NIST Special Publication 1108

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

Office of the National Coordinator for Smart Grid Interoperability

National Institute of Standards and Technology • U.S. Department of Commerce

NIST Special Publication 1108

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

Office of the National Coordinator for Smart Grid Interoperability

January 2010

U.S. Department of Commerce
Gary Locke, Secretary

National Institute of Standards and Technology
Patrick D. Gallagher, Director

Table of Contents

DISCLAIMER

This document has been prepared by the National Institute of Standards and Technology (NIST) and describes standards research in support of its mandate under the Energy Independence and Security Act of 2007 (EISA).

Certain commercial entities, equipment, or material may be identified in this document in order to describe a concept adequately. Such identification is not intended to imply recommendation or endorsement by the National Institute of Standards and Technology, nor is it intended to imply that these entities, materials, or equipment are necessarily the best available for the purpose.

Executive Summary

Background

Under the Energy Independence and Security Act of 2007 (EISA), the National Institute of Standards and Technology (NIST) is assigned the "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…" [EISA Title XIII, Section 1305]. There is an urgent need to establish protocols and standards for the Smart Grid. Deployment of various Smart Grid elements, including smart sensors on distribution lines, smart meters in homes, and widely dispersed sources of renewable energy, is already underway and will be accelerated as a result of Department of Energy (DOE) Smart Grid Investment Grants and other incentives, such as loan guarantees for renewable energy generation projects. Without standards, there is the potential for technologies developed or implemented with sizable public and private investments to become obsolete prematurely or to be implemented without measures necessary to ensure security.

EISA, which designates development of a Smart Grid as a national policy goal, specifies that the interoperability framework should be "flexible, uniform, and technology neutral." The law also instructs that the framework should accommodate "traditional, centralized generation and distribution resources" while also facilitating incorporation of new, innovative Smart Grid technologies, such as distributed renewable energy resources and energy storage.

Recognizing the urgency, NIST developed a three-phase plan to accelerate the identification of an initial set of standards and to establish a robust framework for the sustaining development of the many additional standards that will be needed and for setting up a conformity testing and certification infrastructure. In May 2009, U.S. Secretary of Commerce Gary Locke and U.S. Secretary of Energy Steven Chu chaired a meeting of nearly 70 executives from the power, information technology, and other industries at which these executives expressed their organizations' commitment to support the plan established by NIST to meet its EISA responsibility. Over the past year, these organizational commitments have been realized with the active participation of the broad Smart Grid community to support the NIST plan.

This document, *NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0*, is the output of the first phase of the NIST plan. It describes a high-level conceptual reference model for the Smart Grid, identifies 75 existing standards that are applicable (or likely to be applicable) to the ongoing development of the Smart Grid, specifies 15 high-priority gaps and harmonization issues (in addition to cyber security) for which new or revised standards and requirements are needed, documents action plans with aggressive timelines by which designated standards-setting organizations (SSOs) will address these gaps, and describes the strategy to establish requirements and standards to help ensure Smart Grid cyber security.

This document was drafted through an open public process that engaged the broad spectrum of Smart Grid stakeholder communities and the general public. Input was provided through three public workshops, in April, May and August 2009, in which more than 1,500 individuals representing hundreds of organizations participated. NIST also consulted with stakeholders through extensive outreach efforts carried out by the Office of the National Coordinator for Smart Grid Interoperability. A draft of this report underwent a 30-day public review and

comment period, which ended on November 9, 2009. All comments received were considered during the preparation of this report.

Summary of Key Elements Included in the Report

Smart Grid Conceptual Reference Model

The Smart Grid is a complex system of systems for which a common understanding of its major building blocks and how they interrelate must be broadly shared. NIST has developed a conceptual architectural reference model presented in this document to facilitate this shared view. This model provides a means to analyze use cases, identify interfaces for which interoperability standards are needed, and to facilitate development of a cyber security strategy. The NIST Smart Grid Conceptual Reference Model, as described in Chapter 3, identifies seven domains: bulk generation, transmission, distribution, markets, operations, service provider, and customer. The model identifies interfaces among domains and actors. It also includes applications requiring exchanges of information, for which interoperability standards are needed. The Smart Grid Conceptual Reference Model described in this report will be further developed under the auspices of the Smart Grid Architecture Committee, a standing committee of the Smart Grid Interoperability Panel, which was established on November 16, 2009, to provide an open process for stakeholders to participate in providing input and cooperating with NIST in the ongoing coordination, acceleration and harmonization of standards development for the Smart Grid.

Priorities for Standardization

The Smart Grid will ultimately require hundreds of standards, specifications, and requirements. Some are needed more urgently than others. To prioritize its work, NIST chose to focus initially on standards needed to address the priorities identified in the Federal Energy Regulatory Commission (FERC) Policy Statement,[1] plus additional areas identified by NIST. The eight priority areas are:

- Demand Response and Consumer Energy Efficiency
- Wide-Area Situational Awareness
- Energy Storage
- Electric Transportation
- Advanced Metering Infrastructure
- Distribution Grid Management
- Cyber Security
- Network Communications

[1] Federal Energy Regulatory Commission, *Smart Grid Policy*, 128 FERC ¶ 61,060 [Docket No. PL09-4-000] July 16, 2009.

