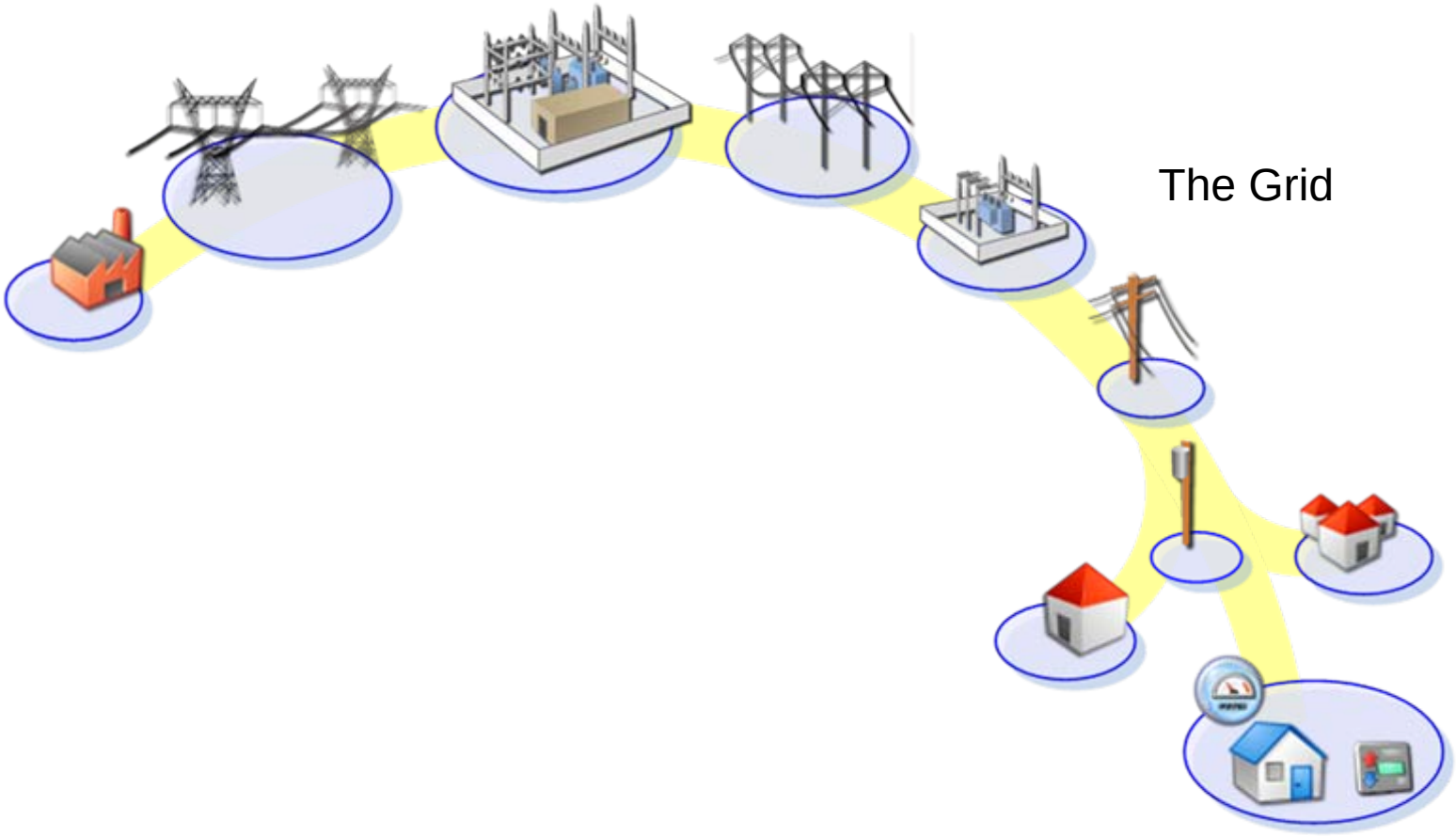
Field Asset Security in a Smart Grid World

