Standards and Security Interoperability in the Smart Grid

Ralph Martinez, PhD
Chief Scientist
Balance Energy™
1 September 2009

ralph.martinez@baesystems.com
Topics

• Smart Grid Activities
• Recent Efforts to Define the Smart Grid
• Security Standards for Smart Grid
• Interoperability in Security
• Plans for the Smart Grid
• Summary
Applied Experience to Smart Grid

- **Emerging cyber capabilities**
  - Large, complex systems
  - Adverse warfare environments
- **Critical infrastructure protection**
  - Shift from platform to data
  - “Active” protection

**Smart Grid Domains**
- Large-scale system of systems engineering and integration
- Renewable resources and storage
- Energy mgmt. systems and services
- Power and control mgmt. systems
- Decision support aids
- Information systems
- Wireless comms and networks
- Cyber security (information assurance)
- Netted sensor systems
- Geospatial systems
- Secure facilities construction mgmt.
- Hybrid electric vehicles
- Deployed mobile platforms
- Global services footprint
Smart Grid Activities

Federal
- FERC
- EISA 2007
- EPACT05 Hearings

State
- T24
- CEC PIER
- Individual Utilities
- MEMS

Private
- EEI
- GridWise Alliance
- Galvin Initiative
- EPRI IntelliGrid
- UCA Users Group WG’s
- IEEE IGCC
- Zoltek Intelligrid

Vision / Operating Model
- European Technology Program - SG
- NIST Roadmap
- NETL Modern Grid Strategy
- LBNL DRAS AUTO DR
- NW GridWise Testbed
- GridWise Program
- CERTS
- CPUC AMI
- NYSERDA
- PSERC
- DOE-OE

Policy & Regulation
- DOE-OE Grid 2030
- NERC (FM)

Systems Integration
- GridWorks
- GridApps

Technology R&D Initiatives
- EPACT05 Hearings

Smart Grid Activities
- T24
- CEC PIER
- Individual Utilities
- MEMS
- Zoltek Intelligrid
- UCA Users Group WG’s
- IEEE IGCC
Recent Efforts to Define the Smart Grid

• EPRI Intelligrid Project, 2006
  –Lack of system and enterprise security architecture

• DOE Modern Grid Initiative, 2006-2008
  –Security a key feature, not system approach or solution

• International Electro-Technical Commission (IEC) Standards in Power Grids
  –Point solutions in security and SCADA standards

• IEEE Standards in Power and Energy
  –Interface standards, minimum security architecture (P1547, P2030), New Working Group

• GridWise Alliance, GWAC Interoperability Framework
  –Addresses security characteristics

• AMI-Sec, Security Requirements, UCAIug document
  –AMI security and start to attempt smart-grid system security

• NIST/EPRI 2009, Smart Grid Interim Roadmap
  –Develop a plan for testing and certification to ensure that smart-grid equipment and systems conform to standards for security and interoperability
  –System integration and security covers networking and exchanges of information among disparate systems. Issues include interoperability of interconnected systems, cyber security, access control, data identity across systems, and messaging protocols. Address cyber security issues
  –Develop security methodology and framework
  –Security control from previous NIST standards
Security Standards for Smart Grid *

An Example of How The IEC and Utilities are Collaborating to Define Interface Standards Based on Common Semantics

IEC TCs

IEC Strategic Group on Smart Grid (SG3)

