



# **UCAIug: Smart Grid Security**

Boot Camp – May 2010 @ Washington, DC

**→ SG Security Working Group**

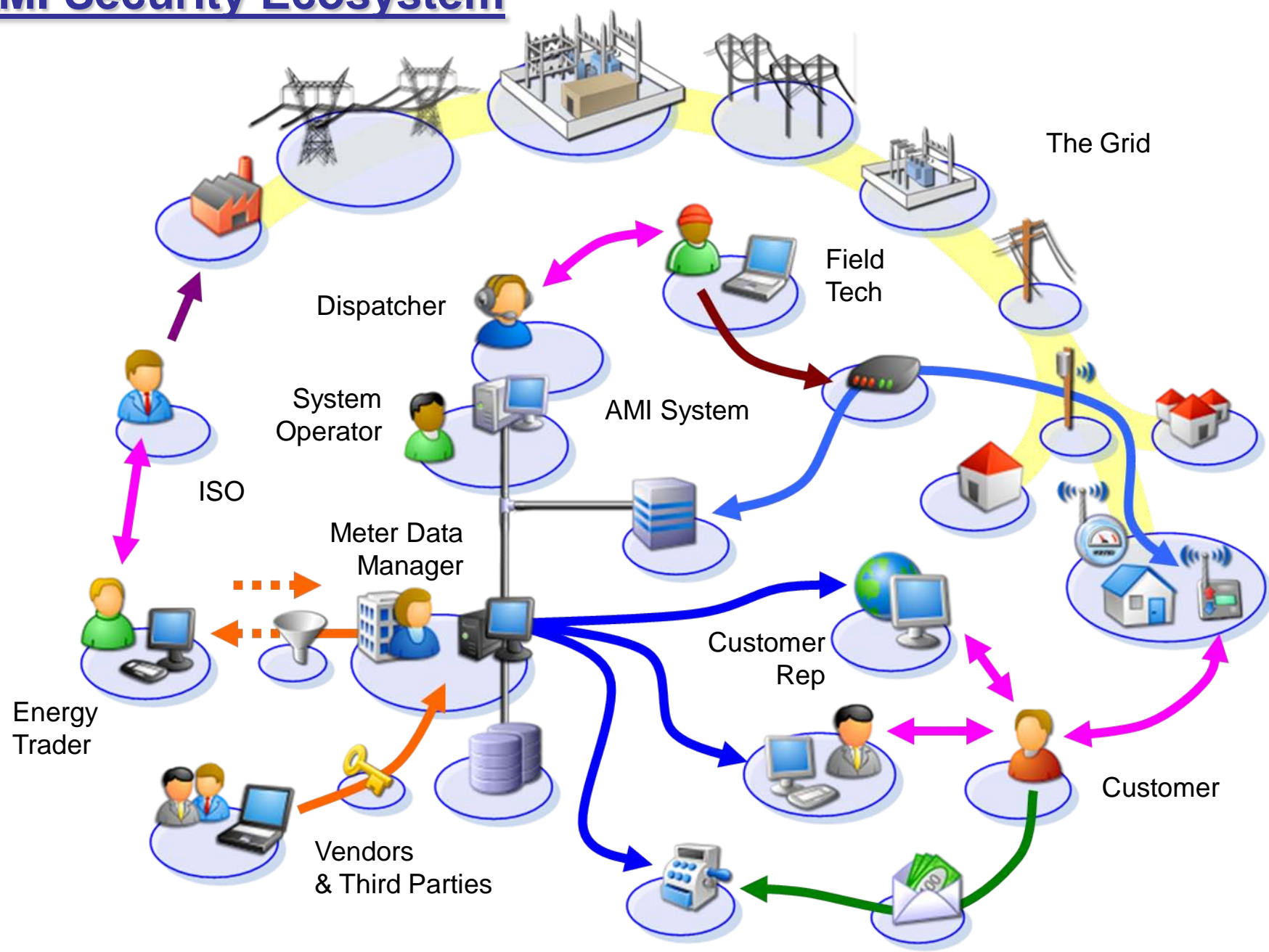
**→ AMI-SEC Task Force**

**SG Security WG Chair:**

Darren Reece Highfill

[darren@utilisec.org](mailto:darren@utilisec.org)

# AMI Security Ecosystem



# Field Elements

## Issues

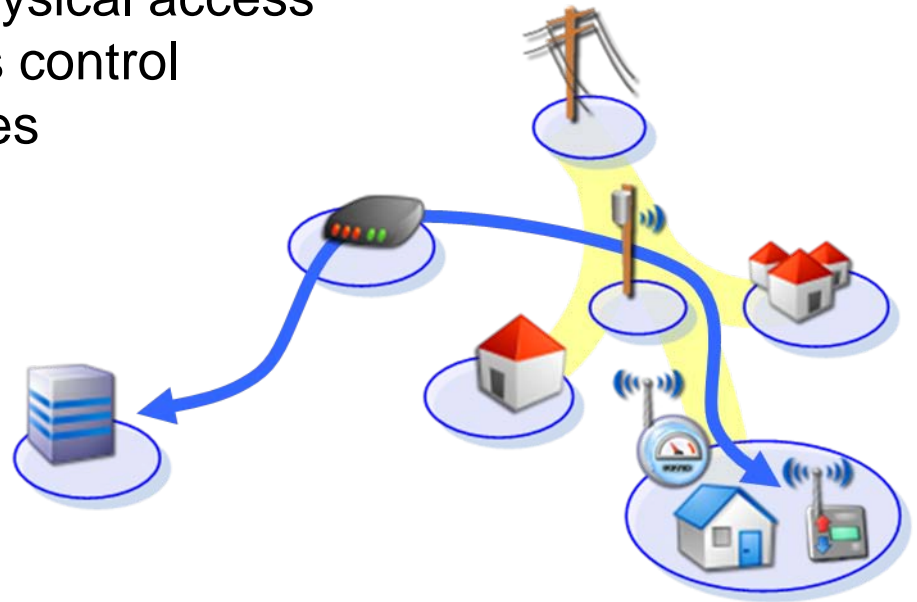
- Limited or no control over physical access
- Wide range of logical access control
- Resource constrained devices
- Large quantity of devices