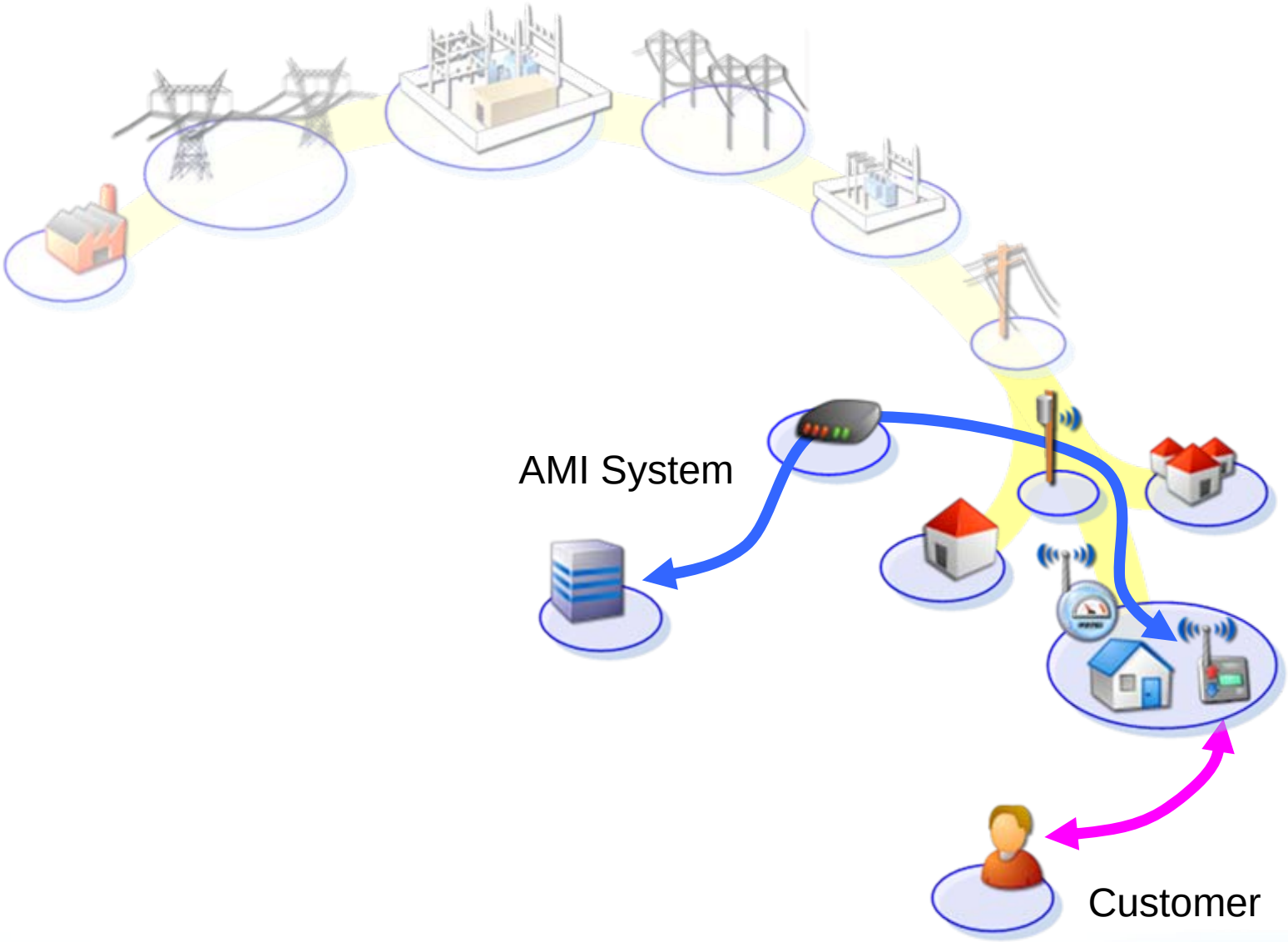
Darren Reece Highfill

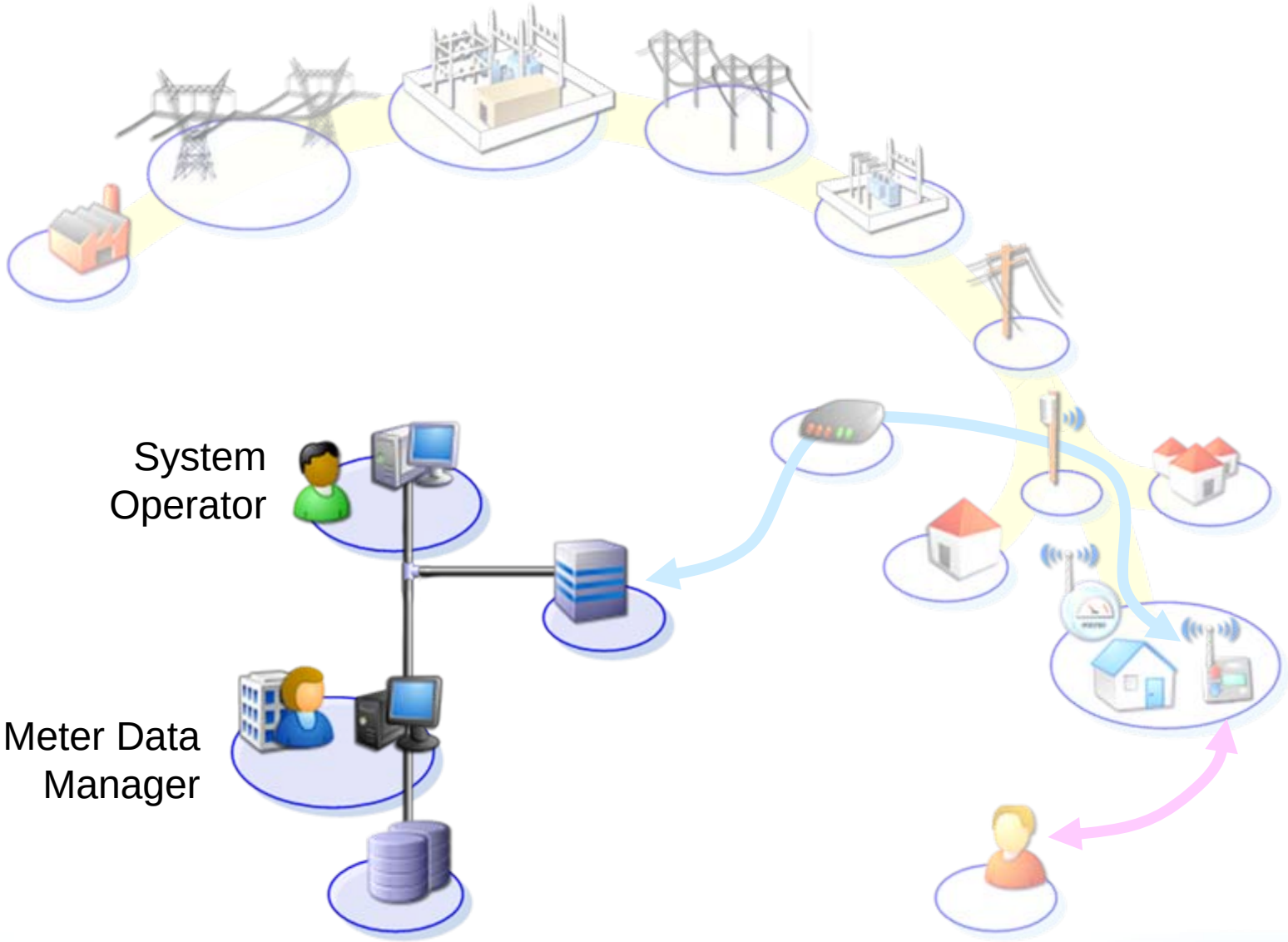
→***Advanced Metering Infrastructure***

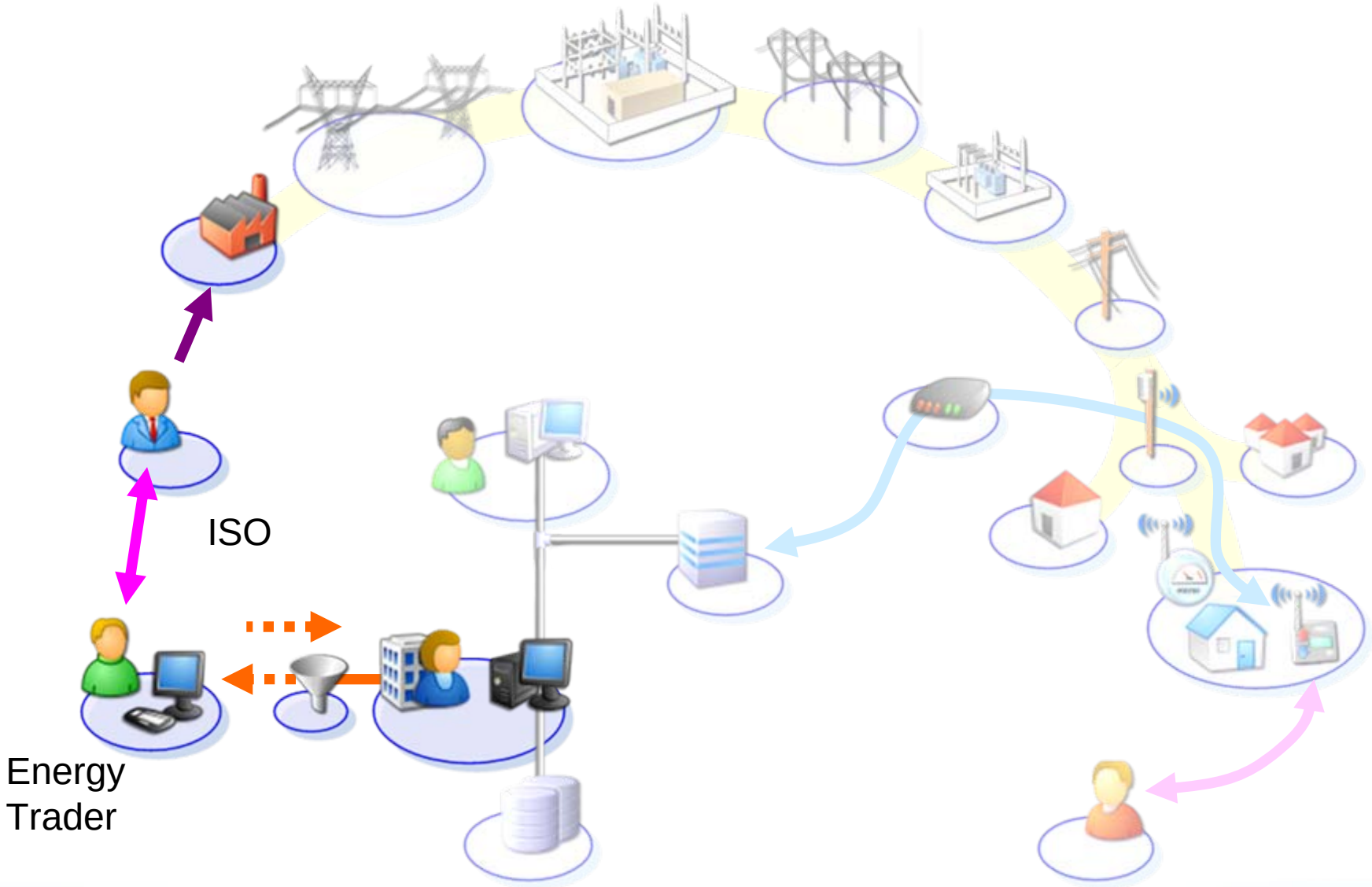
darren@enernex.com

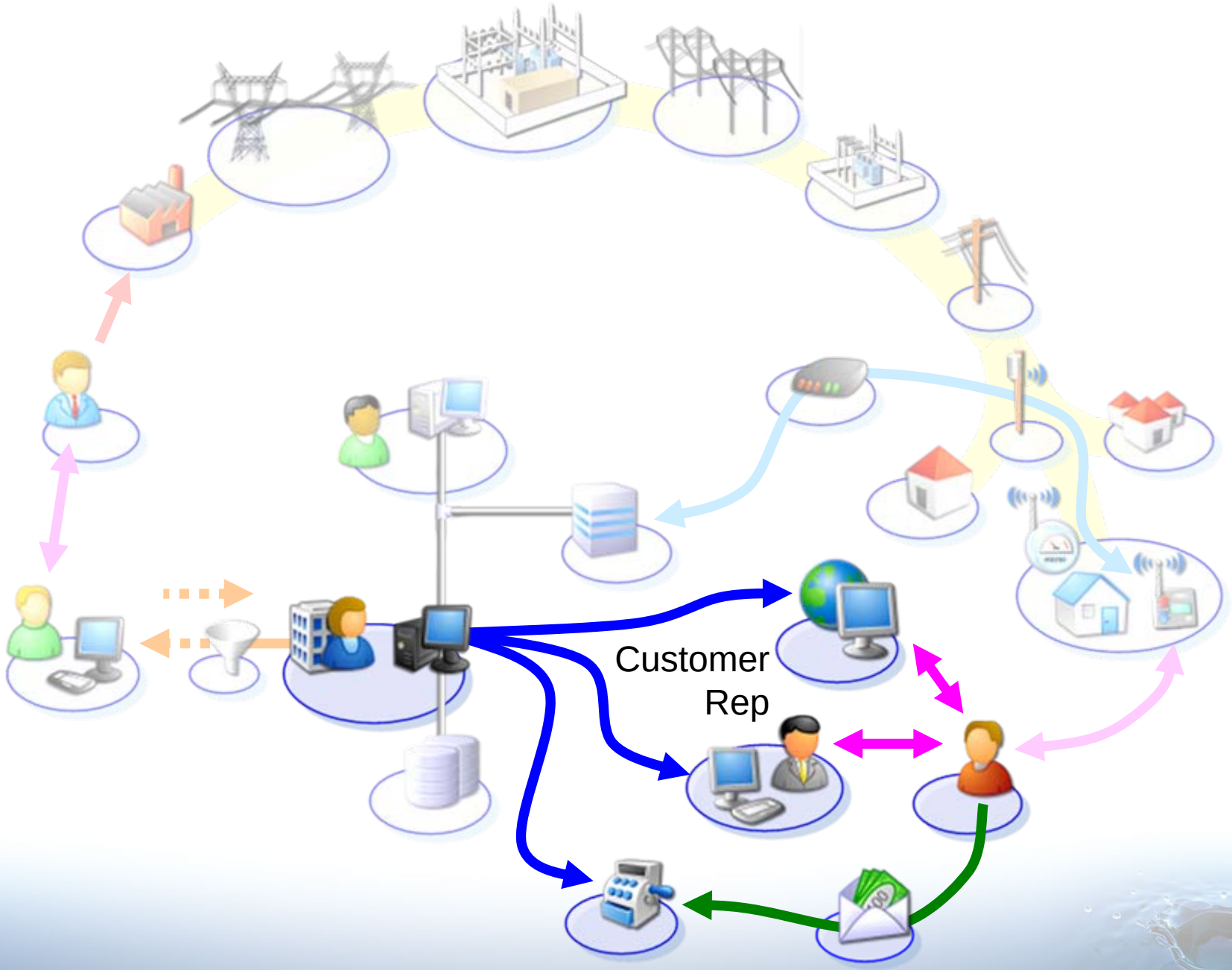


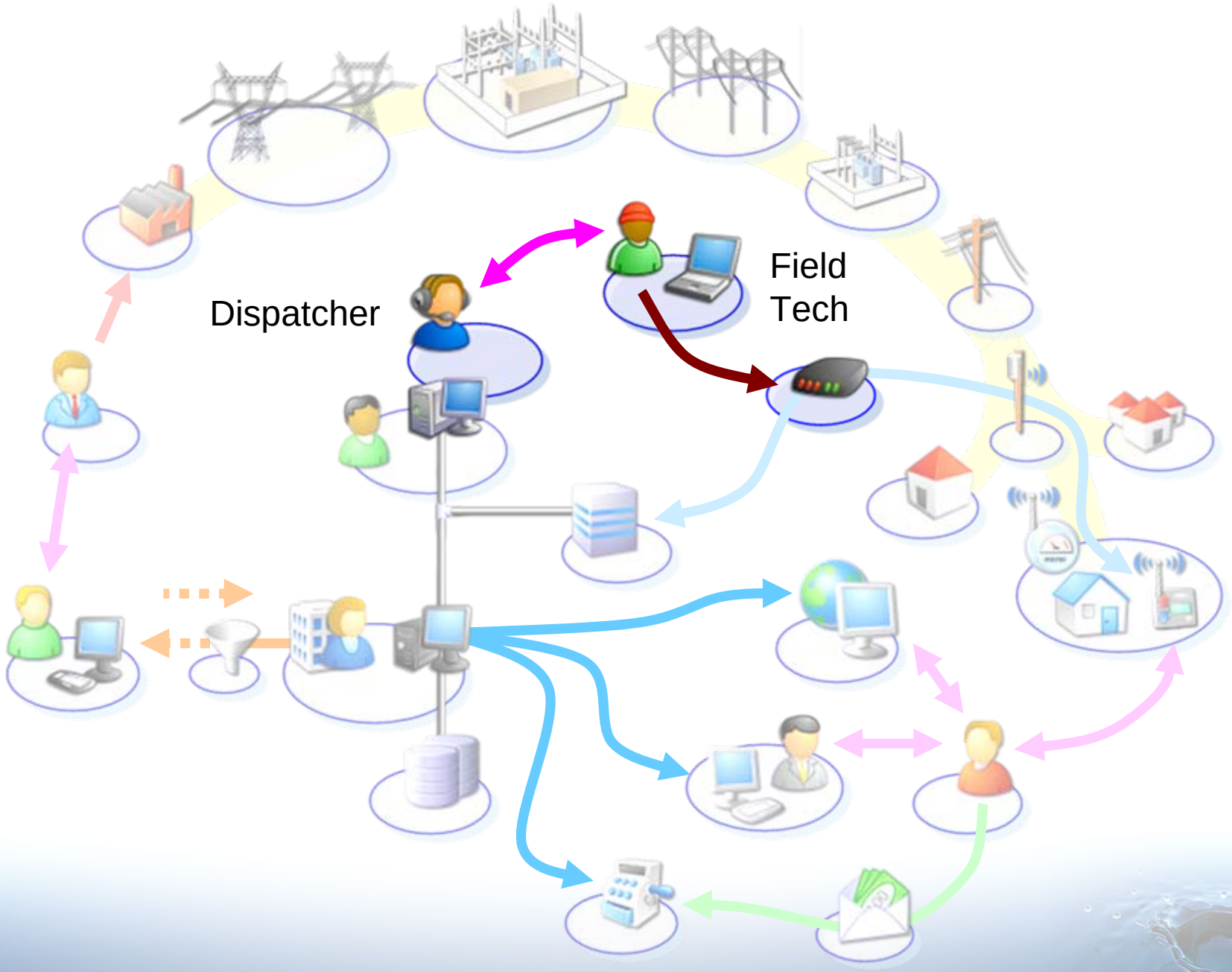
The Grid

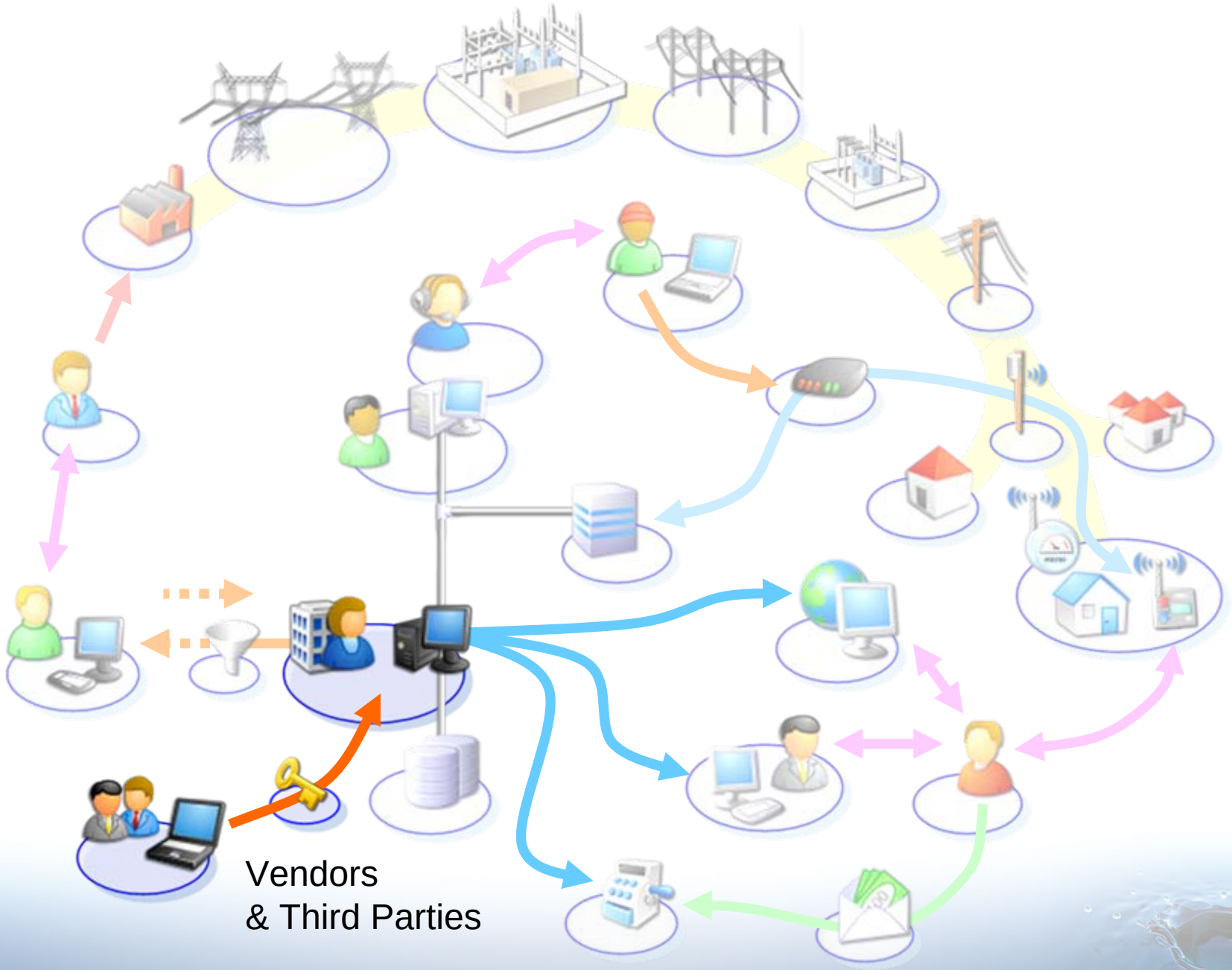

AMI System