IEC TC8

Contextual Framework

Business Requirements / Use Cases

IEC TC57

WG14

TC57

WG14

http://osgug.ucaiug.org/


http://ucaiug.org/

http://cimug.ucaiug.org/

Open Smart Grid (OpenSG) Subcommittee

SG Security (Util/Sec) Working Group

SG Communications (Util/Comm) Working Group

SG Energy (Util/App) Working Group

SG Enterprise (Util/Ent) Working Group

Security SRS Task Force

AMI-Network Task Force

AMI-Security Task Force

OpenHAN Task Force

OpenADR Task Force

Utility/AMI Interest Group

ZigBee Alliance

HOMEPLUG

IEC 61968 (CIM)-Based Information Exchange

Event Histories

AM/FM/GIS

ERP

Work Management

Network Design

Network Planning

Enterprise Semantics

Data Warehouse

EMS

Distribution Management

Distribution Automation

Customer Information

SG Enterprise

SG Security

SG Communications

SG Energy

SG Enterprise

* Greg Robinson, Xtensible Solutions, OpenSG, 13-16 July 2009, Columbus, OH


http://osgug.ucaiug.org/

http://ucaiug.org/

http://cimug.ucaiug.org/

* Greg Robinson, Xtensible Solutions, OpenSG, 13-16 July 2009, Columbus, OH
Use cases definitions
In each Domain that include Security

Conceptual Model

* NIST/EPRI Smart Grid Interim Roadmap Report, June 17, 2009
(IEC) Technical Council (TC) 57: Power Systems Management And Associated Information Exchange

- **IEC 60870-5** which is widely used in Europe and other non-US countries for SCADA system to RTU data communications. It is used both in serial links (Part 101) and over networks (Part 104).
- **DNP 3.0** which was derived from IEC 60870-5 and is in use in the US and now is widely used in many other countries as well, primarily for SCADA system to RTU data communications.
- **IEC 60870-6** (also known as TASE.2 or ICCP) which is used internationally for communications between control centers and often for communications between SCADA systems and other engineering systems within control centers.
- **IEC 61850** which is used for protective relaying, substation automation, distribution automation, power quality, distributed energy resources, substation to control center, and other power industry operational functions. It includes profiles to meet the ultra fast response times of protective relaying and for the sampling of measured values, as well as profiles focused on the monitoring and control of substation and field equipment.
- **IEC 61334 (Device Language Message Specification ,DLMS)** is the suite of standards developed and maintained by the DLMS User Association and has been co-opted by the IEC TC13 WG14 into the IEC 62056 series of standards. COSEM or Companion Specification for Energy Metering, includes a set of specifications that defines the Transport and Application Layers of the DLMS protocol. The DLMS User Association defines the protocols into a set of three specification documents namely Green Book, Yellow Book and Blue Book.
- All together, these international standards account for close to 90% of the data communications protocols in newly implemented and upgraded power industry SCADA systems and substation automation (Modbus, Fieldbus, and other proprietary protocols are still used in older systems and in other industries).

SCADA Security Point Standards, Lack of System Security Approach
Enabling Utility-Scale Cyber Security For The Smart Grid

**Situation understanding**
- Assisted and automated response
- Cyberattack patterns
- Network surveillance
- Spectrum management
- RF network access and attack
- HW/SW agents and payloads
- Cyber forensics

**Defense**
- Intrusion detection and prevention
- Deep packet inspection
- Network monitoring
- Advanced analytics
- Network analysis
- Wireless networking
- Knowledge domain sharing
- Services-oriented architecture
- Data center at-rest security

**Support**
- System performance analysis
- Certification and accreditation
- Insider threat detection / ID mgmt.
- Managed SOA IT services
- Enterprise applications integration
- Knowledge domain engineering
- Network operations and maintenance

**Offense**
- Enterprise systems engineering and integration
- Fixed-wireless comms and network infrastructure

**Smart-grid infrastructure modernization**

**Mission operations analysis**

**Operational & IA Capabilities Analysis**
- Risk Assessment
- Policy Analysis
- IA Systems Capability Definition
- IA Technology Analysis
- Architecture Integration

**Repeatable process**

**Best practices**
Approaches for Interoperability in Security

- Enterprise Security Architecture Framework
  - Functional and services decomposition and interfaces
  - “Baked In” design attributes
- Hierarchical Gateways
  - Message, protocol, interface, and waveform translation
- Domain Common Information Models
  - Message translation via domain CIMs
Summary

• Many standards developments complicate the cyber security interoperability problem

• Architectural driven security and interoperability approaches are recommended to mitigate point solutions enterprise security and interoperability

• A need exists for a Smart Grid “czar agency” to dictate policy and regulations for cyber security in the Smart Grid (i.e., analogous to the Department of Defense and NASA models)