## Requirements

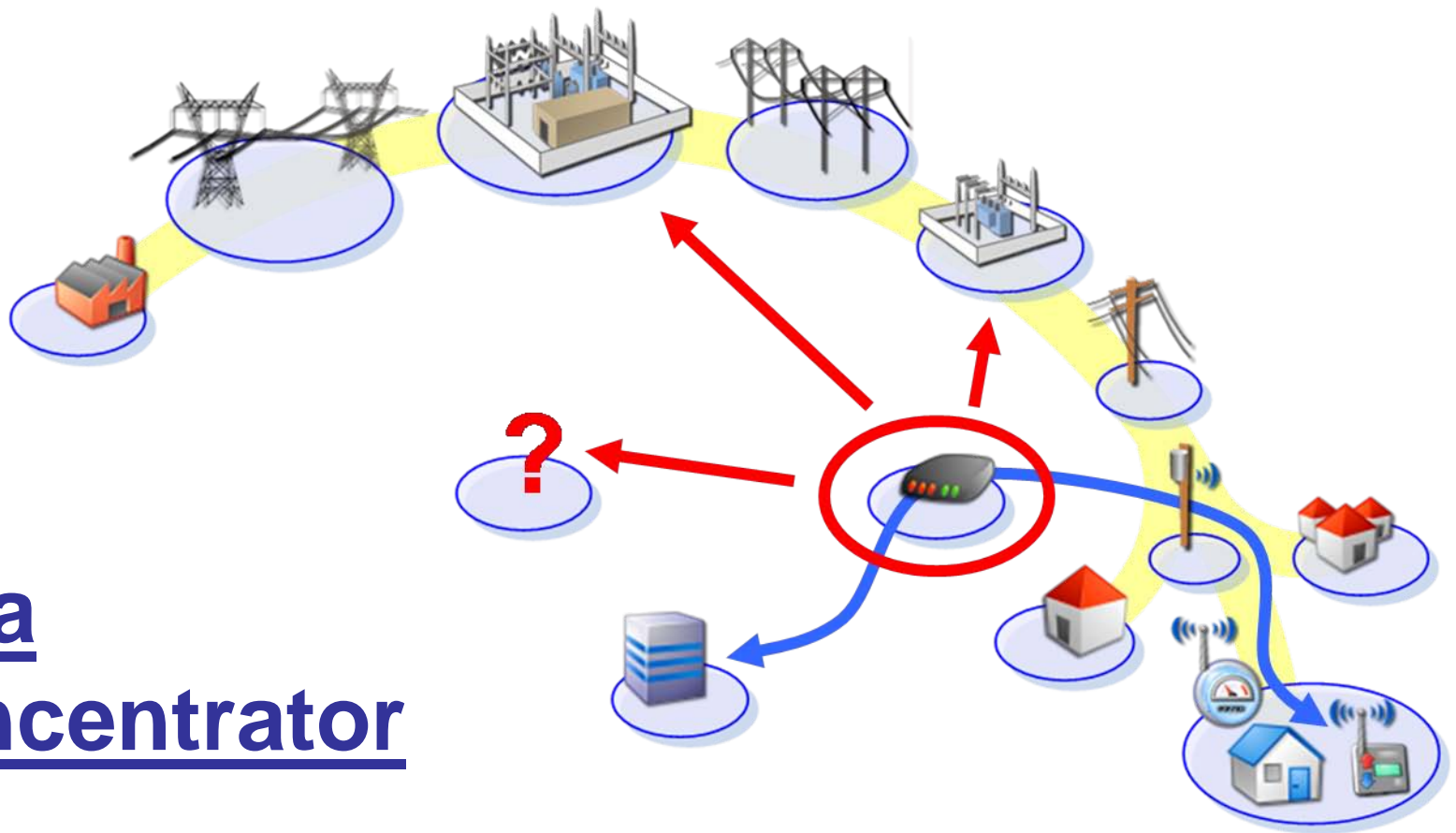
- Device Identity
- Data Integrity
- Customer Privacy

## Considerations

- Intelligence? (How much?)
- Filtering?