Customer

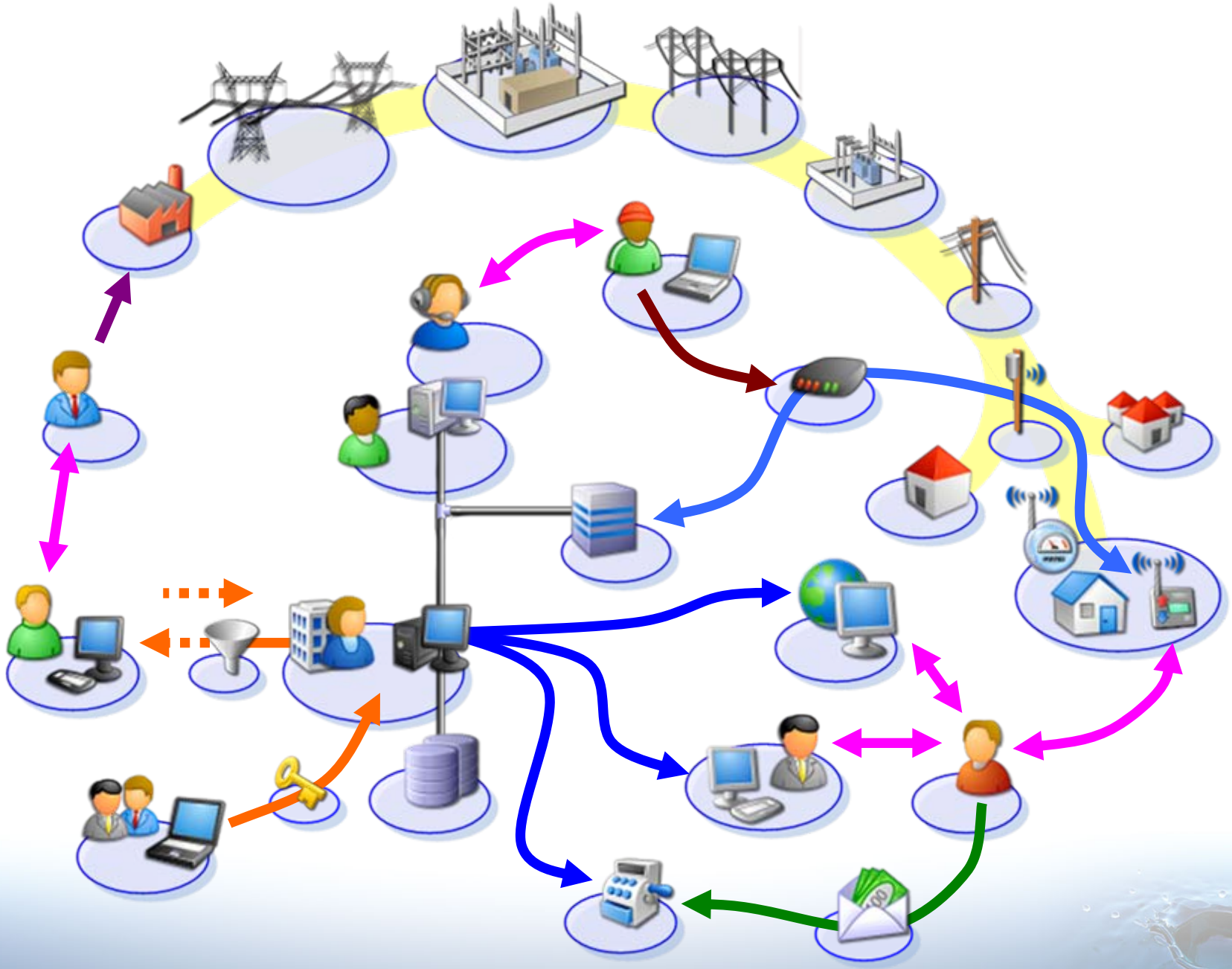

System
Operator
Meter Data
Manager


ISO
Energy
Trader


Customer
Rep


Dispatcher
Field
Tech

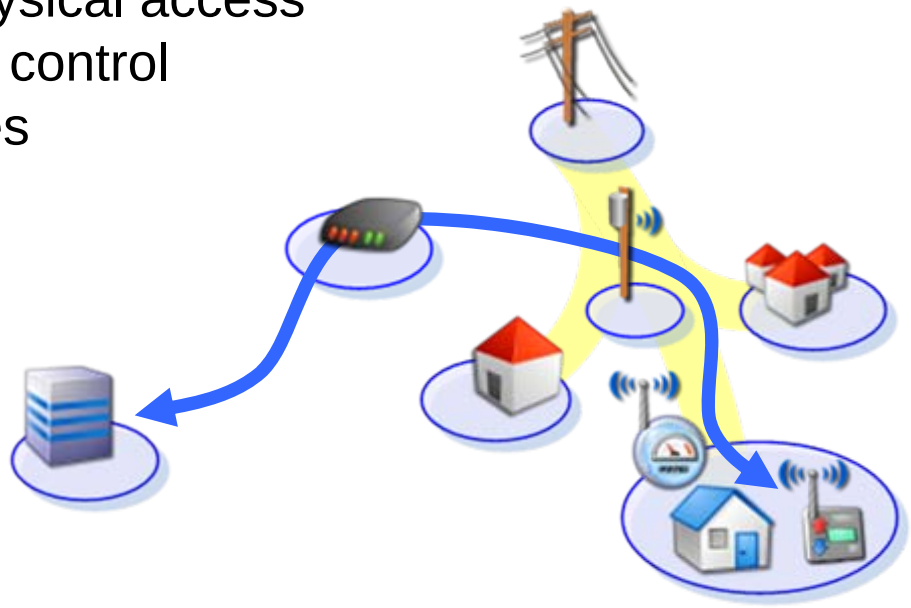

Vendors
& Third Parties



Field Elements

Issues

- Limited or no control over physical access
- Wide range of logical access control
- Resource constrained devices
