UCAIug: Smart Grid Security

Web Conference – April 2nd, 2009

→*AMI Security Task Force*

→*UtiliSec Working Group*

AMI-SEC TF & UtiliSec WG Chair:

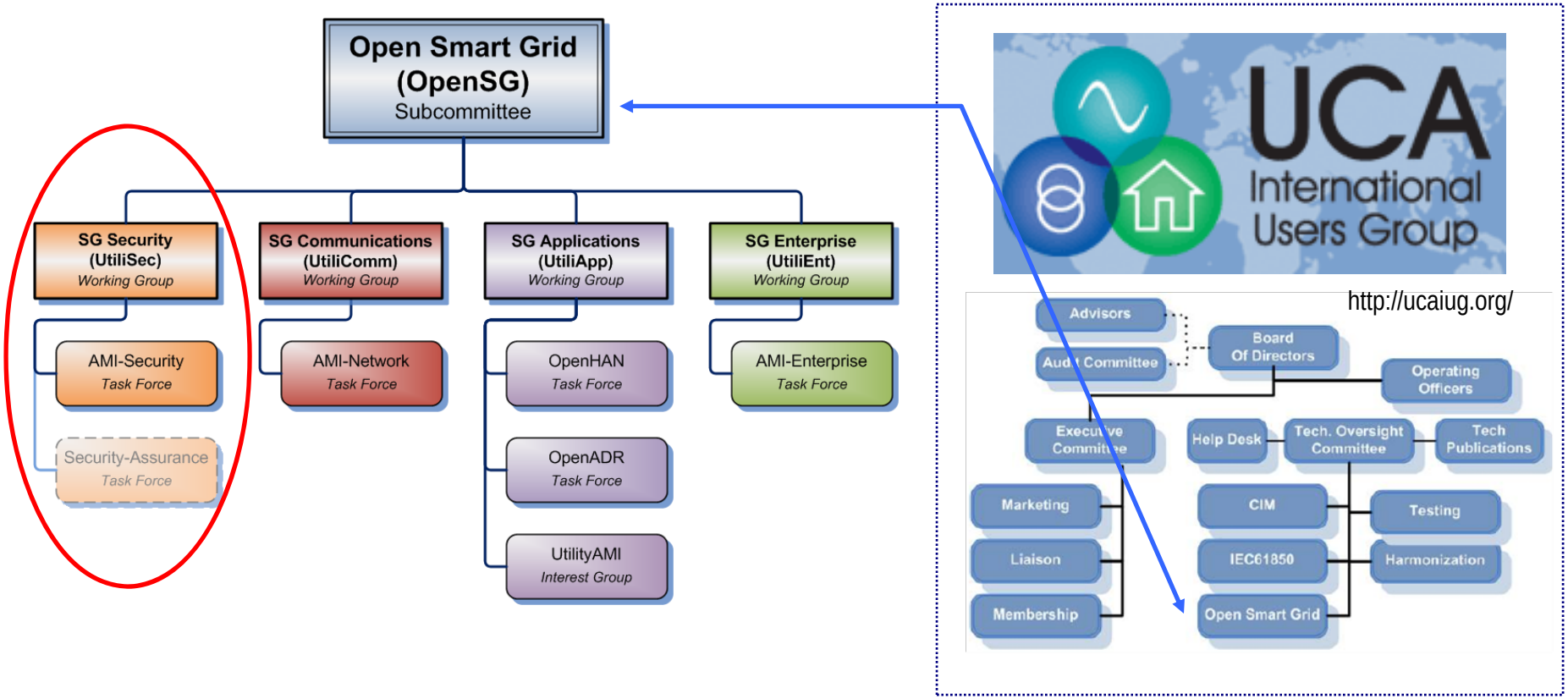
Darren Reece Highfill, CISSP

darren@enernex.com

Agenda

- Preview of ASAP-SG
  - Smart Grid Security Specification
  - Risk Assessments and Security Profiles
  - Participation
- Press about AMI / smart grid security
  - Guiding principles
- Planning and future logistics