Standards Identified for Implementation

On the basis of stakeholder input and NIST's technical judgment, this initial release of the NIST Smart Grid Framework and Roadmap identifies 75 standards, specifications, or guidelines that are immediately applicable (or likely to be applicable) to the ongoing transformation to the Smart Grid. In this report, the total is divided into two sets. The first set of 25 standards, specifications, and guidelines is the product of three rounds of review and comment. The set of 50 additional standards was compiled on the basis of stakeholder inputs received during the second and third rounds of review and comment. Some of the standards in the two sets are mature, others require revisions to accommodate Smart Grid applications and requirements, and still others are in the draft stage and not yet publicly available. As part of the Priority Action Plans devised during the first phase of the NIST plan for Smart Grid interoperability, candidate standards requiring revisions and draft standards still in development are undergoing further review and consensus development. Collectively, these 75 standards represent a small subset of the totality of standards that ultimately will be required to build a safe, secure Smart Grid that is interoperable, end to end.

NIST developed criteria to help guide the evaluation of Smart Grid interoperability standards. Not all of the criteria could be applied to each standard identified in this report. Therefore, decisions were based on a cumulative assessment that considered all of the applicable criteria.

As a general rule, however, NIST believes that Smart Grid interoperability standards should be *open*. This means that *the standards should be developed and maintained through a collaborative, consensus-driven process that is open to participation by all relevant and materially affected parties and not dominated by, or under the control of, a single organization or group of organizations. As important, the standards resulting from this process should be readily and reasonably available to all for Smart Grid applications*. In addition, Smart Grid interoperability standards should be developed and implemented internationally, whenever practical.

For the purpose of this document, it should be noted that NIST is using the term standards (or specifications)-setting organization (SSO) to represent the broad universe of organizations and groups – formal or informal – that develop standards, specifications, user requirements, guidelines, and the like. Included under the SSO umbrella, for example, are standards-developing organizations that develop standards through an accredited process.

Priority Action Plans

Through the NIST workshops, NIST determined that many potentially useful standards will require revision or enhancement before they can be implemented to address Smart Grid requirements. In addition, stakeholders identified gaps requiring entirely new standards to be developed. In all, a total of 70 such gaps or related issues were identified. Of these, NIST selected 15 for which resolution is most urgently needed to support one or more of the Smart Grid priority areas.[2] For each, an action plan has been developed. These Priority Action Plans specify organizations that have agreed to accomplish defined tasks with specified deliverables.

[2] An additional priority action plan was conceived, but was placed on hold in order to focus on the other plans identified. See Section 5.2 Standard Meter Data Profiles (PAP 05) for more information.

For each, aggressive milestones were established (some completed in 2009, and the others expected to be completed during 2010). One action plan has already been completed and substantive progress has been made in meeting the milestones of others. The Priority Action Plans and targets for completion are:

- Smart meter upgradeability standard (completed)
- Common specification for price and product definition (early 2010)
- Common scheduling mechanism for energy transactions (early 2010)
- Common information model for distribution grid management (year-end 2010)
- Standard demand response signals (early 2010)
- Standards for energy use information (mid 2010)
- DNP3 Mapping to IEC 61850 Objects (2010)[3]
- Harmonization of IEEE C37.118 with IEC 61850 and precision time synchronization (mid 2010)
- Transmission and distribution power systems models mapping (year-end 2010)
- Guidelines for use of IP protocol suite in the Smart Grid (mid 2010)
- Guidelines for use of wireless communications in the Smart Grid (mid 2010)
- Energy storage interconnection guidelines (mid 2010)
- Interoperability standards to support plug-in electric vehicles (year-end 2010)
- Standard meter data profiles (year-end 2010)
- Harmonize power line carrier standards for appliance communications in the home (year-end 2010)

Cyber Security

Ensuring cyber security of the Smart Grid is a critical priority. Achieving this goal requires incorporating security at the architectural level. A NIST-led Cyber Security Coordination Task Group consisting of almost 300 participants from the private and public sectors is leading the development of a cyber security strategy and cyber security requirements for the Smart Grid. The task group is identifying use cases with cyber security considerations; assessing risks, vulnerabilities, threats and impacts; performing a privacy impact assessment; assessing relevant standards; specifying research and development topics; developing a security architecture linked to the Smart Grid conceptual reference model; and documenting and tailoring security requirements to provide adequate protection. Results of the task group's work to date are summarized in this document and included in a companion Smart Grid document entitled: *DRAFT NISTIR 7628 Smart Grid Cyber Security Strategy and Requirements*, issued on September 25, 2009. This draft underwent a period of public review, ending December 1, 2009. A subsequent draft that incorporates comments and includes new task-group outputs will be published in early 2010. This cyber security document will also undergo public review and comment.

[3] All acronyms are defined in the Appendix.