- Large quantity of devices



Requirements

- Device Identity
- Data Integrity
- Customer Privacy

Considerations

- Intelligence? (How much?)
- Filtering?

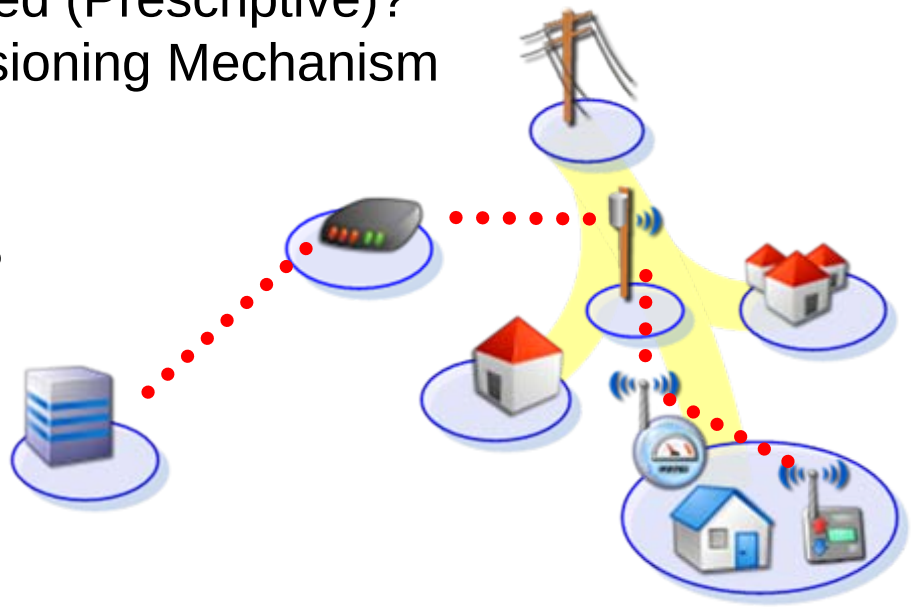
Field Elements

Network Management

- Ad-hoc Structure or Predefined (Prescriptive)?
- Integrity, Availability of Provisioning Mechanism