UCAIug → OpenSG → UtiliSec

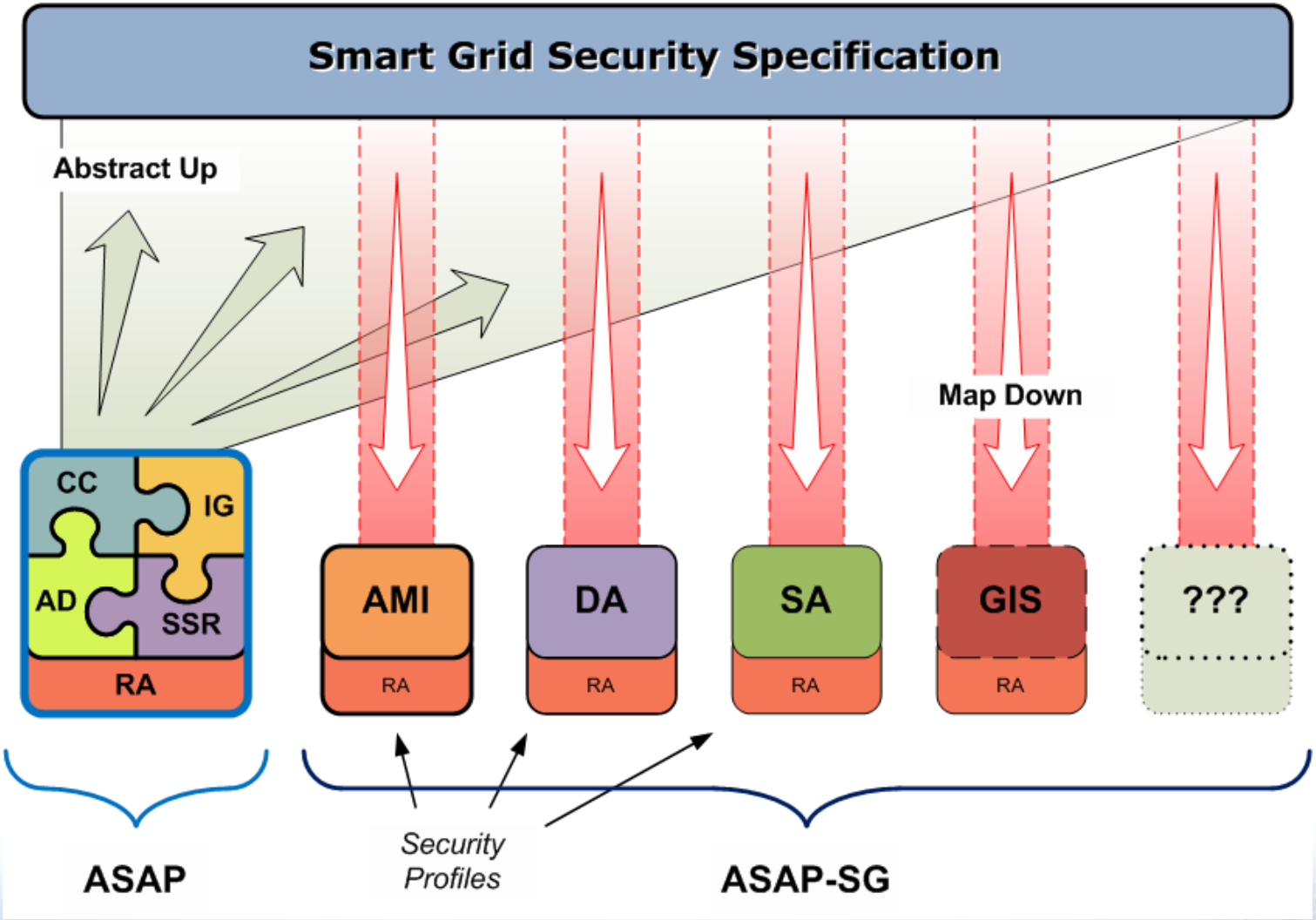


- UtiliSec is focused on developing technology-agnostic requirements for securing smart grid applications
- UtiliSec necessarily coordinates closely with all other OpenSG activities

UtiliSec Working Group

- **Motivation:**
  - Part of a utility-led, electric power industry community effort (***UCAIug***) to define a **common set of requirements** for the procurement of new technologies
- **Status:**
  - Suite of 4 deliverables completed in 2008
    - AMI Security Risk Assessment
    - AMI System Security Requirements (incorporates Architectural Description)
    - AMI Security Component Catalog
    - AMI Security Implementation Guide
  - AMI System Security Requirements document ratified December, 2008 (“1.0”)
- **Current Participation:**
  - 200+ Subscribers to Listserv across 7 countries and 4 continents
  - More than a dozen major North American utilities actively engaged
  - Broad mix of utilities, vendors, government, and academia

Leveraging AMI-SEC into UtiliSec



Smart Grid Security Spec

- 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

Smart Grid Security Spec (continued)

- Scope
  - Generalized security requirements, policies, and processes driven into an application domain for mitigation purposes in subsequent deliverables
- Target Audience: normal level of utility security experience for security architects from utilities, vendors, and system integrators
- Purpose: create a usable and actionable set of policies and procedures

Risk Assessment and Security Profiles

- Prescriptive, actionable guidance for how to build-in and implement security for smart grid functionality
- Tailored to a set of specific smart grid functions, such as
  - Advanced Metering Infrastructure
  - Distribution Automation
  - Outage Management
  - etc.
- May be further decomposed into use case families or even individual business functions

Risk Assessment and Security Profiles (cont.)

- Specifications will be agnostic to vendor, implementation and architecture.
- Scope
  - Risk assessment and security profile for AMI security domains and use cases
- Target audience: normal level of utility security experience for system owners, AMI system implementers and security engineers
  - User is assumed to be experienced at information asset risk estimation
  - User is assumed to be knowledgeable in developing security requirements and guidance

Planning / Logistics

- F2F – Miami: April 16th
  - Full day (9am-5pm EDT)
- Next Telecons?
  - May 7
  - May 28
  - June 18
  - July 2* (two week span)
- F2F – Columbus: July 16th

Questions?

darren@enernex.com

AMI-SEC Collaboration Site
http://osgug.ucaiug.org/utilisec/amisec