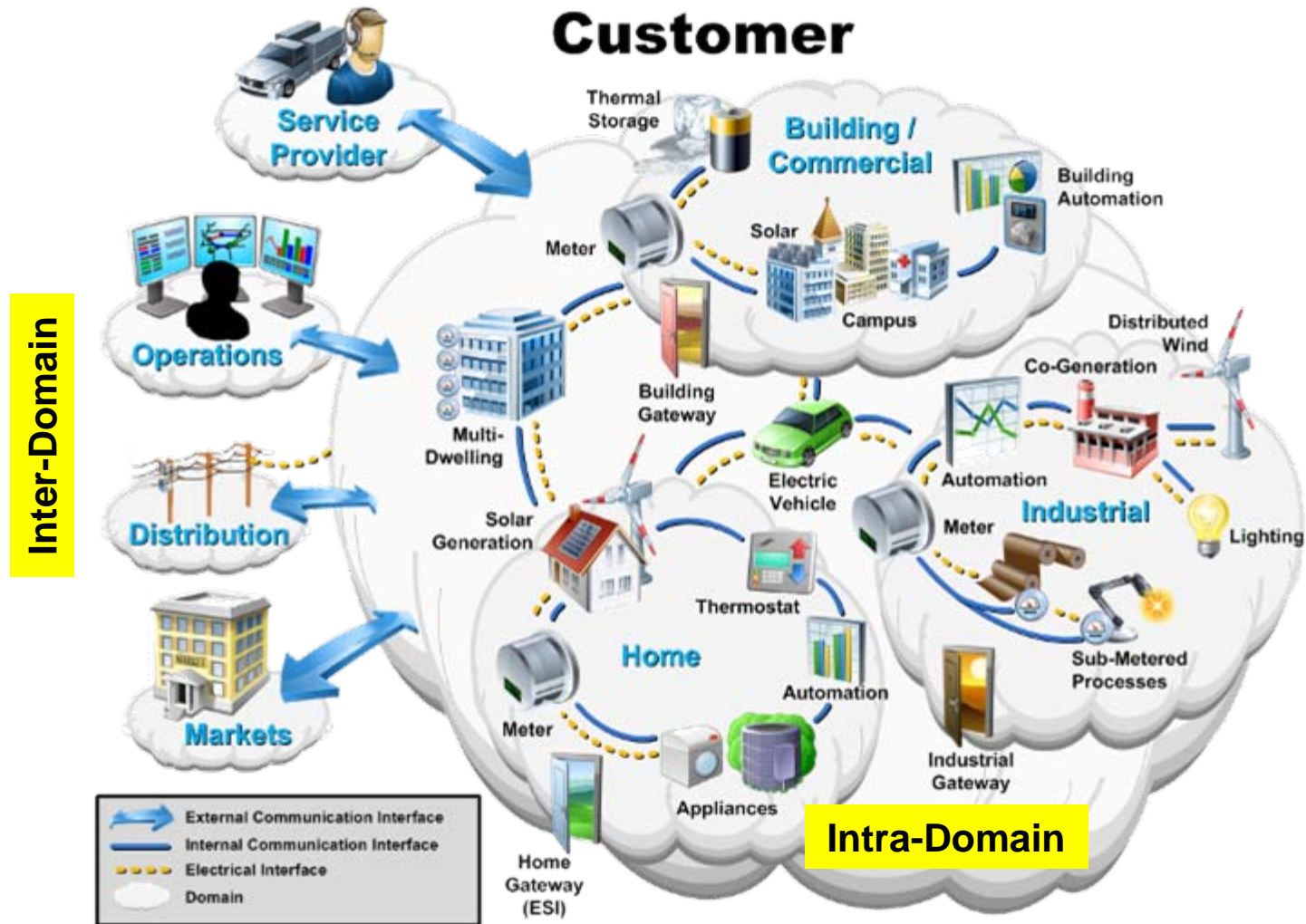
# Core Attributes of Cyber Security

- Confidentiality (e.g. Encryption, VPN, Authentication, etc.)
- Integrity (Digital Signatures, Check Sum, etc.)
- Availability (e.g. % uptime of critical applications)
- Reliability (e.g. Probability of successful transmission over time)
- Accountability (e.g. Digital Signatures, Honey Pots, etc.)