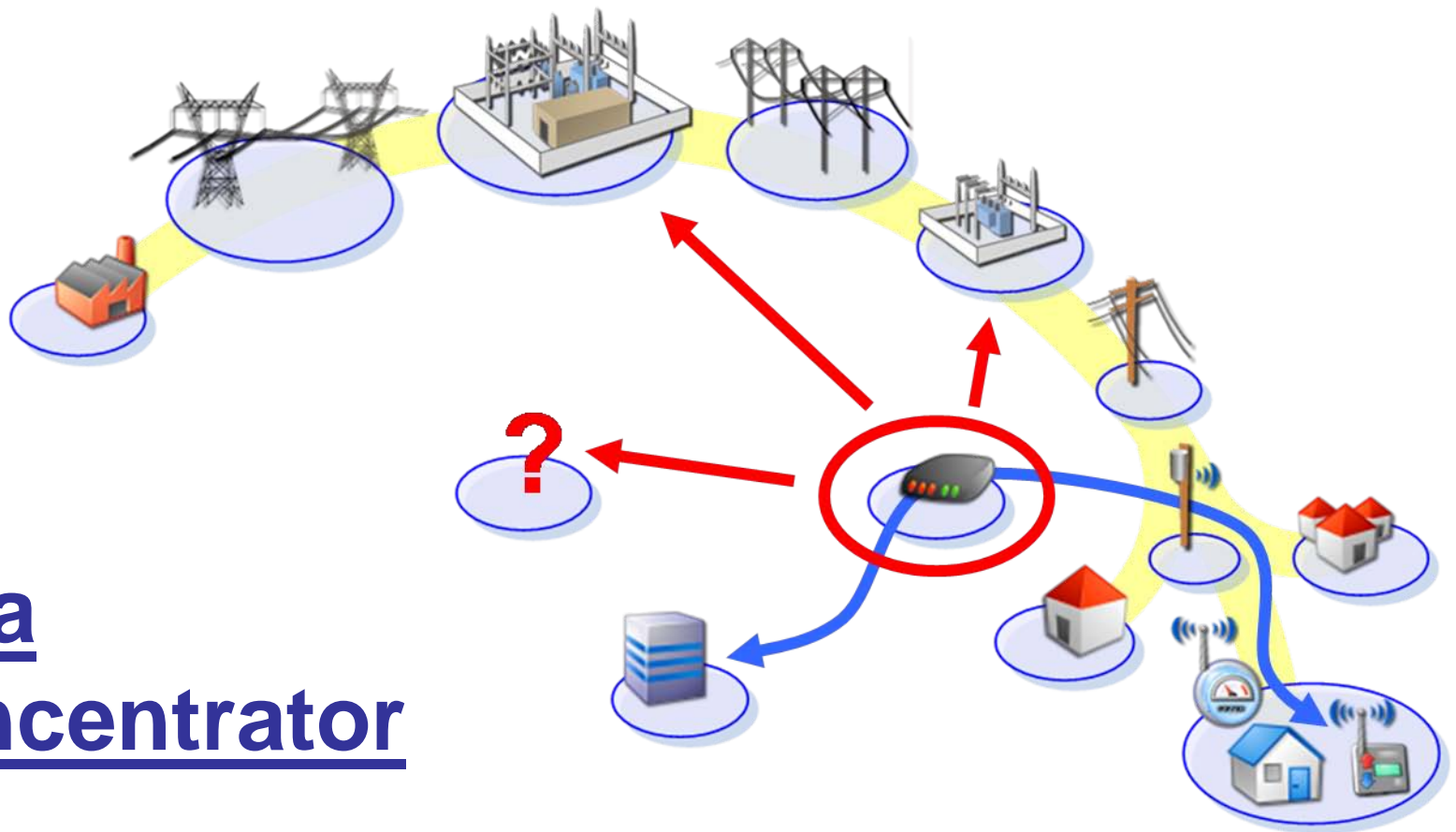


- Role-Based Access Control
- Least Privilege, Need-To-Know
- Unpredictable Credentials
- Intrusion Detection
- Tamper Detection



## 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

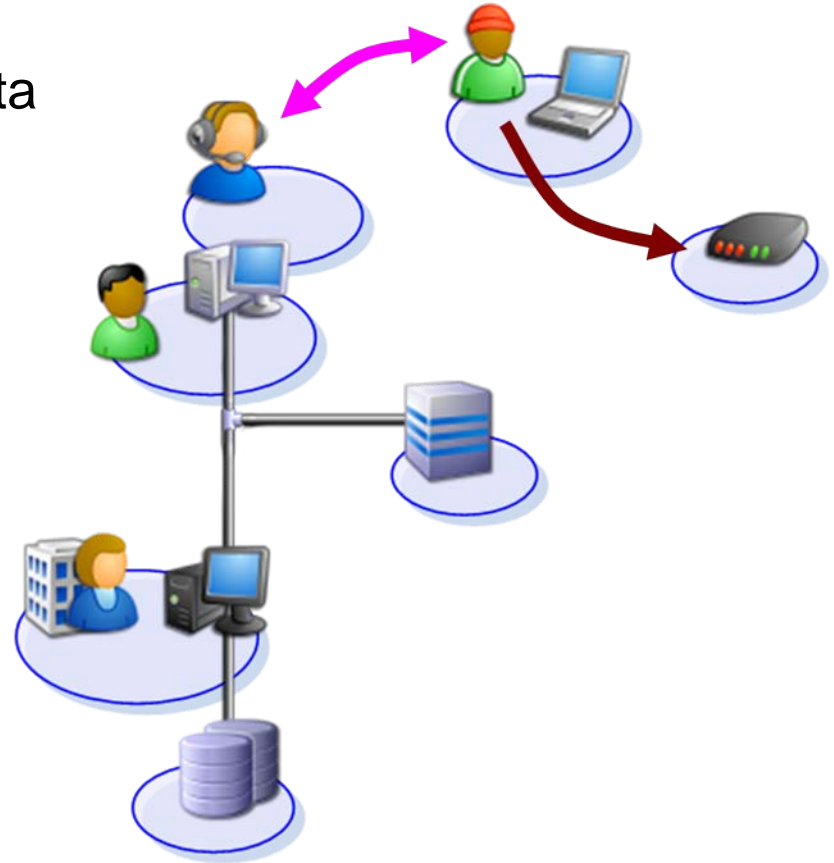
- Data Availability, Integrity
- Filtered View – No Financial Data
- Time Sensitive (Freshness)

## Field Communications

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

## Meter Data Management System

- Data Integrity, Confidentiality
- Multiple Interfaces,  
Heterogeneous Constraints



## Public Interface

# Website

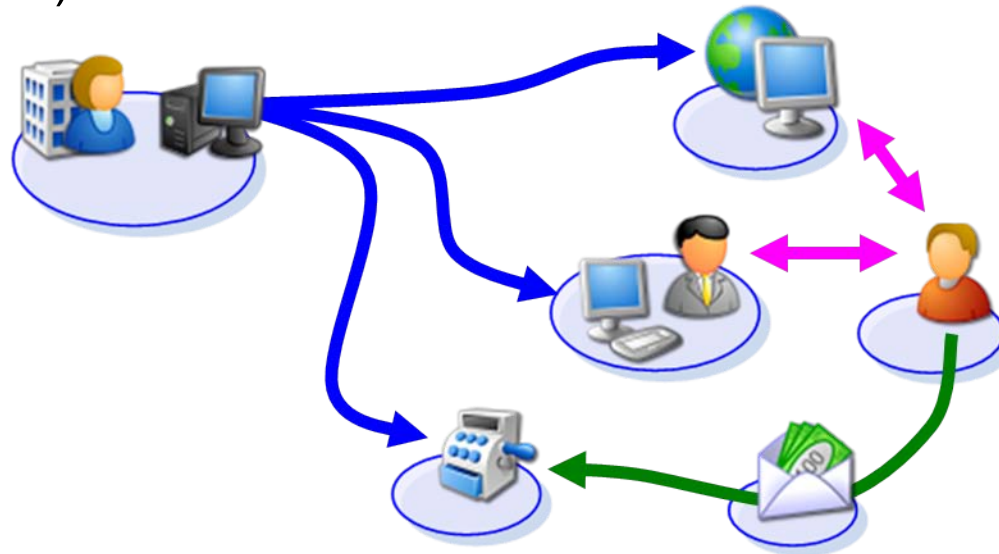
- Data Confidentiality
- Public (General Info) and Private (Customer) Views
- Consumer Portal Best Practices (e.g.: Financial Services)