Next Steps

The reference model, standards, gaps and action plans described in this document provide an initial foundation for a secure, interoperable Smart Grid. These outputs are the results of consensus, achieved through participatory workshops and webinars, formal public reviews of draft documents and a preliminary list of standards, and extensive NIST outreach activities. These efforts mobilized the diverse community of Smart Grid stakeholders, and launched and expedited standardization efforts now spanning more than 20 standards-setting organizations.

Under EISA, the Federal Energy Regulatory Commission (FERC) is charged with instituting rulemaking proceedings, and once sufficient consensus is achieved, adopting the standards and protocols necessary to ensure Smart Grid functionality and interoperability in interstate transmission of electric power and in regional and wholesale electricity markets. Not all of the standards listed in this initial framework are ready or necessary for adoption by regulators at this time. Some of the individual standards listed require specified revisions or developments within formal standards-setting organizations. Additionally, some foundational standards and specifications listed are already in wide use by industry on a voluntary basis and, thus, regulatory adoption may not be necessary. NIST intends to coordinate the development of additional technical information on individual standards and specifications to support their evaluation and potential use for regulatory purposes.

The second phase of the NIST plan was formally launched in November 2009. It involves an ongoing organization and consensus process that is being formalized under the newly formed Smart Grid Interoperability Panel (SGIP). The SGIP is a public-private partnership that provides a more permanent organizational structure to support the continuing evolution of the framework. By mid-December 2009, one month after it was established, the SGIP membership exceeded 400 organizations divided among 22 stakeholder categories.

The objective of the NIST plan, moving forward, is to create a robust, ongoing, "built-in" standards process[4] that supports cycle after cycle of Smart Grid innovation and helps to transform our economy. The resulting process could lead to new collaborative methods and vehicles for developing and deploying standards in technology-based markets, especially during the early phases when standards—or the lack of standards—can strongly influence the course of further technology development and diffusion and the growth and competitiveness of industries.

Although the product of federal legislation, the collaborative standardization process that NIST and Smart Grid stakeholders are building must interface effectively with all states and territories and their regulatory agencies. Many states and their utility commissions are pursuing Smart Grid-related projects. For example, most states have set renewable portfolio standards that set goals for the percentage of electric power supplied by wind, solar, and other renewable energy sources. Ultimately, states and local projects will converge into fully functioning elements of the Smart Grid "system of systems." The interoperability and cyber security standards developed under the NIST framework and roadmap should also support the role of the states in modernizing the nation's electric grid.

[4] As part of this process, the SGIP will help to prioritize and coordinate Smart Grid-related standards. See Section 7.1 for further discussion.

A robust framework for conformity testing and certification of Smart Grid devices and systems will be established as the third phase of NIST's three-phase plan to ensure interoperability and cyber security. In recognition of the importance of testing and certification, the SGIP contains a permanent testing and certification committee. With the SGIP and its governing board, NIST has initiated planning for such a framework in consultation with stakeholders, and it will initiate implementation steps in 2010.

1 Purpose and Scope

1.1 Overview and Background

Under the Energy Independence and Security Act (EISA) of 2007, the National Institute of Standards and Technology (NIST) is assigned "*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…"* [EISA Title XIII, Section 1305][5]

There is an urgent need to establish Smart Grid standards and protocols. Some Smart Grid[6] devices, such as smart meters, are moving beyond the pilot stage into large-scale deployment. Installation of synchrophasors—sensors that provide real-time

NIST Plan for Interoperability Standards

To carry out its EISA-assigned responsibilities, NIST devised a three-phase plan to rapidly identify an initial set of standards, while providing a robust process for continued development and implementation of standards as needs and opportunities arise and as technology advances.

- **Engage stakeholders in a participatory public process to identify applicable standards and requirements, and gaps in currently available standards, and priorities for additional standardization activities.** With the support of outside technical experts working under contract, NIST has compiled and incorporated stakeholder inputs from three public workshops, as well as technical contributions from technical working groups and a cyber security coordination task group, into the NIST-coordinated standards-roadmapping effort.
- **Establish a Smart Grid Interoperability Panel forum to drive longer-term progress.** A representative, reliable, and responsive organizational forum is needed to sustain continued development of interoperability standards. On November 19, 2009, a Smart Grid Interoperability Panel was launched to serve this function.
- **Develop and implement a framework for conformity testing and certification.** Testing and certification of how standards are implemented in Smart Grid devices, systems, and processes are essential to ensure interoperability and security under realistic operating conditions. NIST, in consultation with stakeholders, plans to develop an overall framework for testing and certification, with initial steps completed by early 2010.

[5] DOE is the lead federal agency with responsibility for sponsoring cost-shared Smart Grid investment grants, demonstration projects, and other R&D efforts. The Federal Energy Regulatory Commission (FERC) is tasked with initiating rulemakings for adoption of Smart Grid standards when it determines that the standards identified in the NIST framework development efforts have sufficient consensus. See Title XIII, Section 1305 of the Energy Independence and Security Act of 2007.