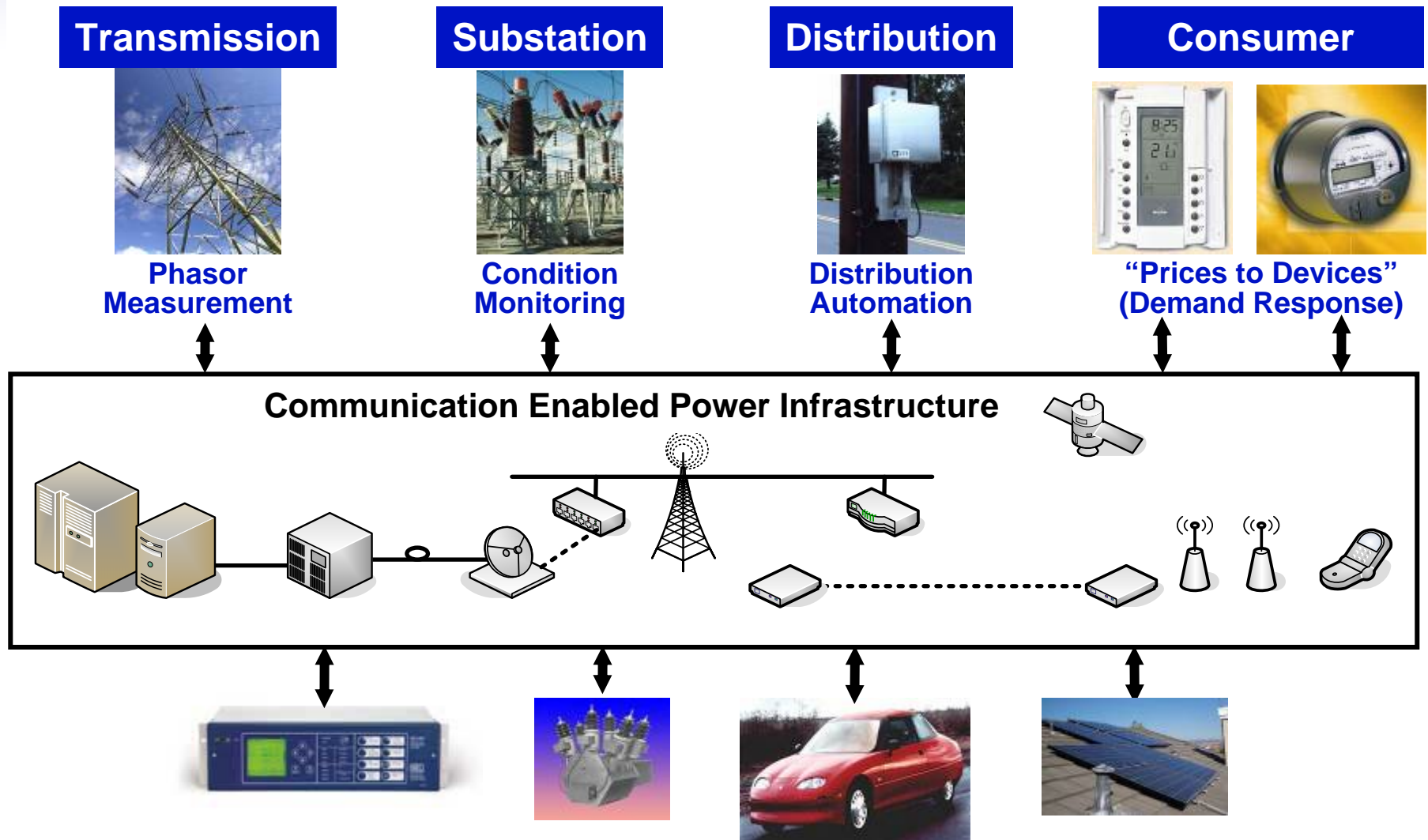
# Key applications enabled by the future electric grid