## Customer Representative

- Data Confidentiality, Integrity
- Filtered View – Billing Related

# Revenue

- Data Integrity, Confidentiality
- Non-Repudiation





# Energy Trader

- Regulated Relationship

## Availability & Control

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

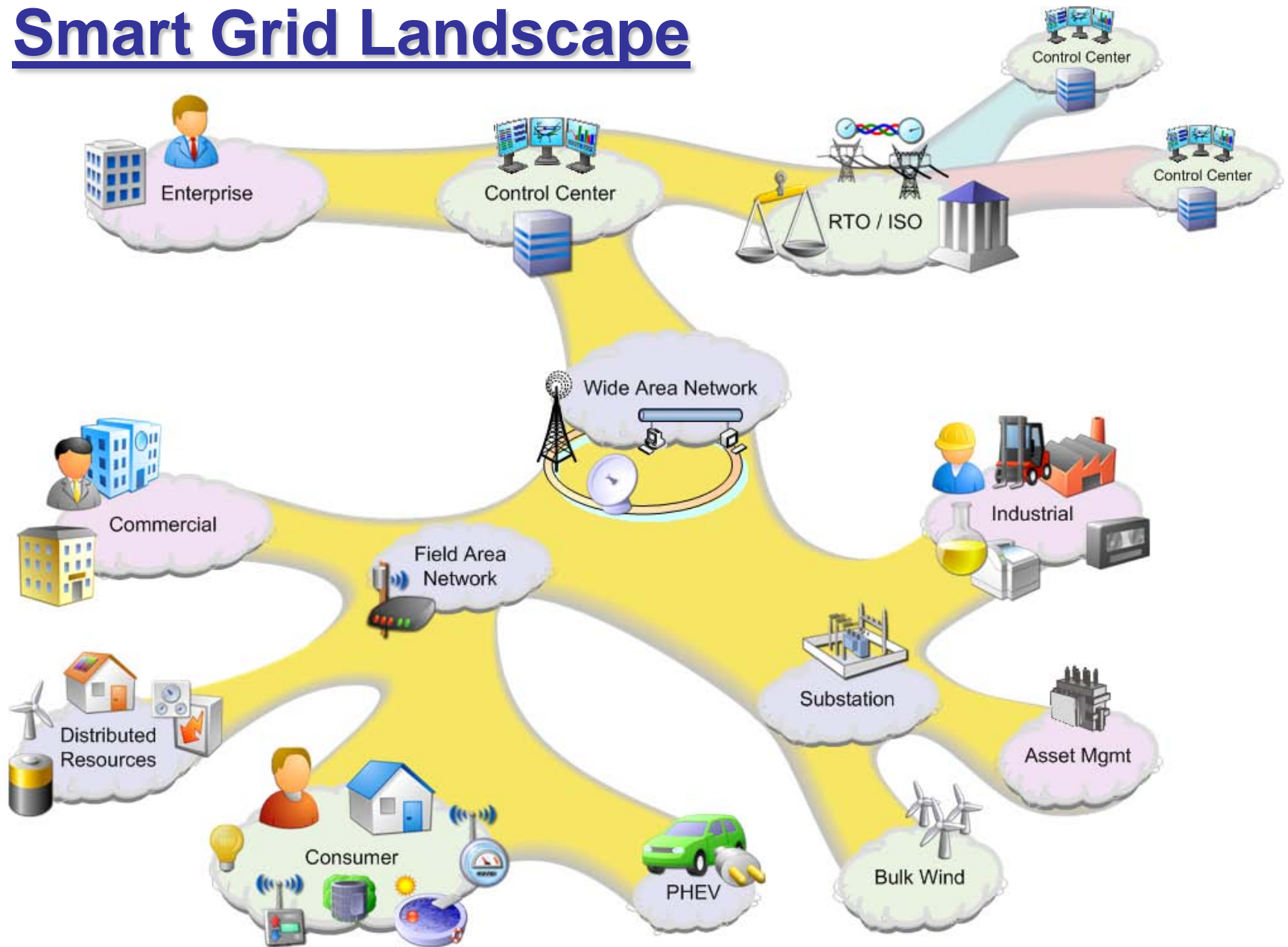
# Vendors & Third Parties

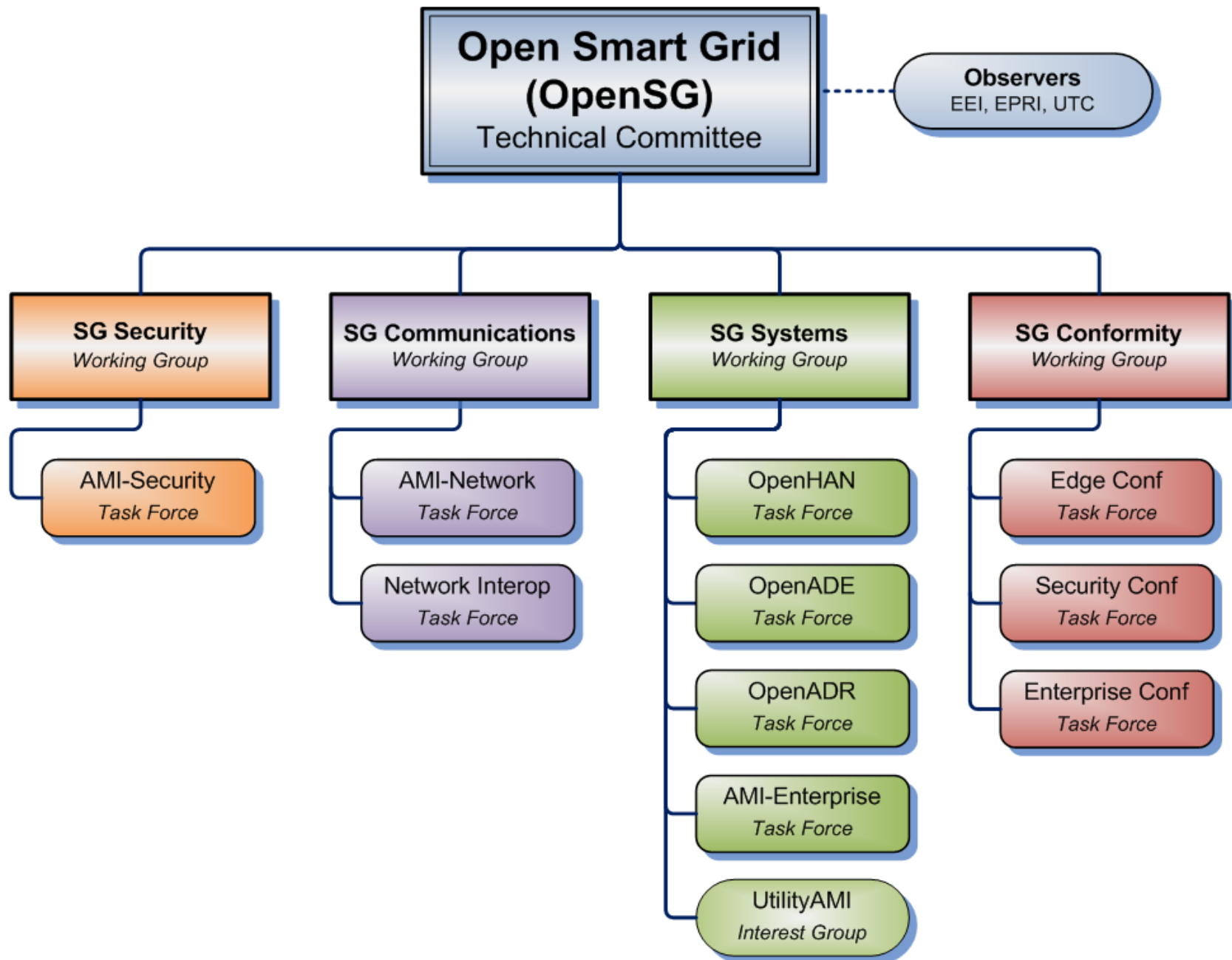
## External Entities

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



# Smart Grid Landscape





# SG Security Working Group



- **Mission:** detailed requirements and best practices guidance for utilities procuring, implementing, and deploying smart grid technology
  - Technology-specific, but vendor-agnostic
  - Feed and accelerate SDO work (IEC, IEEE, etc.)
- **Status**
  - AMI Security Profile v1.0 ratified December, 2009
    - Currently working on v2.0
  - Third Party Data Access Security Profile under review
- **Participation**
  - ~400 Subscribers to various Listservs across 8 countries and 4 continents
  - Broad mix of utilities, vendors, government, and academia
