
Smart Grid Standards Ready for Consideration by Regulators

George W. Arnold, Eng.Sc.D.
National Coordinator for Smart Grid Interoperability
National Institute of Standards and Technology
U.S. Department of Commerce



NIST Process for Identifying Initial Smart Grid Standards

NIST SG Standards Workshops – April to August, 2009

- Identifies interoperable SG standards and issues
- NIST Posts list of 16 consensus standards for public comment
- Charters Priority Action Plan (PAP) working groups to address standards issues
- EPRI delivers Interim Smart Grid Framework and Roadmap Report to NIST
- Two Federal Register Notices soliciting public comments

NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0

- Draft document posted for public comment, September, 2009
- Final Release 1.0 published January, 2010

- Includes list of *guiding principles* for identifying SG standards
- 25 SG standards identified
- 50 standards listed for further review
- no cyber security analysis

SGIP

- Established in November, 2009 to continue the evolution of the Smart Grid standards framework and roadmap
- Cyber Security Working Group
 - publishes NISTIR 7628 on requirements for the Smart Grid, August, 2010
 - Cyber security review of NISTIR 7628 requirements completed for 5 standards, October, 2010

Letter from NIST to FERC, October 2010

- Five standards identified as ready for consideration by regulators
- Narratives containing information important to regulators posted

Five Families of Standards Sent to FERC

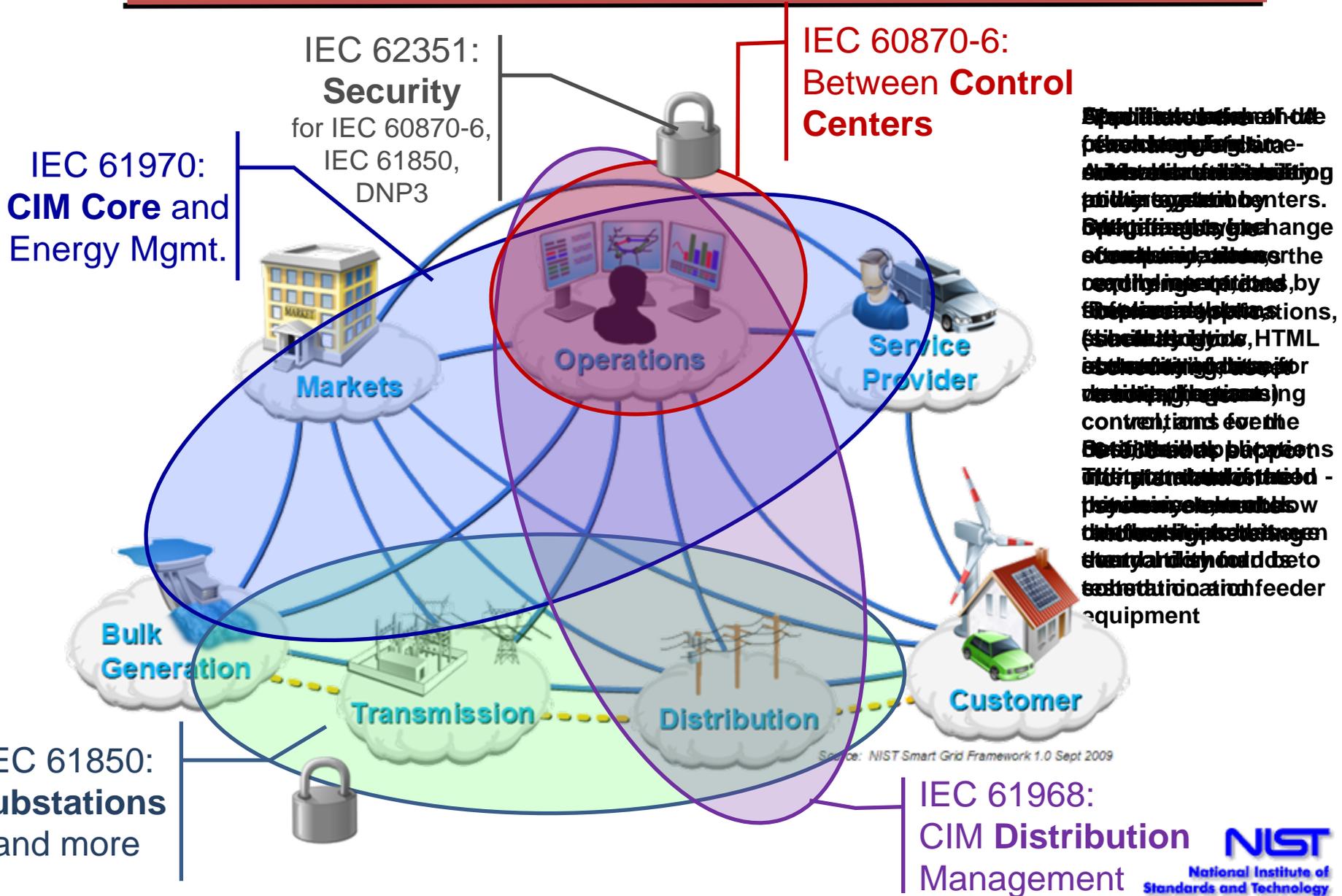
- IEC 61970 and IEC 61968:** Providing a Common Information Model (CIM) necessary for exchanges of data between devices and networks, primarily in the transmission (IEC 61970) and distribution (IEC 61968) domains.
- IEC 61850:** Facilitating substation automation and communication as well as interoperability through a common data format.
- IEC 60870-6:** Facilitating exchanges of information between control centers.
- IEC 62351:** Addressing the cyber security of the communication protocols defined by the preceding IEC standards.