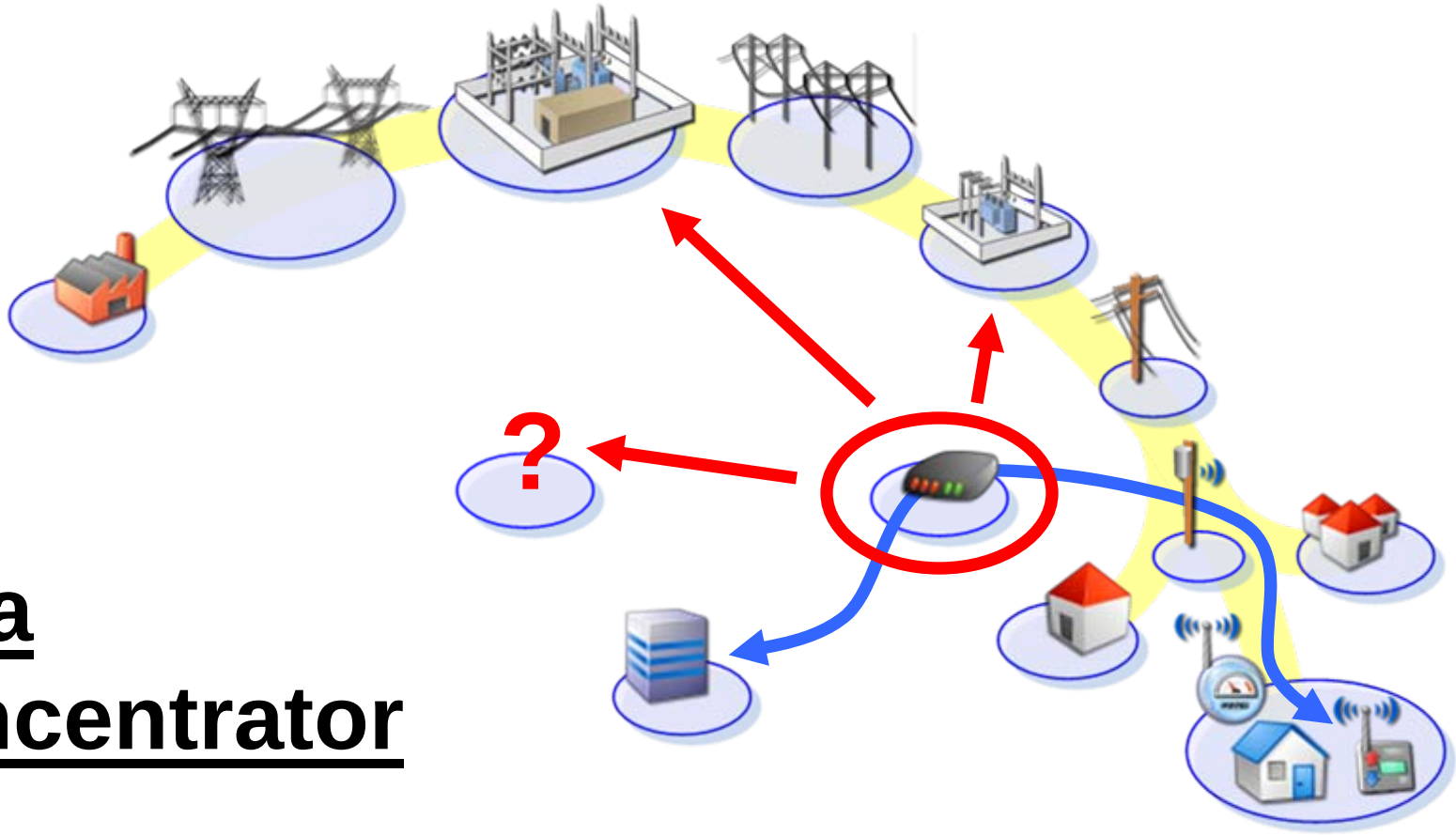
Authentication Mechanism

- End-to-End or Step-by-Step?
- Bi-Directional (“Two-Way”)
- Pre-Shared or Public Key?
- Customer Devices



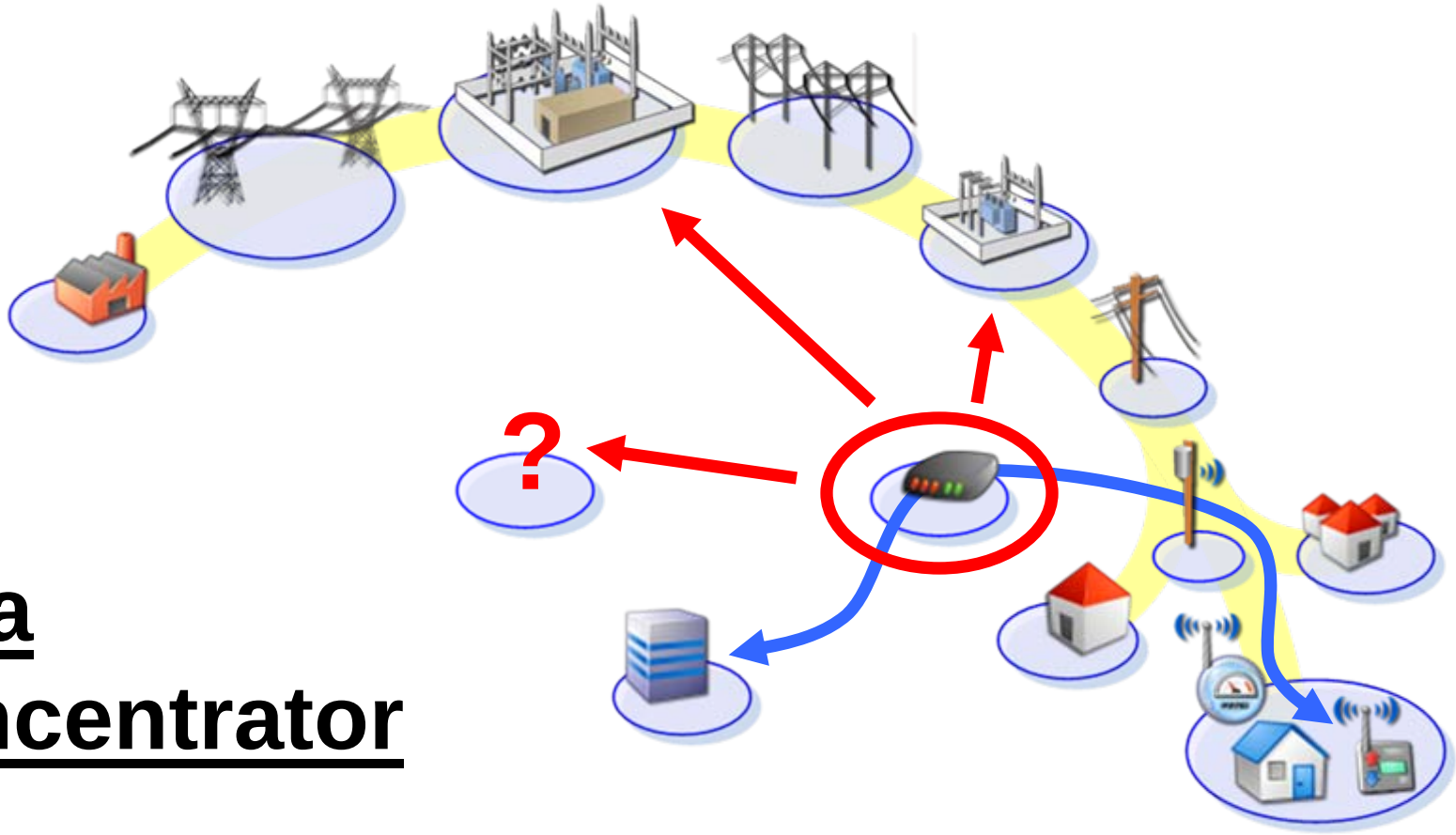
Countermeasures

- Role-Based Access Control
- Least Privilege, Need-To-Know
- Unpredictable Credentials
- Intrusion Detection
- Tamper Detection



Data Concentrator

- At a substation? Somewhere in the field?
- Who owns the property? Is there a fence?
- Does it use wireless technology?
- What kind of access controls are implemented?



Data Concentrator

- How many homes are served? What is peak load?
- More than 300MW (~100,000 homes?) → NERC CIP?
- How does it authenticate / get authorized to the Data Center Aggregator?

Operations Center

System Management Console

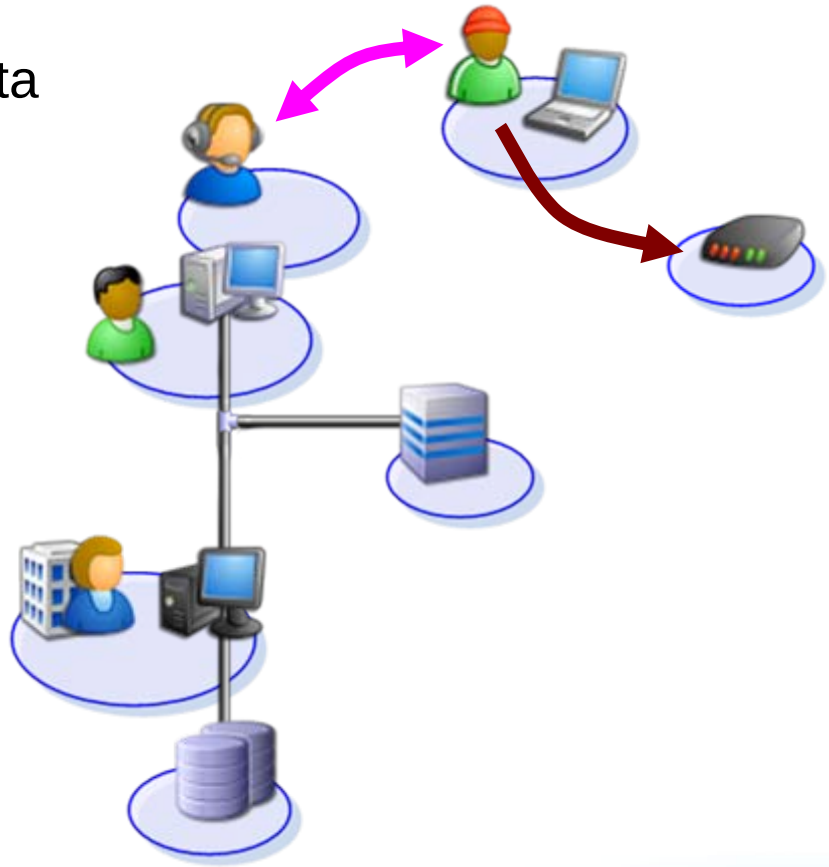
- Data Availability, Integrity
- Filtered View – No Financial Data
- Time Sensitive (Freshness)

Field Communications

- Data Integrity
- Temporal Privilege
- Strict Procedures
- Detailed Accounting

Meter Data Management System

- Data Integrity, Confidentiality
- Multiple Interfaces, Heterogeneous Constraints