  - Chair: Darren Highfill (SCE), VC: Matt Carpenter (InGuardians), Sec: Bobby Brown (EnerNex)

# **SG Security Charter**

- Chartered with developing detailed security and assurance requirements and security best practices guidance for organizations throughout the lifecycle of smart grid technology
- Technology-specific, but vendor-agnostic guidance
- Feed and accelerate SDO work (IEC, IEEE, etc.)

# AMI-SEC Task Force

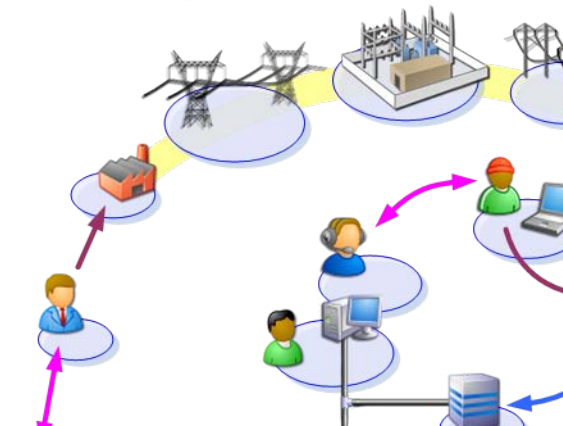
- AMI-SEC is concerned with securing AMI system elements.
  - Contextual Definition:

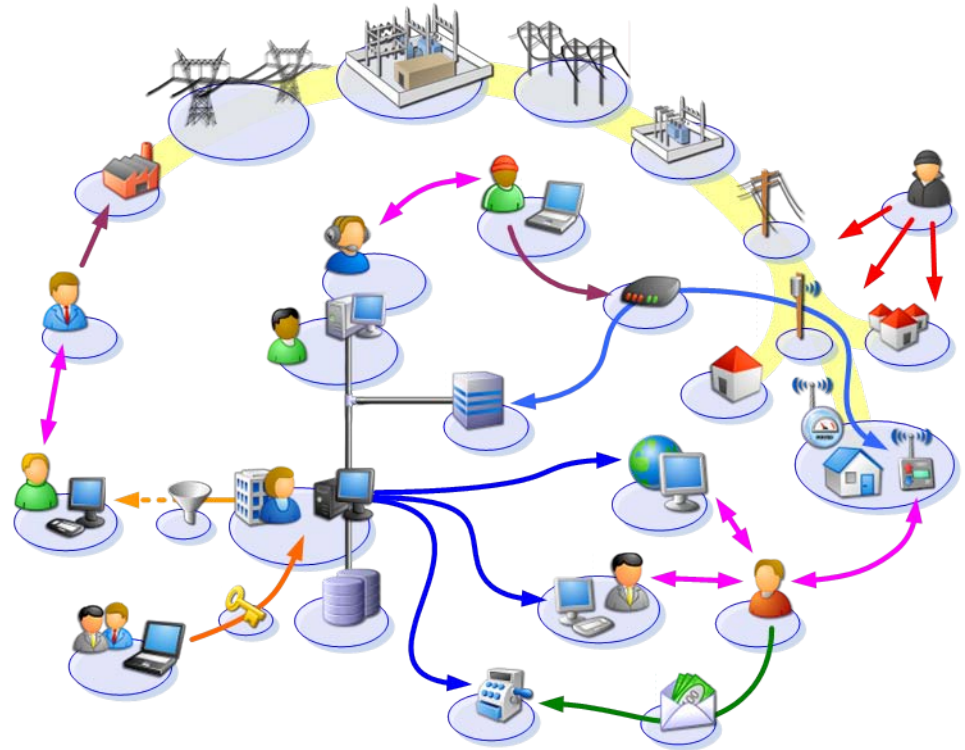
*“...those measures that protect and defend AMI information and systems by assuring their ability to operate and perform in their intended manner in the face of malicious actions.”*
- Purpose
  - Produce technical specification
    - Used by utilities to assess and procure
    - Used by OpenAMI – part of AMI/DR Reference Design
  - Determine baseline level of detail
    - Prescriptive in nature
    - Compliant products will have known functionality and robustness