[6] While recognizing that the different names used for the future grid have meaningful distinctions to some stakeholders, this report generally uses the term "Smart Grid." The capitalized version of the term is used in Title XIII of the Energy Independence and Security Act of 2007. NIST recognizes that lower-case versions of the term also appear in the act. The decision to use Smart Grid is not intended to discount or supersede other terms used to describe a modernized grid that enables bidirectional flows of energy and uses two-way communication and control capabilities that will lead to an array of new functionalities and applications.

assessments of power system health to provide system operators with better information for averting disastrous outages—has accelerated rapidly. By 2013, nearly 900 of these devices will monitor conditions on the power grid, a more than fivefold increase since January 2009. [7]

In late October 2009, President Obama announced 100 Smart Grid Investment Grant Program awards totaling $3.4 billion. This federal investment leveraged an additional $4.7 billion in commitments from private companies, utilities, cities, and other partners that are forging ahead with plans to install Smart Grid technologies and enable an array of efficiency-maximizing and performance-optimizing applications. At the end of 2009, the number of Smart Grid projects in the United States exceeded 130 projects spread across 44 states and two territories.[8]

Federal loan guarantees for commercial renewable energy generation projects,[9] growing venture capital investments in Smart Grid technologies, and other incentives and investments provide additional impetus to accelerate the nationwide transition to the Smart Grid. However, given that investments are ongoing and ramping up rapidly, standards adopted or developed in support of this transition must fully reckon with the need for backward compatibility with deployed technologies.

A recent forecast projects that the U.S. market for Smart Grid-related equipment, devices, information and communication technologies, and other hardware, software, and services will double between 2009 and 2014—to nearly $43 billion. Over the same span, the global market is projected to grow to more than $171 billion, an increase of almost 150 percent.[10]

In the absence of standards, there is a risk that the diverse Smart Grid technologies that are the objects of these mounting investments will become prematurely obsolete or, worse, be implemented without adequate security measures. Lack of standards may also impede future innovation and the realization of promising applications, such as smart appliances that are responsive to price and demand response signals.

Moreover, standards enable economies of scale and scope that help to create competitive markets in which vendors compete on the basis of a combination of price and quality. Market competition promotes faster diffusion of Smart Grid technologies and realization of customer benefits. A recent national survey indicates that most U.S. consumers are favorably disposed toward anticipated household-level benefits made possible by Smart Grid technologies and capabilities. Three-fourths of those surveyed said they are "likely to change their energy use in

[7] Vice President Biden, Memorandum for the President, "Progress Report: The Transformation to a Clean Energy Economy," Dec. 15, 2009. See http://www.whitehouse.gov/administration/vice-president-biden/reports/progress-report-transformation-clean-energy-economy.

[8] On World, "Smart Grid Projects in 90 Percent of U.S. States," Nov. 4, 2009.

[9] U.S. Department of Energy, "Energy Department Announces New Private Sector Partnership to Accelerate Renewable Energy Projects," Oct. 7, 2009.

[10] Zpryme, "Smart Grid: United States and Global Hardware and Software Companies Should Prepare to Capitalize on This Technology," Dec. 14, 2009.

order to save money on their utility bills if they were given new technology solutions." A similar percentage said they "*would like their utility to help them reduce energy consumption*."[11]

In early 2009, recognizing the importance and urgency of modernizing the nation's electric power infrastructure, NIST intensified efforts to accelerate progress in identifying and actively coordinating the development of interoperability standards that will underpin the performance, capabilities, and benefits of the Smart Grid. In May 2009, U.S. Secretary of Commerce Gary Locke and U.S. Secretary of Energy Steven Chu chaired a meeting of nearly 70 executives from the power, information technology, and other industries at which they expressed their organizations' commitment to support NIST's plan. Over the past year, these organizational commitments have been realized with the active participation of the broad Smart Grid community to support the NIST plan.

This report, *NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0,* is an output of NIST's approach to expediting development of key standards and requirements that will enable the networked devices and systems that make up the envisioned Smart Grid to communicate and work with each other. It is the first official output of NIST's three-phase plan to accelerate development and implementation of key standards essential to progress toward realizing the Smart Grid vision.

The majority of the document presents the first steps of a Smart Grid interoperability framework based upon initial standards and priorities to *achieve interoperability of Smart Grid devices and systems.*

It contains:

- a conceptual reference model to facilitate design of an architecture for the Smart Grid overall and for its networked domains;
- an initial set of 75 identified standards for the Smart Grid;
- priorities for additional standards and revisions to existing standards necessary to resolve important gaps and to assure the interoperability, reliability, and security of Smart Grid components;
- initial steps toward a Smart Grid cyber security strategy and requirements document using a high-level risk assessment process; and
- action plans with aggressive timelines by which designated standards-setting organizations (SSOs) with expertise in Smart Grid domains or technology areas will address identified gaps.

