Open Meter Users Group
OpenMUG

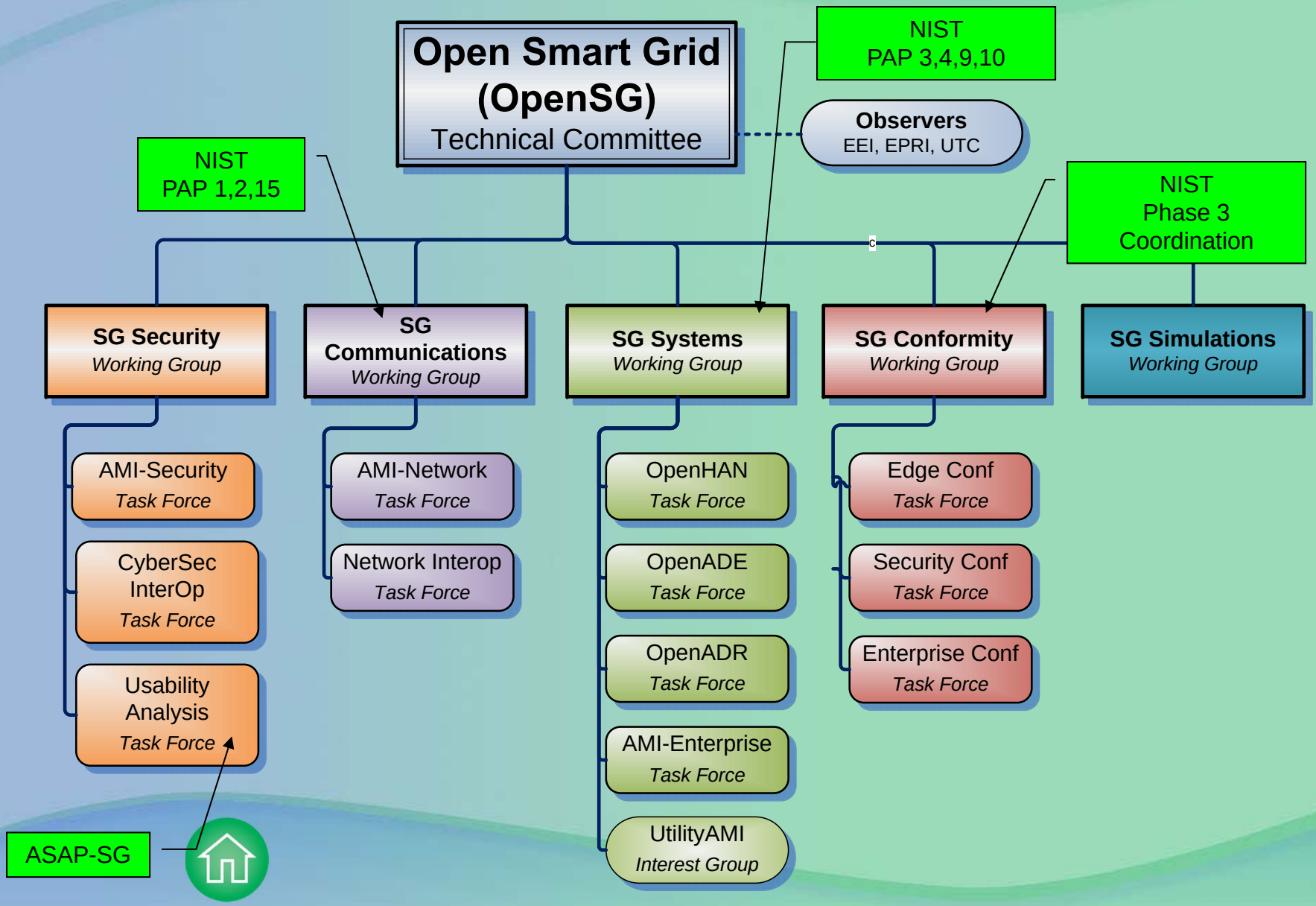
Aaron F. Snyder, EnerNex

OpenSG users group

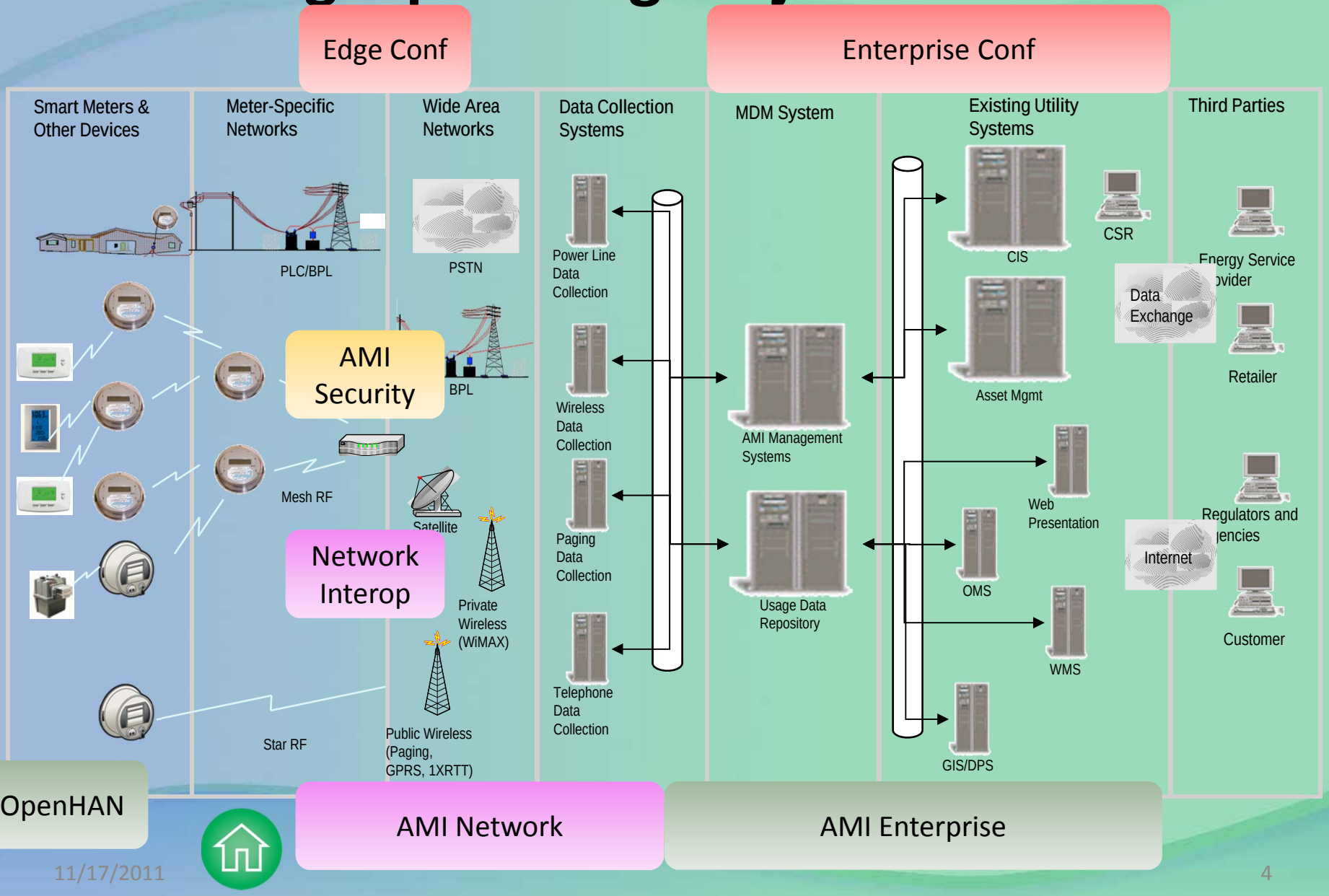
Agenda

- Background
- Motivation for group
- Prepare draft charter
- Next steps

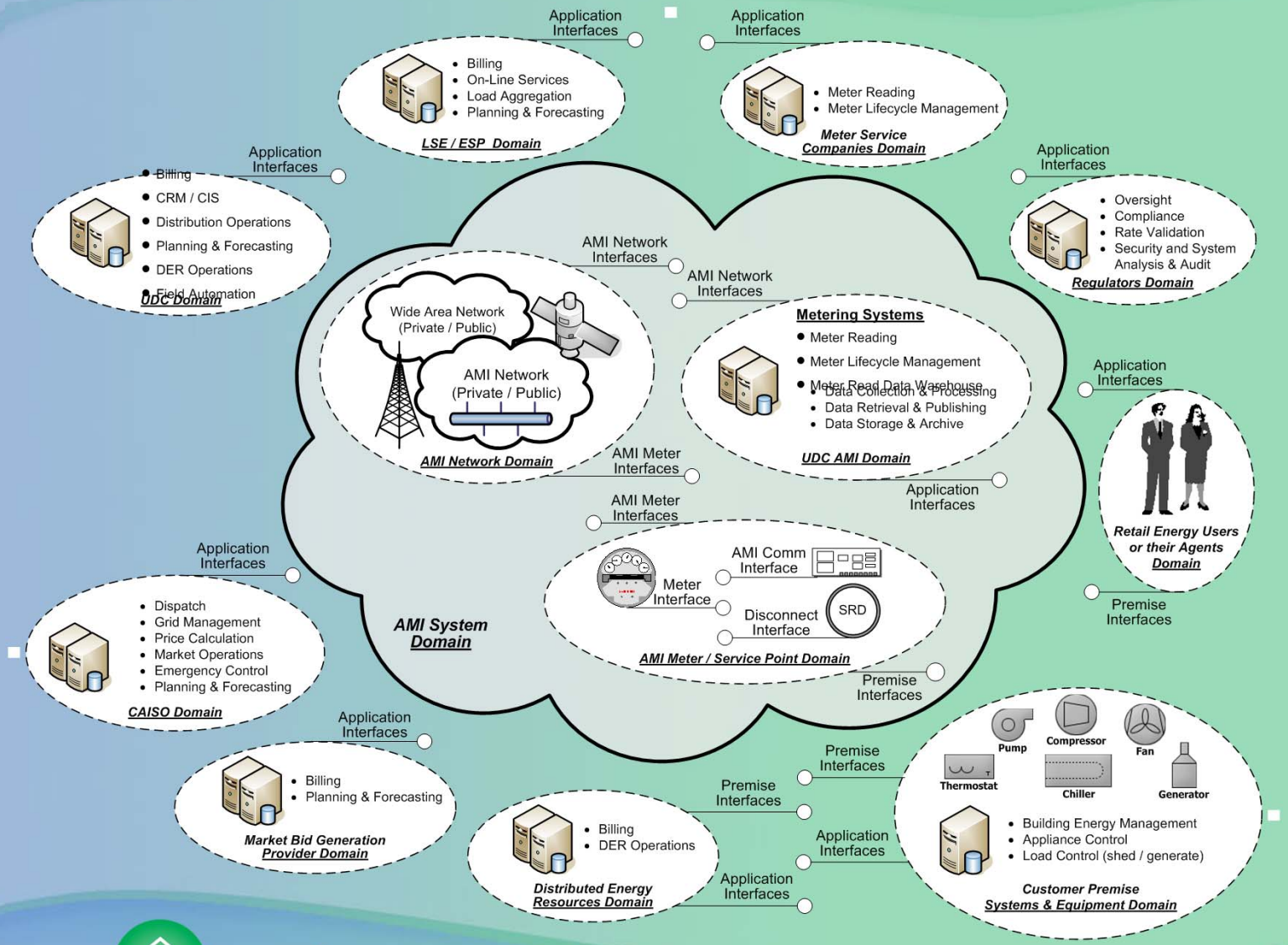
UCAIug-OpenSGug Major Work Areas



UCAIug-OpenSGug Major Work Areas



UCAIug-OpenSGug Major Work Areas



Background

Motivation for group

Prepare draft charter

Next steps

MOTIVATION FOR GROUP

Motivation for Group

- Define utility security requirements for meters (SGIP CSWG review of ANSI C12 standards)
  - http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/CSCTGStandards
- Define utility meter conformity and interoperability testing requirements
- Capture tribal knowledge of the art of metering at a utility