- Demand Response
- Electric Transportation
- Electric Storage
- Wide Area Management System
- Advanced Metering Infrastructure (AMI)
- Distribution Grid Management
- Mobile Workforce

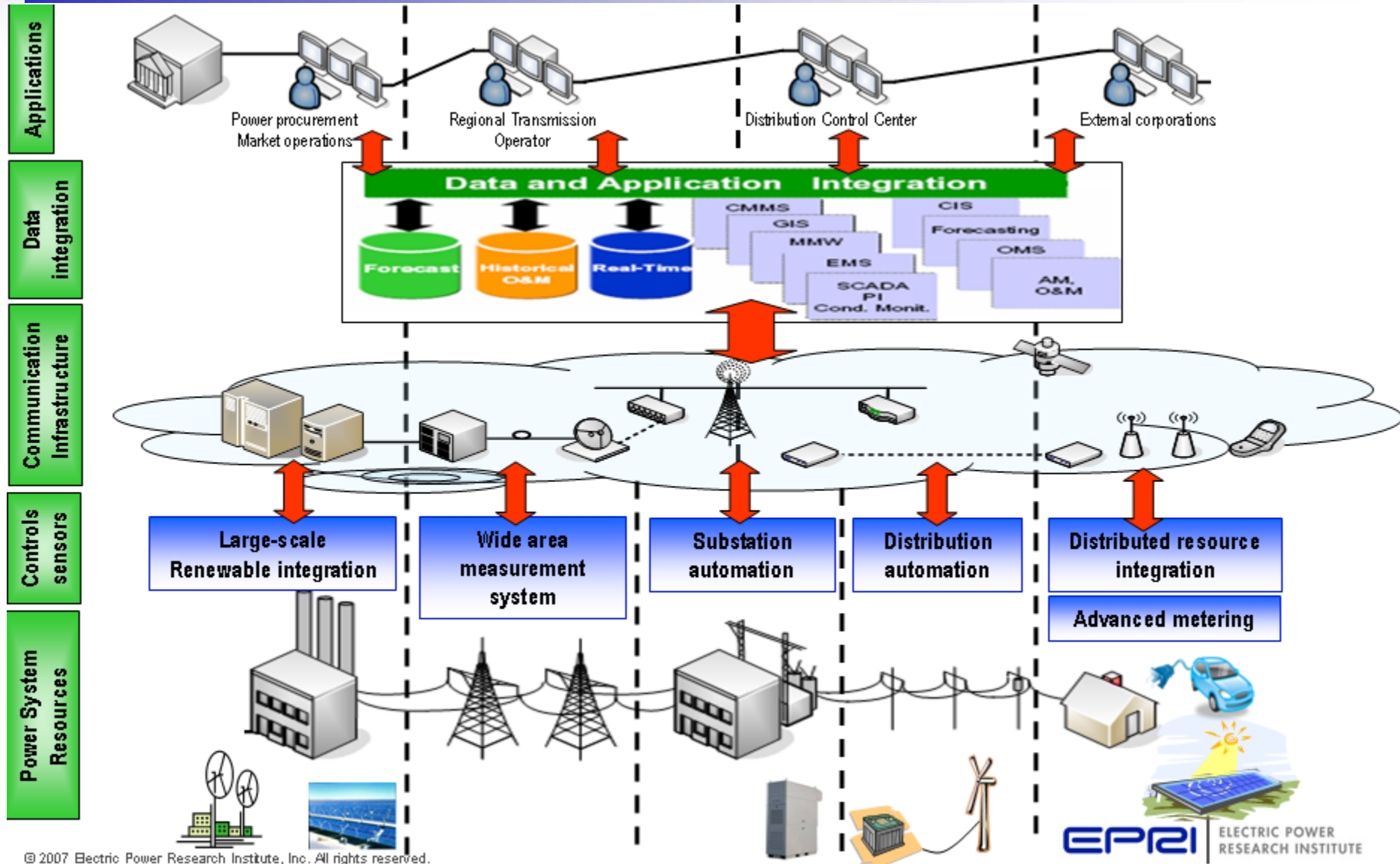
# Architecture Identifies Information Exchange Requirements



