A New Era of Adopting Standards?

Need to Know Now?

Guidelines or Standards?

Actions Needed?

Key Players?

Real-World Trials
Introductions

• Klaus Bender - UTC

• Jon Stitzel – Burns & McDonnell

• Jarad Howard – Burns & McDonnell
Klaus Bender – Standards Update
Why NIST Standards?

- Energy Act of 2007
- Smart Grid Stimulus Funding
- Potential for Malicious Access?
The Smart Grid Wave

• Administration and industry identify electric infrastructure upgrades as key to:
  – Consistent reliable power
  – Demand reduction
  – Distribution automation
  – Reduced dependence on foreign energy products
  – Integration of renewable energy sources

• Congress acts to enact legislation
Many Smart Grid Players

Source: EnerNex, Inc.
Energy Independence and Security Act (EISA) of 2007
Title XIII, Section 1305.
Smart Grid Interoperability Framework

“In cooperation with the DoE, NEMA, IEEE, GWAC, and other stakeholders, NIST has “primary responsibility to coordinate development of a framework that includes protocols and model standards for information management to achieve interoperability of smart grid devices and systems…”

George Arnold, NIST senior level executive
National Coordinator for Smart Grid Interoperability
Three Phase Process
1. Releasing Roadmap as living document
2. Create smart grid interoperability panel (SGIP) and governing board
3. Create testing and certification process - in progress
Roadmap Focus Areas

- FERC-Identified Priority Applications:
  - Demand Response
  - Wide-Area Situational Awareness
  - Electric Storage
  - Electric Transportation
- Additional Priority Applications:
  - Advanced Metering Infrastructure
  - Distribution Grid, Including Distributed Energy Resource Integration
- Cross-cutting priorities
  - Cybersecurity
  - Data networking (i.e. Telecommunications)
The “Roadmap”

- Excellent Reference Document
- Breaks Down Smart Grid Into Manageable Pieces
- Identifies Gaps In Standards Through PAP’s And Subtasks
- Identifies Contributors To Complete Tasks
- Resulting Requirements Mapped To Standards
Conceptual Model

Source: NIST
Levels of the Conceptual Model

Domain Diagram

Model Level
- Domain
- Actor or Application
- Drill-Down / Domain Expansion

Source: NIST

From PAP Project Lifecycle Process
- Notify PMO
- Coordinating with Technical Champion to complete paperwork
- Complete PMO Checklist for completion of all PAP work items

The PAP team may recommend for or against including the standard in the catalog.

Return to PAP Lifecycle
- Notify PAP leadership, SSO, SGIP leadership, provide instructions to PAP team to address issues (if necessary)

PAP Working Groups

PMO

Governing Board

SGIP Administrator

SGIP Valuing Member Reps

CSWG and SGAC

Complete CSWG and SGAC Checklists

Ensure Standard is available on SGIP/SANS Portal or TWiki

Revise PAP/PMO Standards Recommendation document

Vote on recommending addition to SGIP Catalog. Any comments captured will be included on the member ballot for that standard.

GB Recommendation

Tally votes, 75% in favor

The Governing Board may recommend for or against including the standard in the catalog.

Add to SGIP Catalog of Standards

Notify SGIP members

GB affirms PAP closure

Is PAP Done?

Yes

No

Always

Yes

No
Jon Stitzel – Cyber Security
Smart Grid Cyber Security

- SGIP Cyber Security Working Group
  - NIST Sponsored
  - NISTIR 7628: Guidelines for Smart Grid Cyber Security

- UCA International OpenSG Working Group
  - AMI System Security Requirements
  - Also Collaborating with SGIP
• NISTIR 7628
  – Version 1.0 released in Q4 2010
  – Over 300 participants from industry, vendors, & cyber security
  – Includes Large Section Outlining Privacy Assessment
Volume 1 Provides Guidance for Cyber Security Strategies

- Outlines Tasks
- Risk Assessments
- High Level Architecture
- Outlines Privacy Concerns and Assessments
NISTIR 7628

Volume 2 Details Specific Security Controls

- Organized by Impacted Logical Interfaces
- Focus on C.I.A. Model

Volume 3 Provides Additional Research Information

- References and Analysis Used to Create NISTIR
OpenSG Working Group

- AMI System Security Requirements
  - Foundational Smart Grid Cyber Security Document
- Newest version is 2.0
- Working with many Organizations, including SGIP CSWG
- Conformity
- Testing and Certification
- Vulnerabilities
Jarad Howard – A Real World Example
5 Standards Approved as Foundational

- IEC 61970: API for EMS communication
- IEC 61968: API for Distribution Automation
- IEC 61850: Information description and protocol for substation automation
- IEC 60870-6: Information exchange between control centers, formally ICCP.
- IEC 62351: Cyber security
What's In The Standards