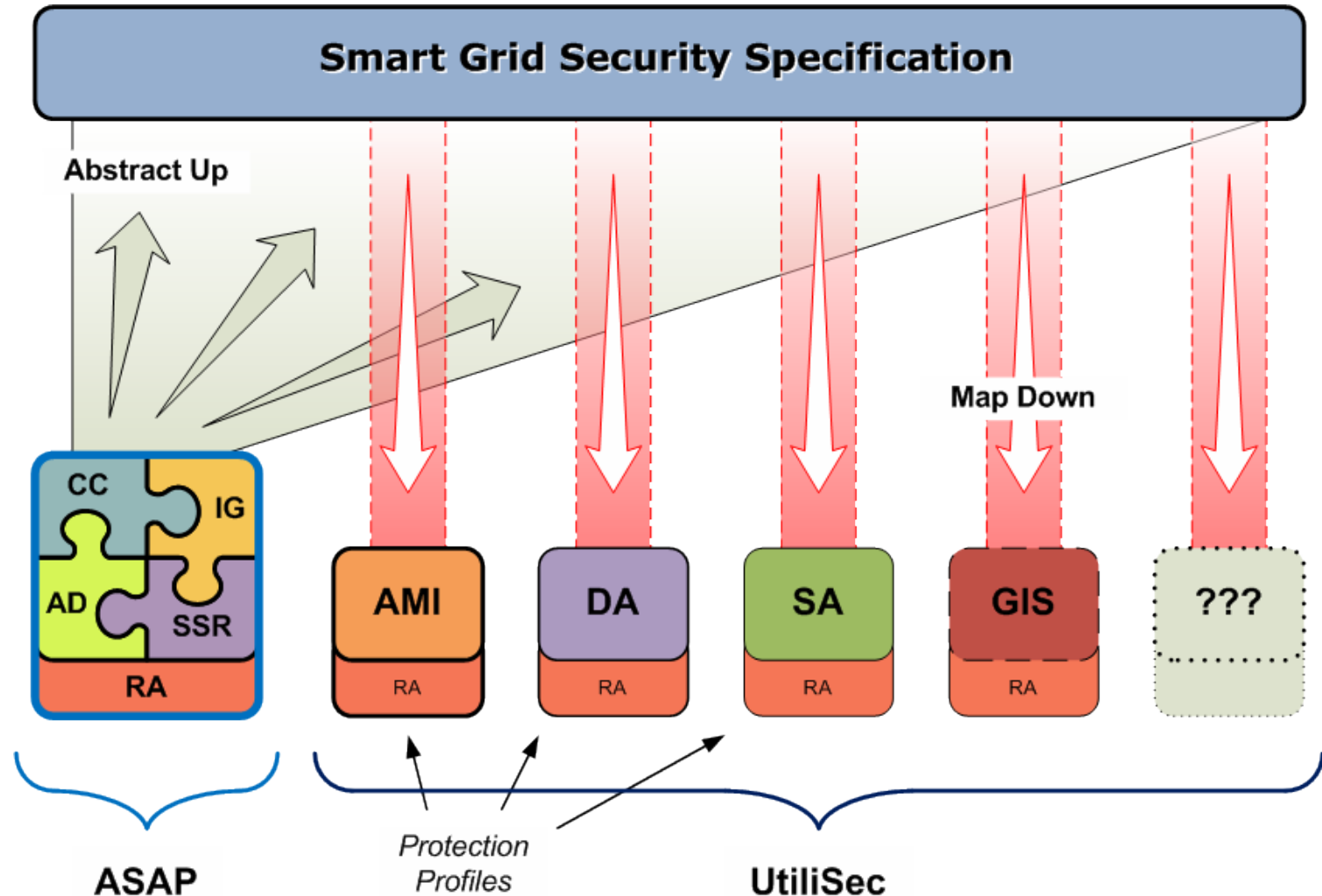
# ASAP-SG

- Public-private collaborative project
    - DOE, NIST, & utilities
  - Purposes:
    - Support the activities of the NIST CSCTG
    - Accelerate the work of the UtiliSec WG
  - Participants:
    - Utilities, regulators, vendors, consultants, national laboratories, & academia
- 

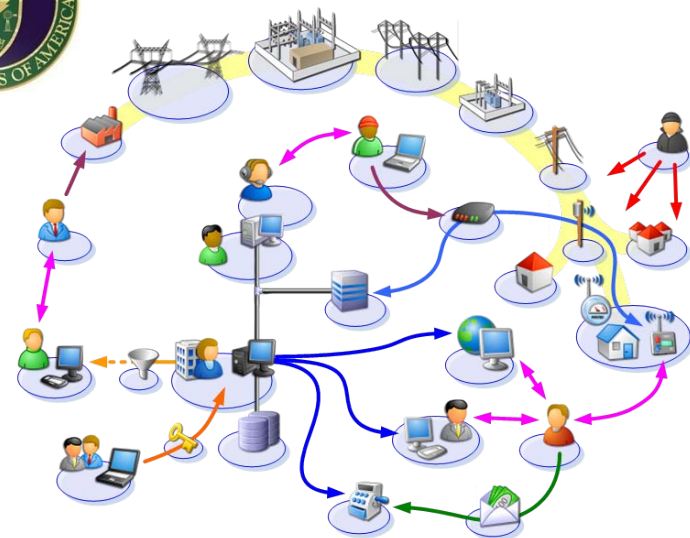




# Leveraging ASAP into ASAP-SG



# ASAP-SG: Summary



- **Project Description:**

- Utility-driven, public-private collaborative project to develop system-level security requirements for smart grid technology