This document is the first installment in an ongoing standards and harmonization process. Ultimately, this process will deliver the hundreds of communication protocols, standard

[11] TechNet, "New Poll Finds Wide Majority of Americans Support New Technologies for Smart Grid and Improved Home Energy Management," Dec. 21, 2009.

interfaces, and other widely accepted and adopted technical specifications necessary to build an advanced, secure electric power grid with two-way communication and control capabilities. It will serve to guide the work of the Smart Grid Interoperability Panel (SGIP) that was established on November 19, 2009, as part of the NIST three-phase approach to achieving end-to-end interoperability, while ensuring the safety, reliability, and security of the grid. The membership of the SGIP, consisting of organizations in 22 Smart Grid stakeholder categories, will provide an open process for stakeholders to participate in providing input and cooperating with NIST in the ongoing coordination, acceleration and harmonization of standards development for the Smart Grid, beginning with but extending well beyond Release 1.0.

In conjunction with and integral to this process, NIST is coordinating the development of a Smart Grid cyber security framework and strategy, which involves almost 300 technical experts. Results of the task group's work to date are included in a companion Smart Grid document entitled: *DRAFT NISTIR 7628 Smart Grid Cyber Security Strategy and Requirements*, issued on Sept. 25, 2009. The next draft of this document is due in early 2010, and will undergo public review and comment. The final Smart Grid cyber security framework and strategy will be completed in collaboration with the SGIP and its Cyber Security Working Group, with the final version anticipated to be published in the spring of 2010.

The results of NIST's ongoing work on standards for the Smart Grid provides input to FERC, which under EISA is charged with instituting, once sufficient consensus is achieved, rulemaking proceedings to adopt the standards and protocols necessary to ensure Smart Grid functionality and interoperability in interstate transmission of electric power and in regional and wholesale electricity markets.

1.2 How This Report Was Produced

This section describes the steps that NIST undertook to engage diverse stakeholders in the identification of the first set of applicable Smart Grid standards as well as initial priorities for developing new standards that address gaps identified in public workshops and through NIST outreach to stakeholders and formal public reviews of draft versions of this document.

This report distills insights, analyses, and recommendations from members of the general public, proffered during stakeholder-engagement workshops that have involved over 1,500 people and four rounds of public review formally announced in *Federal Register* notices. Participants at three workshops (April 28-29, 2009; May 19-20, 2009; August 3-4, 2009) represented a broad range of technical expertise and a diversity of stakeholder perspectives, including power transmission and distribution, information and communications technology, renewable energy, electric transportation, energy storage, smart buildings, state and federal regulators, and consumers. Significant portions of these workshops were devoted to developing use cases and generating requirements to be addressed by interoperability standards. Use cases are a systems engineering tool for defining a system's behavior from the perspective of users. In effect, a use case is a story told in structure and detailed steps—scenarios for specifying required usages of a system, including how a component, subsystem, or system should respond to a request that originates elsewhere.

In addition, NIST drew on the technical contributions of domain expert working groups (DEWGs) that it established in 2008 in partnership with DOE's GridWise Architecture Council

(GWAC) to provide an open, regular means of collaboration among technical experts interested in furthering the goal of Smart Grid interoperability.[12] Involving more than 400 people representing 100 different organizations, the DEWGs engaged in technical activities such as developing domain-specific requirements for Smart Grid functionality and interoperability and identifying cyber security risks and vulnerabilities.

Also, in April 2009, NIST awarded a contract to the Electric Power Research Institute (EPRI), a private, nonprofit research organization to facilitate the April and May stakeholder workshops. Subsequent to the April workshop, NIST identified a preliminary set of standards and specifications for inclusion in the *NIST Framework and Roadmap for Smart Grid Interoperability Standards, Draft Release 1.0.* When the list was announced, NIST stressed its preliminary nature. "Existing standards that do not appear in this first installment to Release 1.0 have not been eliminated from consideration," NIST advised on its Smart Grid Web site. "Moreover, standards currently on the list ultimately may not be included."[13]

The initial list was reviewed at the May 19-20, 2009, stakeholders' workshop, where additional standards were identified as candidates for inclusion in *Release 1.0.* In addition, NIST submitted the preliminary list for public review and comment, June 9 to July 9, 2009, as announced in the *Federal Register*.[14]

Following the workshops, EPRI—using its technical expertise— compiled, distilled, organized, and refined stakeholder contributions, integrated the results with previously prepared information, and produced a *Report to NIST on the Smart Grid Interoperability Standards Roadmap.*[15] Delivered to NIST in mid-June 2009, the report identified issues and proposed priorities for developing interoperability standards and conceptual reference models for a U.S. Smart Grid. The report listed more than 80 existing standards that might be applied or adapted to Smart Grid interoperability or cyber security needs and identified more than 70 standardization gaps and issues.

The EPRI-prepared document was made available for public review and comment.[16] NIST consulted the report and evaluated the comments received as it drafted this standards roadmap. A key intermediate NIST output was a distillation of priorities that, in addition to the long-standing, cross-cutting requirement for cyber security, NIST proposed for immediate, focused action by standards-setting organizations (SSOs) and stakeholder groups. A formalized Smart Grid standards Priority Action Plan (PAP) approach was developed to define the problem, establish the objectives, and identify the likely standards bodies and users associations pertinent

---

[12] Organized by Smart Grid domains, the six DEWGs are: transmission and distribution, building to grid, industry to grid, home to grid, business and policy, and a cross-cutting cyber security coordination task group. An additional working group on electric-vehicle-to-grid issues has recently been initiated.