Public Interface

Website

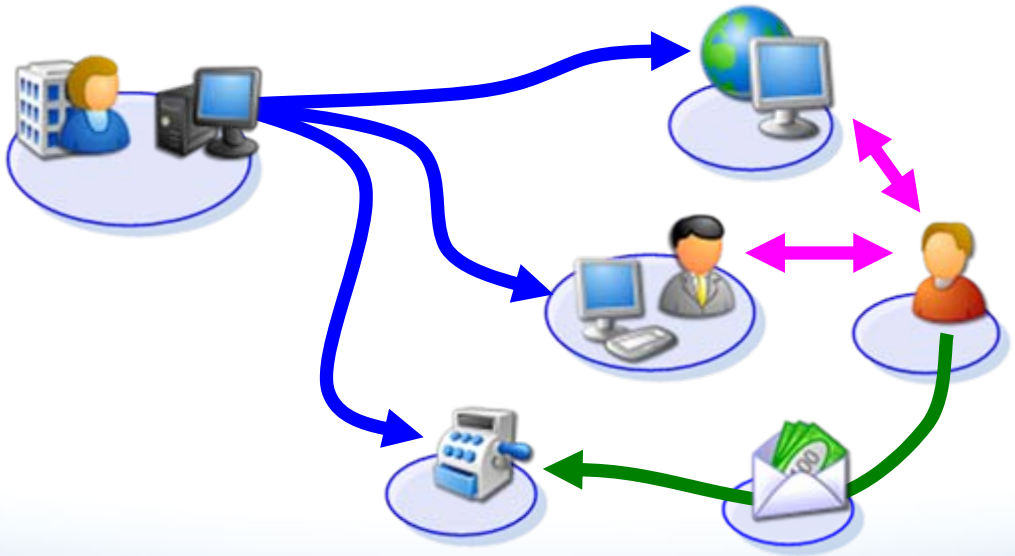
- Data Confidentiality
- Public (General Info) and Private (Customer) Views
- Consumer Portal Best Practices (e.g.: Financial Services)

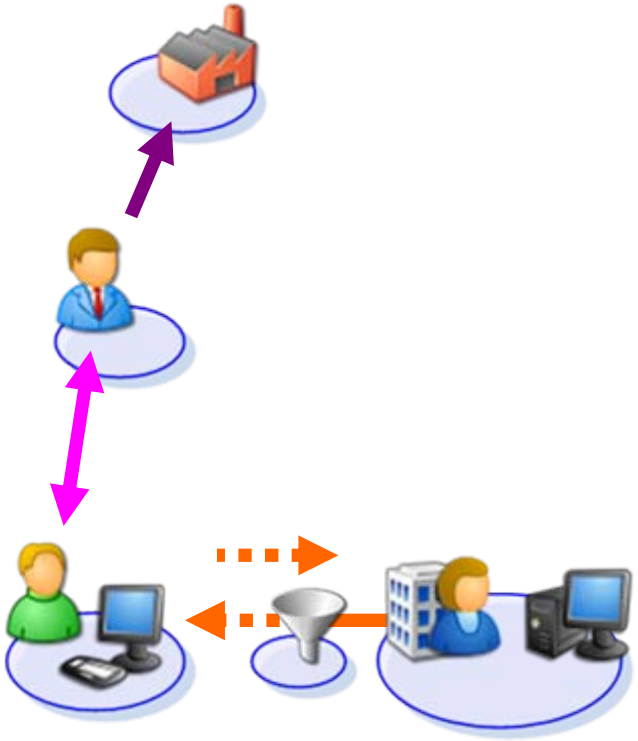
Customer Representative

- Data Confidentiality, Integrity
- Filtered View – Billing Related

Revenue

- Data Integrity, Confidentiality
- Non-Repudiation





Demand-Response

Energy Trader

- Regulated Relationship

Availability & Control

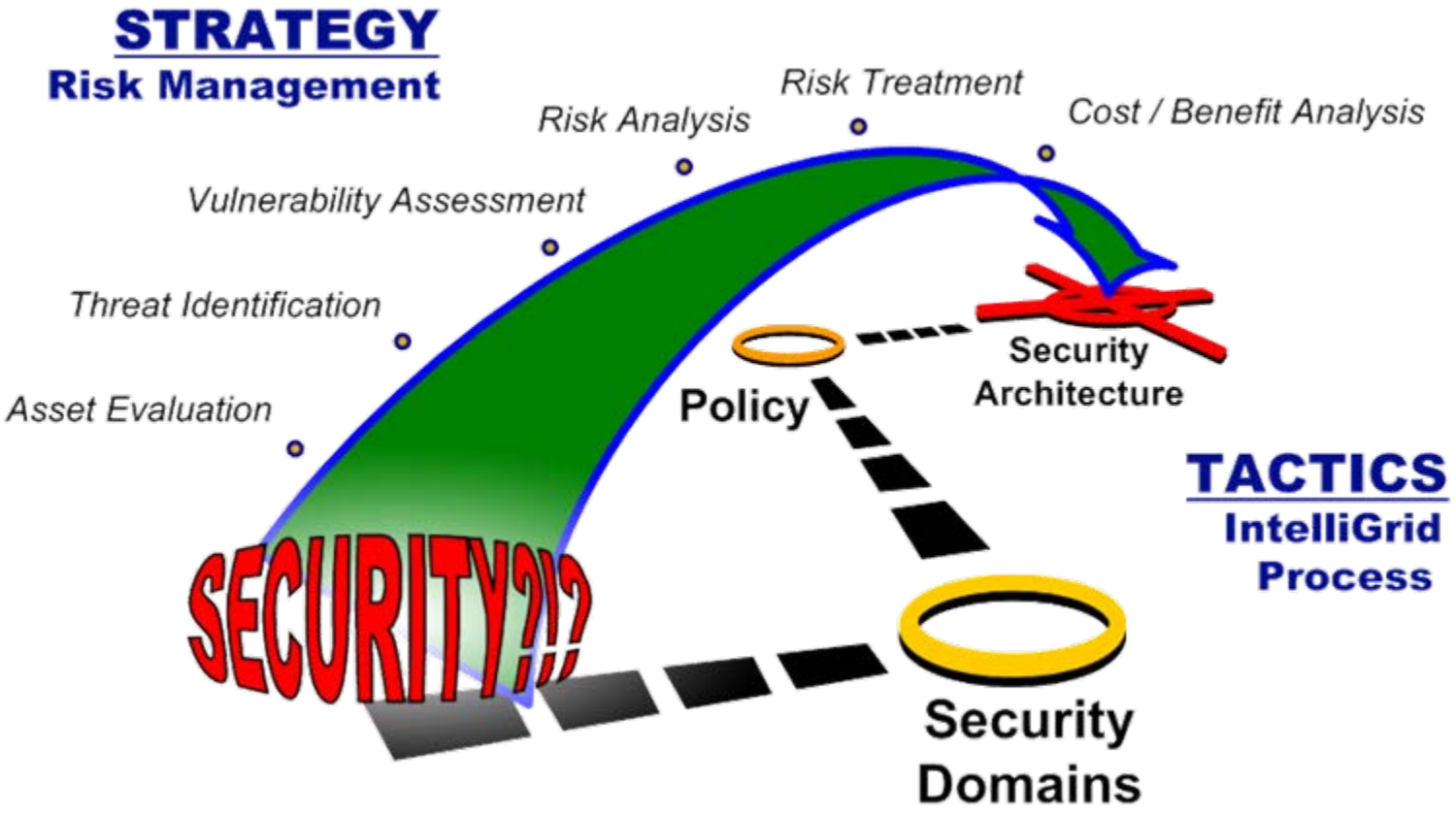
- Data Confidentiality, Integrity
- Negotiated “Contract”
- Similarities to Dealing with an External Entity