General Benefits of the Five

These standards have the following general benefits for all stakeholders:

- **Reduce Cost:** Enables interoperability of Smart Grid technologies and future choices for companies that choose to install any particular type of technology independent of vendor.
- **Streamline Processes:** Permits the integration of equipment and systems for controlling the electric power process into complete system solutions, necessary to support utilities' processes.
- **Risk Management:** Achieve cyber security objectives through digital signatures, authenticated access, preventing eavesdropping, playback and spoofing, and intrusion detection.
- **Vendor Lock-in:** Significantly reduces if not eliminates the vendor lock-in problem historically experienced in utility systems that use vendor specific proprietary information exchange technologies

Conceptual Model and the "First Five"



Specialized software for the
 production of the
 data and information
 for the system centers.
 Data is exchanged
 between the
 operations centers,
 by the use of
 applications,
 (such as XML,
 HTML,
 etc.) for
 exchanging
 information
 between the
 operations
 centers and the
 production
 equipment.
 The operations
 centers are
 responsible for
 the control of
 the system
 and the
 production
 equipment.



Why Should Regulators Care?

With these standards, utility customers benefit because you can:

- Integrate new systems with much less effort
- Create vendor competition, minimize/eliminate vendor lock-in
- Enable innovation
- Drive down costs
- Ensure uniformity throughout the grid
- Build in security

It is important to understand that the standards are not static.

They continue to be maintained and updated to reflect evolving technology and requirements – a normal part of the standards process.

What Does “Adoption” Mean?

- Purely voluntary
 - Many standards that are already in widespread use in the market may not need any regulatory action
- Encourage
 - Some standards may need “help” to accelerate market adoption
 - There are a number of ways regulators can encourage the use of standards without mandating them
- Mandate
 - Some standards that are critical to grid safety, reliability or security may need to be mandated

Considering Standards – Why?

- Each of the standards needs to be reviewed to determine relevance to state jurisdiction
- What does it mean to my state?
 - Do they enable an existing or envisioned policy to be cost effectively implemented?
 - Will/could/should this standard impact previous, current, or future proceedings or rulemakings such as those related to approved or pending utility smart grid projects?
- What can I do as a State Regulatory Agency?
 - Analyze all existing dockets for applicability
 - Analyze against core policy objectives for applicability
 - Develop guidelines for when/how utilities should consider them
 - Mandate specific standards be considered in certain situations
 - “Score” utility project proposals based on use of standards

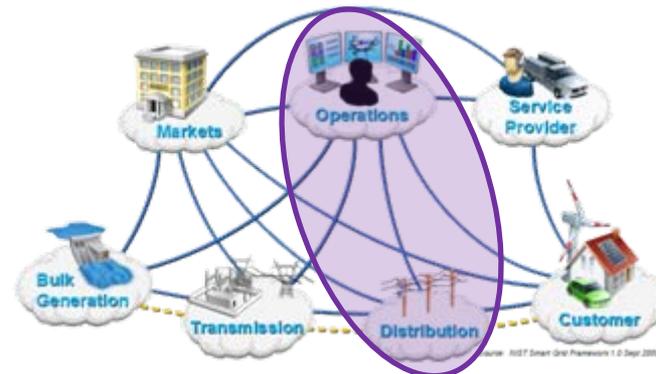
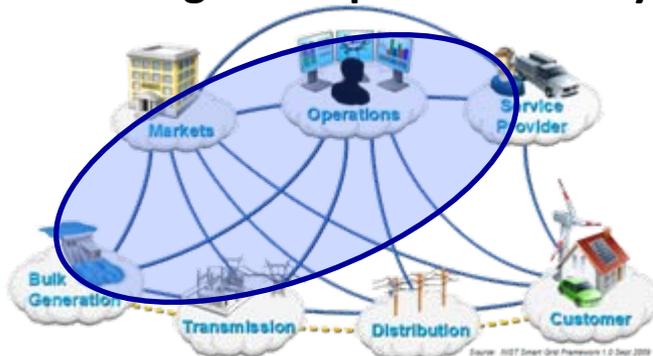
Questions?