[13] 74 FR 27288 (June 9, 2009).

[14] Ibid.

[15] *Report to NIST on the Smart Grid Interoperability Standards Roadmap* (Contract No. SB1341-09-CN-0031—Deliverable 7) Prepared by the Electric Power Research Institute (EPRI), June 17, 2009. Available at: http://www.nist.gov/smartgrid/Report%20to%20NISTlAugust10%20%282%29.pdf

[16] 74 FR 31254 (June 30, 2009).

to the standards modifications, enhancements, and harmonization required. This fast-tracking PAP approach was applied to the initial top priorities and has been instituted as part of the SGIP structure to support the continued evolution of the framework.

The initial PAPs and the status of cyber security efforts were reviewed and further developed at a public workshop, held on August 3 and 4, 2009. With representatives of more than 20 standards organizations among the participants, the workshop was devoted to discussing individual SSO and stakeholder perspectives on the evolving roadmap for Smart Grid interoperability standards, reaching agreement on which organizations should resolve specific standards needs, and developing plans and timelines for meeting these responsibilities as described in the PAPs. Progress on the PAPs and cyber security are summarized in Chapters 5 and 6 of this document, respectively.

On September 24, 2009, U.S. Commerce Secretary Gary Locke announced the availability of the draft version of this report, *NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0 (Draft)* and the *DRAFT NISTIR 7628 Smart Grid Cyber Security Strategy and Requirements*. In his remarks, Secretary Locke invited public review of both documents. Subsequently, NIST solicited public review and comment on both drafts through *Federal Register* notices.[17] Individuals from more than 80 organizations submitted approximately 400 comments on the NIST framework and roadmap document. All of these comments were reviewed by NIST, and responses were incorporated into this document when appropriate. [18] However, not all comments were relevant to the scope of the framework and roadmap.

1.3 Key Concepts

Although it makes up only one aspect of the transformation to a Smart Grid infrastructure, the expedited development of an interoperability framework and a roadmap for underpinning standards is fundamentally important.

Technical contributions from numerous stakeholder communities will be required to realize an interoperable, secure Smart Grid. Because of the diversity of technical and industrial perspectives involved, most participants in the roadmapping effort are familiar with only subsets of Smart Grid-related standards. Few have detailed knowledge of all pertinent standards, even in their own industrial and technical area.

This report contributes to an increased understanding of standards-related priorities, strengths and weaknesses of individual standards, the level of effective interoperability among different Smart-Grid domains, and cyber security requirements that are critical to realization of the Smart Grid.

[17] 74 FR 52181 (October 9, 2009) for Release 1.0 and 74 FR 52183 (October 9, 2009).

[18] NIST's responses will be posted at: http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/IKBFramework

1.3.1 Definitions

Several important terms appear throughout the roadmap. Definitions of some may vary among stakeholders. To facilitate clear stakeholder discourse, NIST used the following definitions for the key terms below:

Architecture: The conceptual structure and overall organization of the Smart Grid from the point of view of its use or design. This includes technical and business designs, demonstrations, implementations, and standards that, together, convey a common understanding of the Smart Grid. The architecture embodies high-level principles and requirements that designs of Smart Grid applications and systems must satisfy.[19]

Harmonization: The process of achieving technical equivalency and enabling interchangeability between different standards with overlapping functionality. Harmonization requires an architecture that documents key points of interoperability and associated interfaces.

Interoperability: The capability of two or more networks, systems, devices, applications, or components to exchange and readily use information—securely, effectively, and with little or no inconvenience to the user.[20] The Smart Grid will be a system of interoperable systems. That is, different systems will be able to exchange meaningful, actionable information. The systems will share a common meaning of the exchanged information, and this information will elicit agreed-upon types of response. The reliability, fidelity, and security of information exchanges between and among Smart Grid systems must achieve requisite performance levels.[21]

Interchangeability: An extreme degree of interoperability characterized by a similarity sometimes termed "plug and play." Interchangeable components can be freely substituted without loss of function and requiring minimum to no additional configuration.

Reference Model: A set of views (diagrams) and descriptions that are the basis for discussing the characteristics, uses, behavior, interfaces, requirements, and standards of the Smart Grid. This model does not represent the final architecture of the Smart Grid; rather it is a tool for describing, discussing, and developing that architecture.

Requirement: 1) A condition or capability needed by a user to solve a problem or achieve an objective. 2) A condition or capability that must be met or possessed by a system or system

---

[19] Pacific Northwest National Laboratory, U.S. Department of Energy. *Gridwise™ Architecture Tenets and Illustrations*, PNNL-SA-39480 October 2003.