Vendors & Third Parties

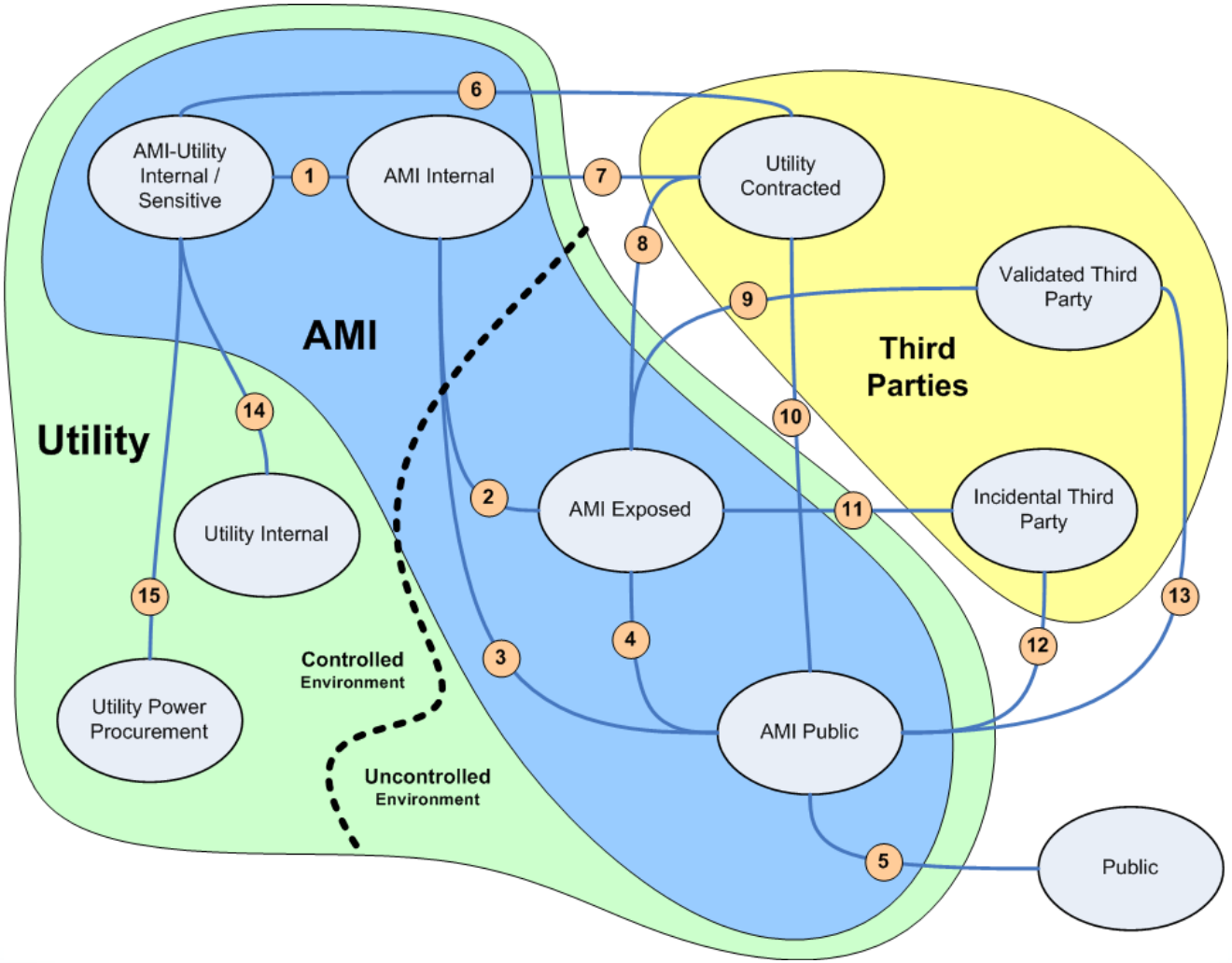
External Entities

- Data Confidentiality
- Contractual Agreement
- Least Privilege, Need-To-Know

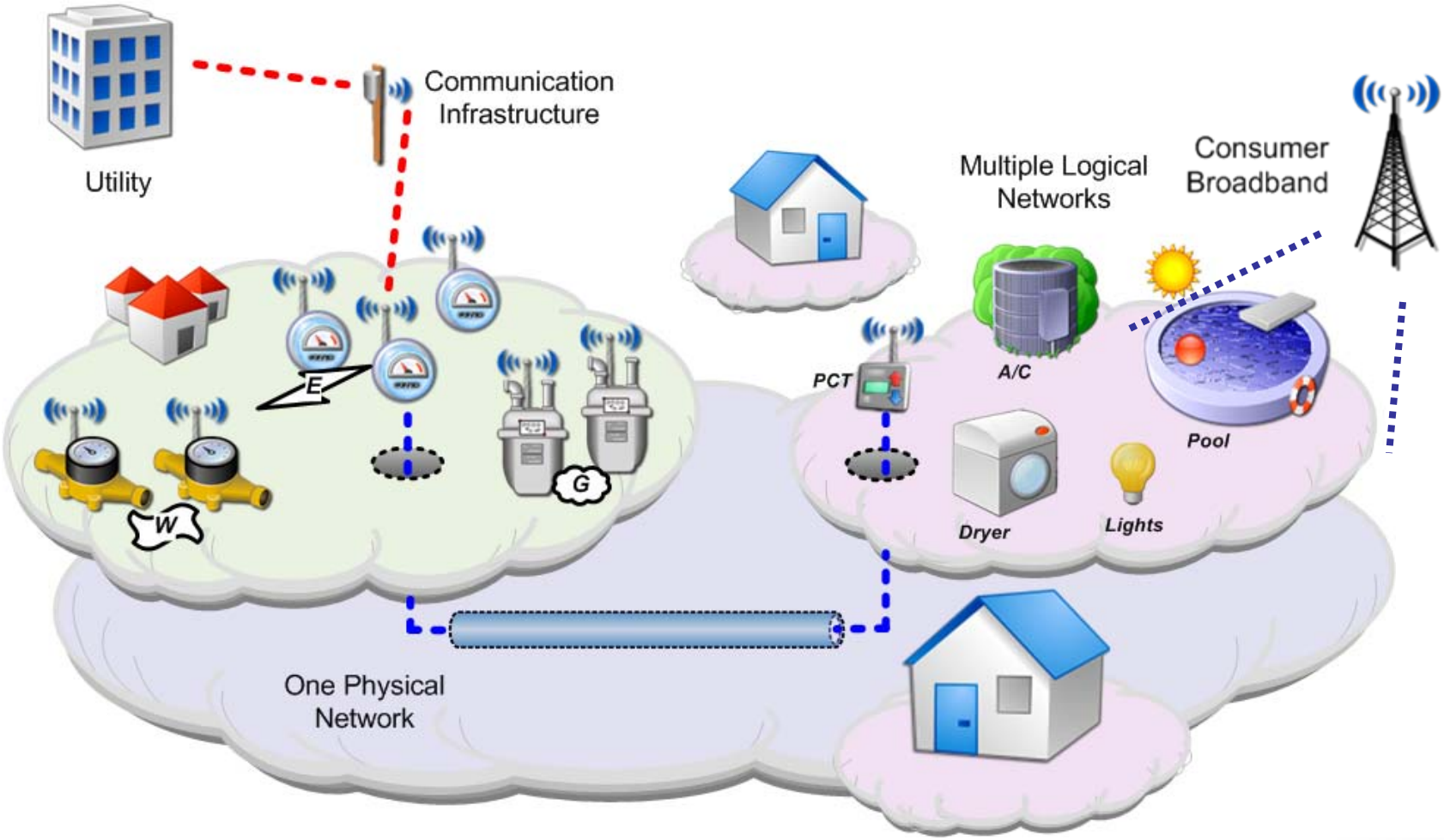
Security Strategy & Tactics



AMI Security Domains



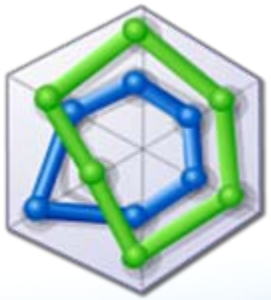
AMI-HAN Security Policy

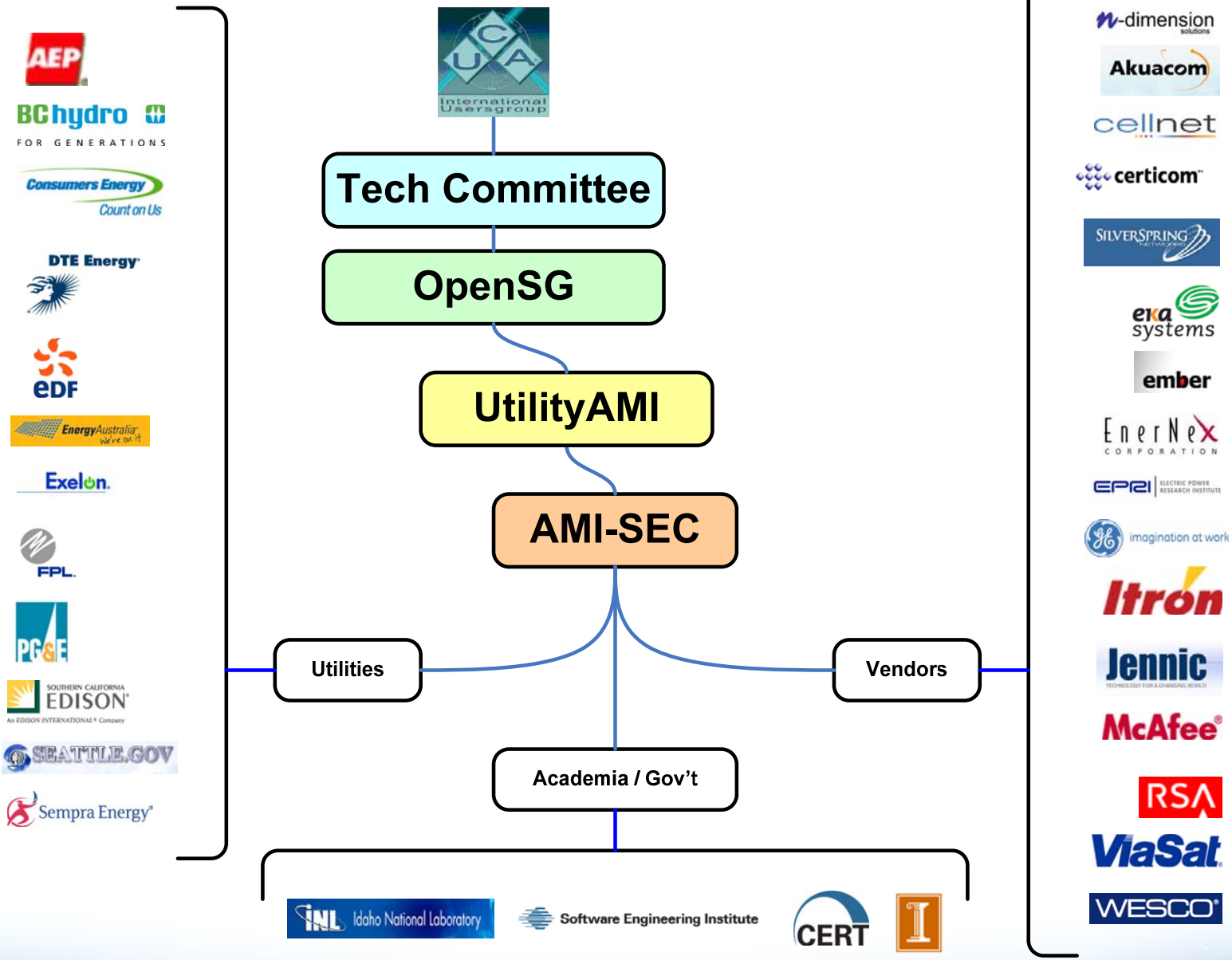


AMI-SEC Task Force

- AMI-SEC is concerned with securing AMI system elements.
  - *Contextual Definition:*