- **Needs Addressed:**

- **Utilities:** specification in RFP
- **Vendors:** reference in build process
- **Government:** assurance of infrastructure security
- **Commissions:** protection of public interests

- **Approach:**

- Architectural team → produce material
- Usability Analysis team → assess effectiveness
- NIST, UtiliSec → review, approve

- **Deliverables:**

- Strategy & Guiding Principles white paper
- Security Profile Blueprint
- 6 Security Profiles
- Usability Analysis

**Schedule:** June 2009 – May 2011

**Budget:** \$3M

(\$1.5M Utilities + \$1.5M DOE)

**Performers:** Utilities, EnerNex, Inguardians, SEI, ORNL

**Partners:** DOE, EPRI

**Release Path:** NIST, UCAIug

**Contacts:**







Bobby Brown [bobby@enernex.com](mailto:bobby@enernex.com)

Darren Highfill [darren@utilisec.org](mailto:darren@utilisec.org)

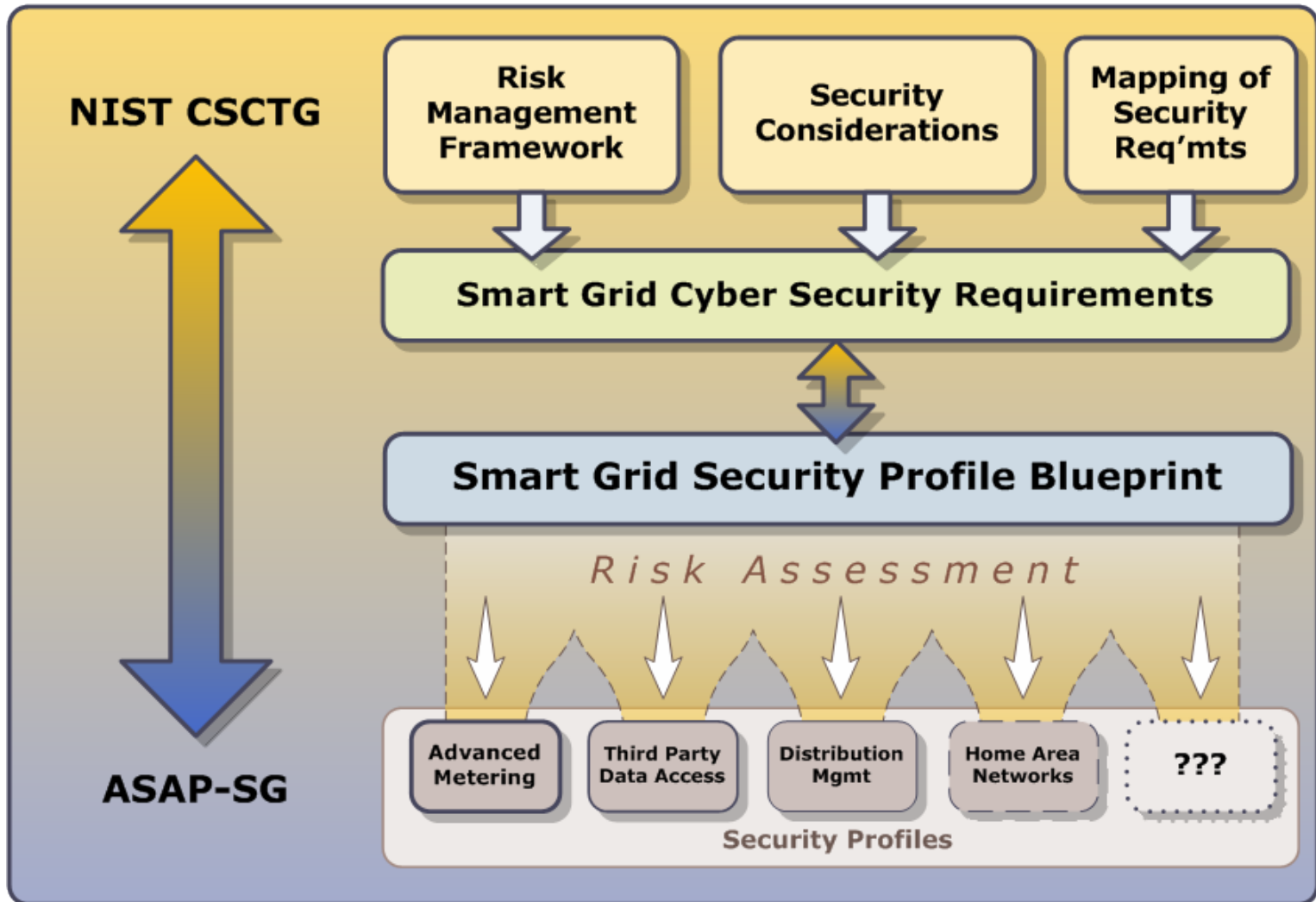
# **Smart Grid Security Profile Blueprint**

- Understandable and user-friendly framework, set of tools, and methodology
- Derive and apply smart grid domain-specific security profiles
- Delineates:
  - Repeatable security risk assessment methodology
  - High-level Smart Grid policy set
  - Smart Grid policy to a domain requirement mapping process
  - Application security profile development process