[20] Recovery Act Financial Assistance, Funding Opportunity Announcement. U. S. Department of Energy, Office of Electricity Delivery and Energy Reliability, Smart Grid Investment Grant Program Funding Opportunity Number: DE-FOA-0000058.

[21] GridWise Architecture Council, *Interoperability Path Forward Whitepaper*, November 30, 2005 (v1.0).

component to satisfy a contract, standard, specification, or other formally imposed documents.[22]

Standards: Specifications that establish the fitness of a product for a particular use or that define the function and performance of a device or system. Standards are key facilitators of compatibility and interoperability. They define specifications for languages, communication protocols, data formats, linkages within and across systems, interfaces between software applications and between hardware devices, and much more. Standards must be robust so that they can be extended to accommodate future applications and technologies. An assortment of organizations develops voluntary standards and specifications, which are the results of processes that vary on the basis of the type of standards setting-organization and its purpose. Government regulations may incorporate or reference voluntary standards.

Additional terms pertinent to cyber security and to other important security-related considerations relevant to the safety, reliability, and overall performance of the Smart Grid and its components are defined in the *DRAFT NISTIR 7628 Smart Grid Cyber Security Strategy and Requirements*.

1.3.2 Applications and Requirements: Eight Priority Areas

The Smart Grid will ultimately require hundreds of standards. Some are more urgently needed than others. To prioritize its work, NIST chose to focus on six key functionalities plus cyber security and network communications, aspects that are especially critical to ongoing and near-term deployments of Smart Grid technologies and services, including priority applications were recommended by FERC in its policy statement:[23]

- **Wide-area situational awareness:** Monitoring and display of power-system components and performance across interconnections and over large geographic areas in near real time. The goals of situational awareness are to understand and ultimately optimize the management of power-network components, behavior, and performance, as well as to anticipate, prevent, or respond to problems before disruptions can arise.

- **Demand response and consumer energy efficiency:** Mechanisms and incentives for utilities, business, industrial, and residential customers to cut energy use during times of peak demand or when power reliability is at risk. Demand response is necessary for optimizing the balance of power supply and demand.

- **Energy storage:** Means of storing energy, directly or indirectly. The significant bulk energy storage technology available today is pumped hydroelectric storage technology. New storage capabilities—especially for distributed storage—would benefit the entire grid, from generation to end use.

[22] IEEE Std 610.12

[23] Federal Energy Regulatory Commission, *Smart Grid Policy*, 128 FERC ¶ 61,060 [Docket No. PL09-4-000] July 16, 2009.

- **Electric transportation:** Refers, primarily, to enabling large-scale integration of plug-in electric vehicles (PEVs). Electric transportation could significantly reduce U.S. dependence on foreign oil, increase use of renewable sources of energy, and dramatically reduce the nation's carbon footprint.

- **Cyber security:** Encompasses measures to ensure the confidentiality, integrity and availability of the electronic information communication systems and the control systems necessary for the management, operation, and protection of the Smart Grid's energy, information technology, and telecommunications infrastructures.

- **Network communications:** The Smart Grid domains and subdomains will use a variety of public and private communication networks, both wired and wireless. Given this variety of networking environments, the identification of performance metrics and core operational requirements of different applications, actors, and domains—in addition to the development, implementation, and maintenance of appropriate security and access controls—is critical to the Smart Grid.

- **Advanced metering infrastructure (AMI):** Currently, utilities are focusing on developing AMI to implement residential demand response and to serve as the chief mechanism for implementing dynamic pricing. It consists of the communications hardware and software and associated system and data management software that creates a two-way network between advanced meters and utility business systems, enabling collection and distribution of information to customers and other parties, such as the competitive retail supplier or the utility itself. AMI provides customers real-time (or near real-time) pricing of electricity, and it can help utilities achieve necessary load reductions.

- **Distribution grid management:** Focuses on maximizing performance of feeders, transformers, and other components of networked distribution systems and integrating with transmission systems and customer operations. As Smart Grid capabilities, such as AMI and demand response, are developed, and as large numbers of distributed energy resources and plug-in electric vehicles (PEVs) are deployed, the automation of distribution systems becomes increasingly more important to the efficient and reliable operation of the overall power system. The anticipated benefits of distribution grid management include increased reliability, reductions in peak loads, and improved capabilities for managing distributed sources of renewable energy.

1.4 Content Overview

Chapter 2, "Smart Grid Vision," provides a high-level description of the envisioned Smart Grid and describes major organizational drivers, opportunities, challenges, and anticipated benefits.

Chapter 3, **"**Conceptual Reference Model," presents a set of views (diagrams) and descriptions that are the basis for discussing the characteristics, uses, behavior, interfaces, requirements, and standards of the Smart Grid. Since the Smart Grid is an evolving networked system of systems, the high-level model is a tool for developing the more detailed, formal Smart Grid architectures.

Chapter 4, "Standards Identified for Implementation," presents and describes existing standards and emerging specifications applicable to the Smart Grid. It includes descriptions of proposed selection criteria, a general overview of the standards identified by stakeholders in the NIST-coordinated process, and a discussion of their relevance to Smart Grid interoperability requirements.