SGIP CSWG C12.1 Review

- ANSI C12.1, http://collaborate.nist.gov/twiki-sggrid/pub/SmartGrid/CSCTGStandards/CSWG_Standards_ANSI_C12.01_Review_final.docx
- CSWG Recommendations
  - Although basic physical security considerations have been included in the standard, such as sealing the meter against unauthorized access, it does not attempt to address the more complex cyber-physical security requirements of electric meters with sensitive and private information stored within it.
  - It is therefore recommended that a standard be developed to cover the cyber-physical security requirements of electric meters, including:
    - The impact of physical tampering, physical damage, and unauthorized physical access on the security of the stored information and the communication of that information, and
    - The use of physical technology, including hardware technology, to help protect cyber information, deter attackers, and/or provide information on what or how an attack was made.

SGIP CSWG C12.18 Review

- ANSI C12.18, http://collaborate.nist.gov/twiki-sggrid/pub/SmartGrid/CSCTGStandards/CSWG_Standards_ANSI_C12.18_Review_final.docx
- CSWG Recommendations
  - Access through the optical port should be made more secure, such as ensuring that optically opaque shielding and/or using a challenge/response authentication mechanism prohibiting the replay of credentials. Either extend the ANSI C12.18 protocol to address this deficiency or update the ANSI C12.22 communication interface over ANSI Type 2 optical port, to supersede ANSI C12.18.
  - Audit logging and storage security requirements should be added to this or a related standard.