- Not Just Protocols
- Use Cases
- Define Actors
- Common Information Model (CIM)
- Communications Protocol
• DOE Funded Smart Grid Demonstration Project
• Committed To Following The Standards
  – Exploring Application of Guidelines
• Piloting Lots Of Innovative Ideas & Systems
  – Operating It Like Separate District With Slightly Different Procedures Based On New Systems
• Documenting “Real-World” Best Practices & Lessons Learned
  – Shared Learning Nationally
Project Description

• Smart Grid Demonstration Project
  – Distribution Management System
    • Real-Time Electric Model Based On GIS Data
  – Meter Data Management System
    • Integrates AMI, AMR, & Manual Systems
  – Home Area Network
    • Load Control Via Thermostats & Switches
Developing Use Cases

1. Start With Published Use Cases
2. Easy To Identify Differences
3. Faster Than Developing From Scratch
4. Migrate Toward Industry Standards
Use Case Development

- Labor Intensive
- Clarifies Communication
- Incompatibilities Identified – Accountable Parties for Solutions Defined.
- Invaluable In Communicating & Evaluating Project Deliverables.
- Establishes “Best Practices” — Post Project “+’s” and “-’s”
• Procurement Challenges
  – Must Vendors Follow Standards?
  – Standards Are Not Approved
• ARRA Wants You To Stimulate Economy
  – Spending $ Prior to Use Case Results
• Proven Smart Grid Business Case
• Long-Term Costs of Grid Complexity & Automation Unknown
Procurement Process Inclusion

- Incorporate Standards From Project Start.
- Mandate Standards Compliance in Procurement Documents.
- Can Reduce Procurement Risks.
- Encourages Standards Adoption by Vendors.
Go-Forward Strategy

- Standards Committee Participation
- **Stay Current** – Draft Standards, Proposed Changes, Final Approval Dates
- Company & Organizational “Champion”
- Procurement Process Inclusion
- Provide What You Have Today With A Promise To Upgrade In Future
FERC Technical Conference

- FERC open meeting 1/31/2011 to discuss “sufficient consensus”
- Two panels with written testimony and discussion
- Industry experts and observers testified
• George Arnold opening statements:
• Five IEC Standards
  – Fit within the NIST process
  – Because they are a “good start” and are “mature”
  – Added that DNP3 and MultiSpeak may be included as part of the Framework later following a cybersecurity review by the Cyber Security Working Group (CSWG)
• **Panelist Comments**
  
  • Standards review process needs to improve and introduce more phases and rigor as to give better assurance of clarity, consistency, and broad acceptance
  
  • Currently the SGIP is structured such that someone who decides to open a one-person business has the same vote as a utility
  
  • Only one standard addresses cybersecurity (IEC62351) and this standard needs updating
  
  • Three main issues: transparency issues, consensus issues and process/participation issues
  
  • Initial IEC group sent to FERC “lack of functional review of the standards”
Panelist Comments

- NIST did not prioritize input from utilities
- Five IEC standards are a “good start, but as currently written are neither comprehensive (communication centric) nor do they provide any specifications for security certification.”
- Utility representation was effectively diluted as “one voice among many” in NIST
Panelist Comments

- Standards must evolve over time and that they should be assessed according to four criteria:
  - a) Established standard compliance and interoperability testing regimes;
  - b) Products from multiple suppliers are “commercially available”;
  - c) Successful reference implementations; and
  - d) Backward compatibility assessment or legacy migration considerations.

- It is critical that NIST consider the licensing rights associated with certain standards before they are adopted.
• George Arnold, NIST
• This question of what “adoption” means is really critical.
  • If it means they are mandatory, and everyone assumes that to be the case, my prediction is that there will be no standards in the catalog. If that is the course we take, we will stop progress.
• In looking at EISA language, “as may be necessary”, I would recommend that FERC looks at where it is really necessary to adopt standards.
  • I would suggest that requesting information about how the utilities plan to use the standards (as suggested by Kevin Kelly) would be helpful.
The Future?

- NIST standards roadmap is at a crossroads
- Arnold: “We want a mechanism that would allow us to move forward, with the private sector leading the effort, as opposed to the government.”
- “One can’t expect the government to fund [the effort] at such a high level forever.”
The Future?

- Comments on the FERC Technical Conference and the testimony is due March 2, 2011
- Reply comments are due March 16, 2011
- We don’t expect FERC to require use of one technology over another
- FERC may look to SGIP catalog of standards
- Testing and certification process will be key for interoperability
Questions?
Appendix
Additional Reference Sources

NISTIR 7628

Security Profile for AMI

Use Cases Repositories
http://www.sgiclearninghouse.org/UseCases