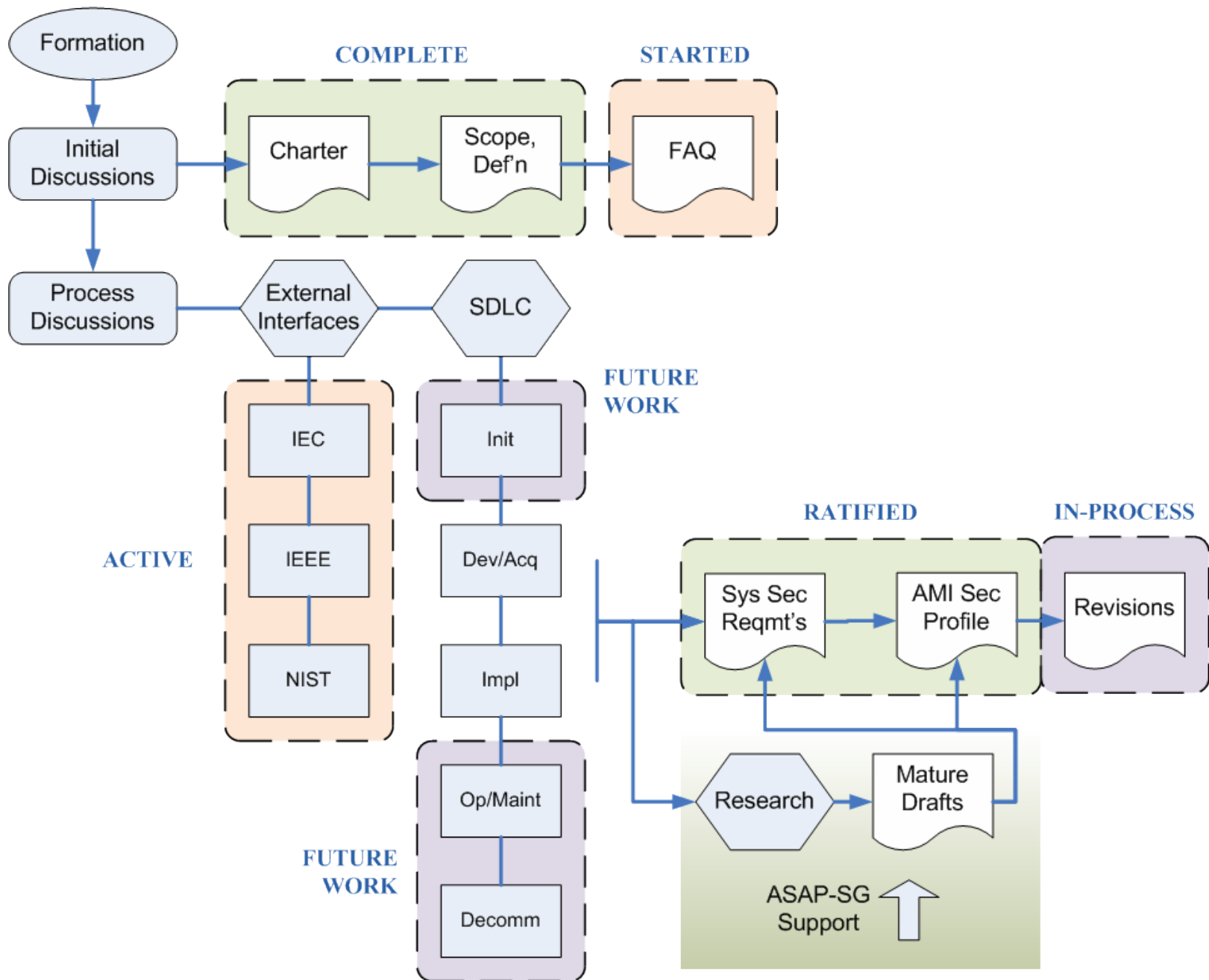
# ASAP-SG Security Profiles

- Prescriptive, actionable guidance
  - How to build-in and implement security
- Tailored to a set of specific smart grid functions, such as
  - Advanced Metering Infrastructure  COMPLETE
  - Automated Data Exchange  COMPLETE
  - Distribution Management  UNDERWAY
  - Home Area Networks  PROPOSED
  - Wide Area Situational Awareness (Synchrophasors)  PROPOSED
  - Substation Automation  PROPOSED

# Technical Coordination with NIST



- Cyber Security Working Group
  - Cyber security focus for Interoperability Framework development
  - Led by Annabelle Lee, NIST
  - Focusing on high-level requirements for securing the smart grid  
***across all stakeholders***
    - Utilities, Grid Operators, Regulators, Consumers, Third Parties
- Numerous active sub-groups
  - “Bottom-up”
  - Vulnerability Analysis
  - Standards
  - Architecture
  - High-Level Requirements
  - Privacy
  - R & D





# Agenda

Day	Timeslot	Subject	Group	Room
Monday	1300-1430	OpenSG Boot Camp	OpenSG	Old Domion (4 <sup>th</sup> Floor)
	1500-1700	SG Security Boot Camp	SG Sec WG	Collonade (6 <sup>th</sup> Floor)
Tuesday	0800-1000	Opening Plenary	OpenSG	Salon I&II (5 <sup>th</sup> Floor)
	1030-1200	Status updates AMI Security Profile v1.9 DOE grants	SG Sec WG AMI-SEC TF	Salon II (5 <sup>th</sup> Floor)
	<b>1300-1500</b>	<b>OpenADE/OpenADR</b>	<b>Joint Session</b>	Salon II (5 <sup>th</sup> Floor)
Wednesday	0800-1000	CyberSec-Interop NISTIR comments ASAP-SG process update	CS-Interop TF SG Sec WG	Salon III (5 <sup>th</sup> Floor)
	1030-1200	Privacy Vulnerability disclosure	SG Sec WG	Salon III (5 <sup>th</sup> Floor)
	<b>1300-1500</b>	<b>OpenHAN</b>	<b>Joint Session</b>	Salon III (5 <sup>th</sup> Floor)
Thursday	<b>1030-1200</b>	<b>AMI-ENT</b>	<b>Joint Session</b>	Salon II (5 <sup>th</sup> Floor)
	1300-1500	External groups (SG Security Conformity, SG Network) Prioritization and planning	SG Sec WG	Old Dominion (4 <sup>th</sup> Floor)
	1530-1730	Closing Plenary	OpenSG	Salon I&II (5 <sup>th</sup> Floor)



# Questions?



[darren@utilisec.org](mailto:darren@utilisec.org)

UtiliSec Collaboration Site  
<http://osgug.ucaiug.org/utilisec>