Detail Slides

In Plain Language

#1+2 IEC 61970/61968 - the Common Information Model Standard (CIM) – Core Methods/Transmission + Distribution/Metering

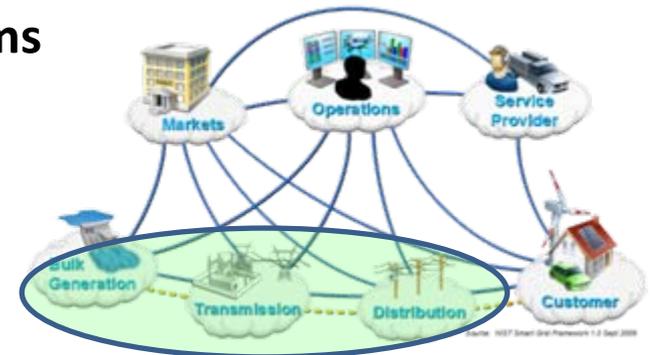
- Foundational - provides basic methods of describing power system components in a structured manner readily interpreted by software systems (similar to how HTML is the foundation for web applications)
- Describes the components of a power system and the relationships between them
- Facilitates the exchange of data between utilities
- Within a single company, allows the exchange of data between applications, such as work scheduling, asset tracking, etc.
- Example: 1) Planning group sends characteristics of new transmission line to operations - CIM describes what line will look like physically and electrically. 2) Allows data to move from multiple vendor metering system access points and head ends through multiple software systems into the billing system.



In Plain Language

#3 IEC 61850 - The Substation Automation Standard

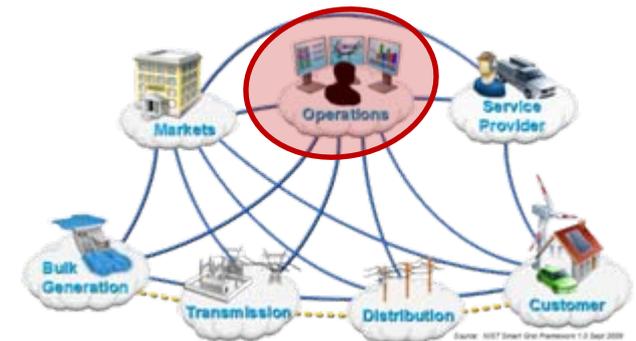
- **This is a standardized framework for substation automation and integration**
 - Specifies the communications requirements, functional characteristics, structure of data in devices, the naming conventions for the data, how applications interact and control the devices, and how conformity to the standard should be tested.
 - Key attributes are ease of multi-vendor integration, low installation costs, faster and more accurate system configuration
 - Standard names for standard things – common language for station devices
 - Results in fewer errors, more capability and flexibility than previous standards
 - Implements modern networking technology in the substation
- **Example: Facilitates unambiguous exchange of information between multiple vendor equipment and systems**



In Plain Language

#4 IEC 60870-6: Inter-Control Center Protocol Standard

- The standard specifies the method of exchanging ISO-compliant time-critical data between control centers at utilities.
 - Includes the exchange of real-time data indications, control operations, time-series data, scheduling and accounting information, remote program control, and event notification.
 - The standard is used between control centers in almost every utility for communication.
 - Benefits are measured in terms of reliability and interoperability.
- **Example: Transmission line failure reported to multiple utilities in multiple jurisdictions in real time.**



In Plain Language

#5 IEC 62351 Parts 1-7 The Cyber Security Standard

- **Applies to each of the other standards.**
 - Adds more reliability to the system by mitigating cyber attacks
 - Replaces the “security by obscurity” concept used in the past
- **Example: Secures link between utility and substation - minimizes chances that hacker can issue control commands to substation and feeder equipment**
- **Security objectives include**
 - Authentication of entities through digital signatures
 - Ensuring only authorized access
 - Prevention of eavesdropping, playback and spoofing
 - Provides some degree of intrusion detection.