# Future Electric Grid – Exchanging Information Seamlessly Across the Enterprise



# Technology at Different Levels



# Securing future electric grid infrastructure

## Requires Comprehensive Approach

- Hardening Issues (e.g. Stateful Inspection, Access Control, Anti-virus)
- Managing Residual Risk (e.g. Intrusion Detection & Prevention)
- Process Control (e.g. Role based access control, biometrics etc.)
- People Training (e.g. Counter measures to social conditioning)

# Cybersecurity best practices

- Establish use case based security requirements at Electric Grid Interfaces (Eg. NISTIR 7628)
- Determine cyber security posture at the system level
- Need Layered Defense Model to thwart potential hacker at multiple levels
- Adopt open security standards that support the requirements

# The inter-connectedness of security and communications

- Availability, integrity and reliability require a properly provisioned communication network to support the applications
- Properly segmented networks are quieter and much easier to monitor for nefarious behavior (e.g. using intrusion detection and prevention systems)
- Payload sizes of encrypted messages should preferably fit the MTU of the communication network to avoid unnecessary fragmentation and latency
- Security features should not add such a burden on the interface processors and memory to cause time outs for the power system applications that are being secured – need a systemic view of security

# What is layered defense?

- Challenge user with multiple authentications/authorizations to access resources across multiple domains based on role
- Inter-connect Access Control Lists, Firewalls and Intrusion Detection Systems for thwarting nefarious behavior at multiple levels
- Monitor nefarious behavior across geographical, logical and temporal boundaries

# Why is securing the future electric grid a challenge?

- Too many inter-connected trust domains – New threat vectors associated with new applications and user profiles
- Communication protocols have known vulnerabilities that can be exploited
- Several open standards based communication protocols have cyber security specifications that are still under development
- Security and privacy requirements are coming from various sources in the industry – no single harmonized resource available yet

# Current activities in securing the electric grid

- National Electric Cyber Security Organization Group (NESCOG – A DoE collaborative project between NESCO led by EnergySec and NESCOR lead by EPRI) FOA 0000245
- NIST Cyber Security Working Group (CSWG)
- National Energy Reliability Corporation Critical Infrastructure Protection Standards (CIPS 002-009)
- DHS Industrial Control Systems Joint Working Group
- UCA OpenSG Utilisec Working Group

# NESCO Group background

**DOE issued a Funding Opportunity Notice (FOA DE 0000245) in April 2010 to establish the National Electric Sector Cyber Security Organization (NESCO) as a public private partnership to:**

- Evaluate cyber security posture for legacy systems
- Evaluate deployability of emerging cyber security technologies
- Collaborate and coordinate to identify cyber security requirements
- Perform use case analysis for risk identification, assessment, and development of risk mitigation strategies
- Develop cyber security best practices and metrics
- Establish and operate a Cyber Incident Data Center (CIDC)

# Concluding remarks

- Future electric grid applications pose new security threats
- Cyber security posture needs to be determined at the system level using an “all hazards approach” to truly protect
- Security and communications need to be studied in an integrated manner
- Need to balance compliance requirements with managing risk for long term economic viability in delivering electric grid services
- Collaborative research is needed to address scalability, interoperability and manageability issues for electric grid security and privacy

# Q&A

# Contact Info

Erfan Ibrahim, Ph.D.  
Technical Executive  
Power Delivery & Utilization  
Intelligrid Cyber Security Lead  
EPRI Lead on NESCOR Project

[eibrahim@epri.com](mailto:eibrahim@epri.com)

(925) 785-5967

# Together...Shaping the Future of Electricity