    "…*those measures that protect and defend AMI information and systems by assuring their ability to operate and perform in their intended manner in the face of malicious actions.*"

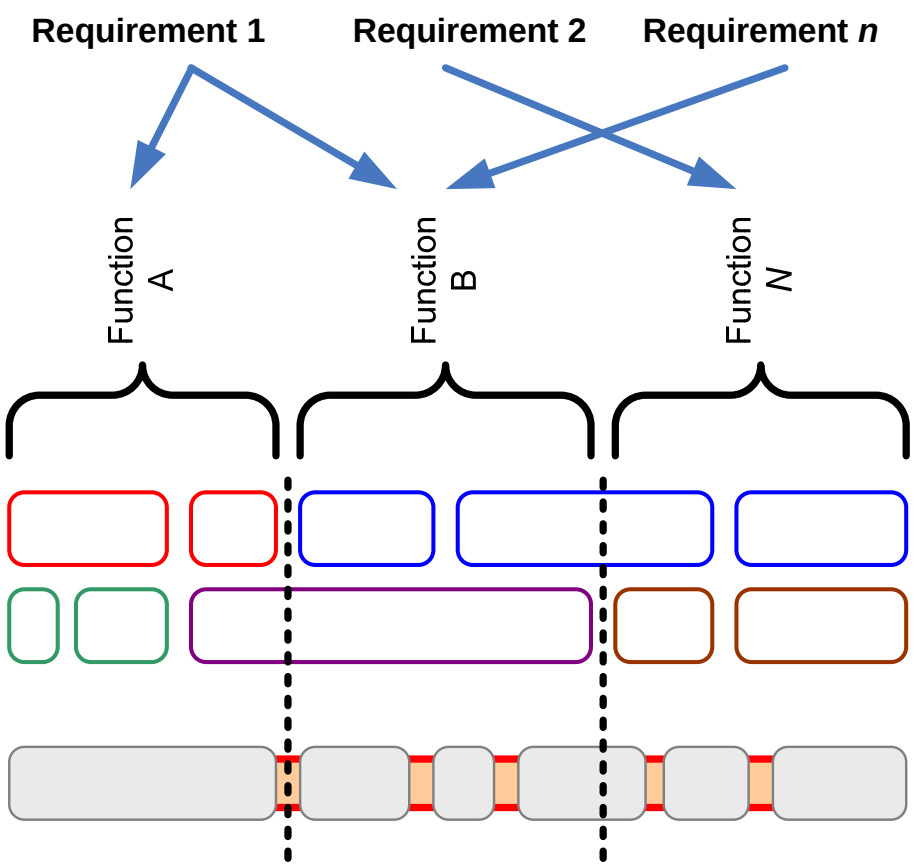



UCA International Usersgroup
Tech Committee
OpenSG
UtilityAMI
AMI-SEC
Utilities
Vendors
Academia / Gov't
AEP
BC hydro
FOR GENERATIONS
Consumers Energy
Count on Us
DTE Energy
eDF
EnergyAustralia
Exelon.
FPL.
PG&E
SOUTHERN CALIFORNIA EDISON
An EDISON INTERNATIONAL Company
SEATTLE.GOV
Sempra Energy
n-dimension
Akuacom
cellnet
certicom
SILVERSPRING
eka systems
ember
EnerNex CORPORATION
EPRI ELECTRIC POWER RESEARCH INSTITUTE
imagination at work
Itron
Jennic
McAfee
RSA
ViaSat
WESCO
INL Idaho National Laboratory
Software Engineering Institute
CERT

AMI-SEC Task Force

- Purpose
  - Produce technical specification
    - Used by utilities to assess and procure
    - Used by OpenAMI – part of AMI/DR Reference Design
  - Determine baseline level of detail
    - Prescriptive in nature
    - Compliant products will have known functionality and robustness

AMI-SEC 2008 Deliverables



System Requirements

System Security Design

Component Catalog

Implementation Guide

Timeline & Resource Challenges

- AMI-SEC TF is volunteer-based
  - Operates like a standards body
  - 4 deliverables in 12 months – aggressive schedule
  - Utilities are personnel resource constrained

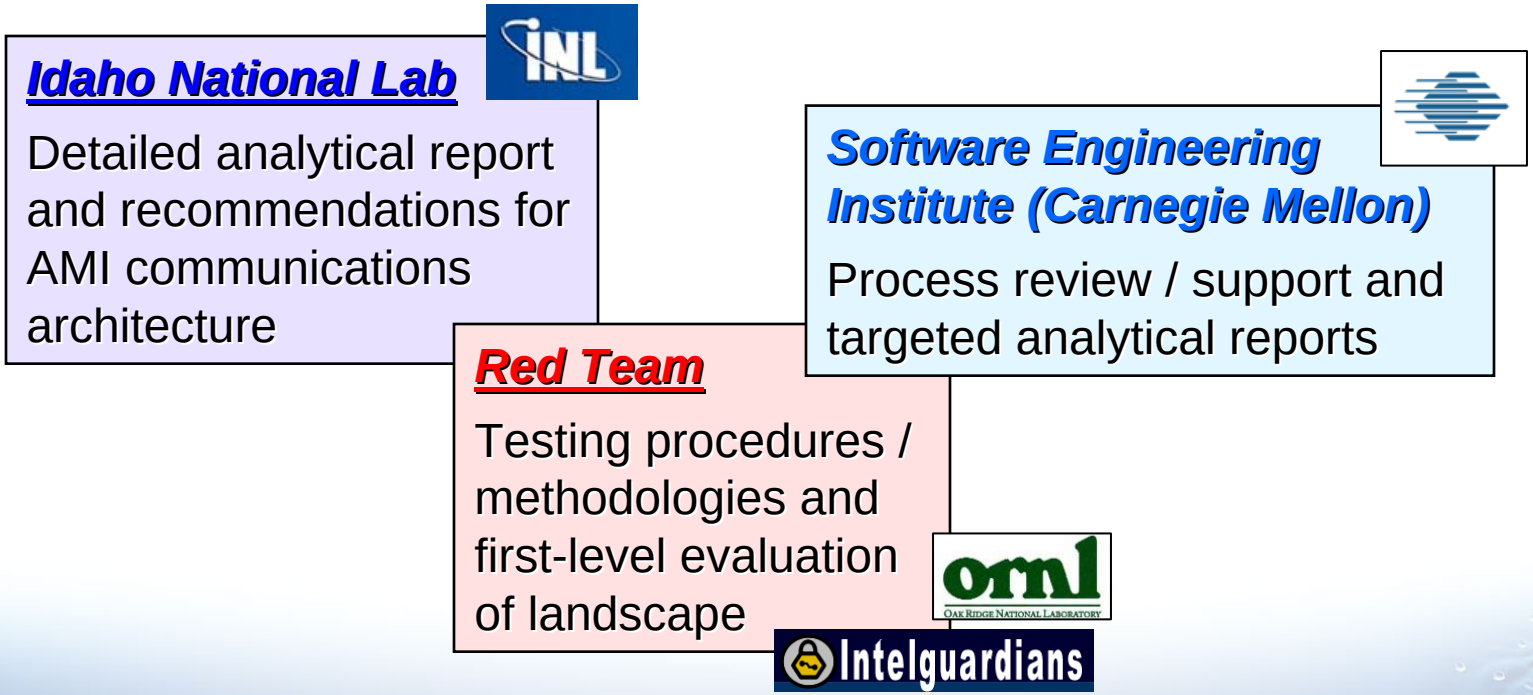
- Deliverables done in December, 08?
  - Not good enough
  - *Will have missed the window of opportunity*

AMI Security Acceleration Project (ASAP)

- Collaborative opportunity for electric utilities.
- Matching ($1-for-$1) funds from **DOE** for FFRDC participation.
- Dedicated, accountable resources
  - Assist in production of content for AMI-SEC
  - Work products belong to AMI-SEC
- Accelerate and augment the activities of AMI-SEC

ASAP

- Targeted augmentation of security requirements
  - Supplement to Risk Assessment / System Requirements
  - Goal of providing “drop-in” security section for RFP
- Additional benefits from collaborating organizations



Questions / Discussion

darren@enernex.com