SGIP CSWG C12.18 Review

- ANSI C12.19, http://collaborate.nist.gov/twiki-sggrid/pub/SmartGrid/CSCTGStandards/CSWG_Standards_ANSI_C12.19_Review_final.docx
- CSWG Recommendations
  - More importantly, it is recommended that a comprehensive standard be developed to address cybersecurity requirements for metering systems, including the secure storage of sensitive and private information, authentication requirements for accessing information, and protection for security-relevant information, such as passwords. For instance, in order to conform to such a cybersecurity standard:
    - Sensitive fields within tables should be required to be protected against unauthorized access.
    - Table 78's "signature" fields should be required to use an authenticated integrity technique to protect against malicious reprogramming and audit log manipulation.
    - Audit logs should capture all sensitive events, including tampering, changing of access controls on fields, recalibration of metrology, changes affecting performance, and physical changes.

SGIP CSWG C12.21 Review

- ANSI C12.21, http://collaborate.nist.gov/twiki-sggrid/pub/SmartGrid/CSCTGStandards/CSWG_Standards_ANSI_C12.21_Review_final.docx
- CSWG Recommendations
  - Either deprecate C12.21 or extend it, using the identification service extension mechanism to support a better security model.
  - The use of the DES cryptographic algorithm should be deprecated for any new meters, although it may remain supported for older meters.

SGIP CSWG C12.22 Review

- ANSI C12.22, http://collaborate.nist.gov/twiki-sggrid/pub/SmartGrid/CSCTGStandards/CSWG_Standards_ANSI_C12.22_Review_final.docx
- CSWG Recommendations
  - The standard should correct, through addendums or other mechanisms, the explicit issues identified in the last bullet in section 2.3.3 of this review.
  - One or more additional cybersecurity documents should be developed to:
    - Clarify all of the assumptions made in the C12.xx series with respect to cybersecurity.
    - Identify the exact location and implications of the cybersecurity requirements in this series of standards.
    - Provide higher level guidance for cybersecurity policies, methodologies, and technologies that are out of scope for these individual standards but that are needed for securing the networking infrastructure.
    - Provide cybersecurity requirements for metering devices that mandate features assumed or supported by ANSI C12.22 but not mandated there. Such requirements should implement NISTIR requirements related to equipment.
  - Only pre-stored keys are referenced in the default security mechanisms, thus leaving key management outside the scope of this standard. A new proposal was made to ANSI C12 SC17 to work on a key management add-on standard for C12.22. This is may be contributed to the SGIP for the formation of a new PAP.
  - The ANSI C12.22 Standard should be revised to be more specific on whether the C12.22 Master Relay should prevent de-registration unless approved by a C12.22 Authentication Host. This way a rogue node may not cause a malicious deregistration of C12.22 Nodes from the network.
- The standard is not well structured for understanding what cybersecurity requirements (or options) actually exist. The document mixes normative and informative items that are not clearly distinguished, and does not clearly identify the security aspects.
  - Some cybersecurity guidelines do exist in other documents, such as the AEIC document developed in PAP 5: “SmartGrid/AEIC AMI Interoperability Standard Guidelines for ANSI C12.19 / IEEE 1377 / MC12.19 End Device Communications and Supporting Enterprise Devices, Networks and Related Accessories”. Although focused on interoperability issues, that document did identify some cybersecurity gaps in ANSI C12.22.
  - Some other documents provide more general guidelines on implementing cybersecurity for metering systems.

Motivation Continued…

- Define utility meter conformity and interoperability testing requirements; identify gaps in…
  - ANSI Standards
  - FCC Requirements
  - New equipment (service switch)
- Capture tribal knowledge of the art of metering at a utility
  - Utility expectations of conforming devices, and do they really mean interoperable devices?

Background

Motivation for group

Prepare draft charter

Next steps

PREPARE DRAFT CHARTER

Proposed Short Description

"OpenMUG is a forum for defining conformity and interoperability requirements and guidelines for electricity, water and gas metering (and meter + communications) products."

Proposed Scope

- OpenMUG *will* develop recommendations for SDOs, expressed as requirements. The work products of OpenMUG will be published as UCAIug products and submitted to the appropriate SDO's (*e.g.*, ANSI C12, IEC TC13 WG14) so that their efforts may consider how *users* view those standards.
- OpenMUG *will* develop requirements for conformance certification programs along the lines of the IEC 61850 users group under UCAIug and the SGIP Smart Grid Testing and Certification Committee (SGTCC).
- OpenMUG *will* facilitate users of metering products and communication systems leveraging industry experience and standards across the entire utility enterprise by bringing together the metering communications experts, distribution automation and communications experts, and utility information system architects.
- OpenMUG *will not* develop standards.
- OpenMUG *will not* interpret standards – this is a portion of the scope of work of the standards developing organizations.

Background

Motivation for group

Prepare draft charter

Next steps

NEXT STEPS

Next Steps?

- Create formal charter, get OpenSG TC approval
  - Chair
  - Vice Chair
  - Secretary
- Define deliverables, leads, schedule
- Setup periodic Webmeetings, F2F to meet schedule and deliverables