Chapter 5 describes 16 "Priority Action Plans," to address standard-related gaps and issues for which resolution is most urgently needed to support one or more of the Smart Grid priority areas. For each, an action plan has been developed, specific organizations tasked, and aggressive milestones in 2009 or early 2010 established. One—a plan to develop a smart meter upgradeability standard—already has been completed. The full set of detailed priority action plans, which are works in progress undergoing continuing development and refinement, can be reviewed on-line at the NIST Smart Grid Collaboration Web site.[24]

Chapter 6, "Cyber Security Risk Management Framework and Strategy," reviews the criticality of cyber security to the Smart Grid, and describes how this overriding priority is being addressed.

In Chapter 7, "Next Steps," the report concludes with a discussion of the establishment of the Smart Grid Interoperability Panel to assist NIST to sustain expedited development of standards and continuing evolution of the framework, plans to establish a conformance testing and certification infrastructure, and additional issues impacting standardization efforts and progress toward realizing a safe, secure, innovation-enabling Smart Grid.

[24] http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/WebHome

2 Smart Grid Vision

2.1 Overview

In the United States and many other countries, modernization of the electric power grid is central to national efforts to increase energy efficiency, transition to renewable sources of energy, reduce greenhouse gas emissions, and build a sustainable economy that ensures prosperity for current and future generations. Around the world, billions of dollars are being spent to build elements of what ultimately will be "smart" electric power grids.

Definitions and terminology vary somewhat, but whether called "Smart," "smart," "smarter," or even "supersmart," all notions of an advanced power grid for the 21st century hinge on adding and integrating many varieties of digital computing and communication technologies and services with the power-delivery infrastructure. Bidirectional flows of energy and two-way communication and control capabilities will enable an array of new functionalities and applications that go well beyond "smart" meters for homes and businesses. The Energy Independence and Security Act (EISA) of 2007, which directed NIST to coordinate development of this framework and roadmap, states that support for creation of a Smart Grid is the national policy. Distinguishing characteristics of the Smart Grid cited in the act include:[25]

- Increased use of digital information and controls technology to improve reliability, security, and efficiency of the electric grid;
- Dynamic optimization of grid operations and resources, with full cyber security;
- Deployment and integration of distributed resources and generation, including renewable resources;
- Development and incorporation of demand response, demand-side resources, and energy-efficiency resources;
- Deployment of ''smart'' technologies for metering, communications concerning grid operations and status, and distribution automation;
- Integration of ''smart'' appliances and consumer devices;
- Deployment and integration of advanced electricity storage and peak-shaving technologies, including plug-in electric and hybrid electric vehicles, and thermal-storage air conditioning;
- Provision to consumers of timely information and control options;
- Development of standards for communication and interoperability of appliances and equipment connected to the electric grid, including the infrastructure serving the grid; and
- Identification and lowering of unreasonable or unnecessary barriers to adoption of Smart Grid technologies, practices, and services.

The U.S. Department of Energy (DOE), which leads the overall federal Smart Grid effort, summarized the anticipated advantages enabled by the Smart Grid in its June 25, 2009, funding opportunity announcement. The DOE statement explicitly recognizes the important enabling role of an underpinning standards infrastructure:

[25] Energy Independence and Security Act of 2007 [Public Law No: 110-140] Title XIII, Sec. 1301.

> The application of advanced digital technologies (i.e., microprocessor-based measurement and control, communications, computing, and information systems) are expected to greatly improve the reliability, security, interoperability, and efficiency of the electric grid, while reducing environmental impacts and promoting economic growth. Achieving enhanced connectivity and interoperability will require innovation, ingenuity, and different applications, systems, and devices to operate seamlessly with one another, involving the combined use of open system architecture, as an integration platform, and commonly-shared technical standards and protocols for communications and information systems. To realize Smart Grid capabilities, deployments must integrate a vast number of smart devices and systems**.** [26]

To monitor and assess progress of deployments in the United States, DOE is tracking activities grouped under six chief characteristics of the envisioned Smart Grid:[27]

- Enables informed participation by customers;
- Accommodates all generation and storage options;
- Enables new products, services, and markets;
- Provides the power quality for the range of needs;
- Optimizes asset utilization and operating efficiently; and
- Operates resiliently to disturbances, attacks, and natural disasters.

Interoperability and cyber security standards identified under the NIST-coordinated process in cooperation with DOE will underpin component, system-level, and network-wide performance in each of these six important areas.

The framework described in EISA lists several important characteristics. These include[28]:

- that the framework be "flexible, uniform and technology neutral, including but not limited to technologies for managing smart grid information;"
- that it "accommodate traditional, centralized generation and transmission resources and consumer distributed resources;"
- that it be "flexible to incorporate regional and organizational differences; and technological innovations;"
- that it "consider the use of voluntary uniform standards for certain classes of mass-produced electric appliances and equipment for homes and businesses that enable customers, at their election and consistent with applicable State and Federal laws, and are manufactured with the ability to respond to electric grid emergencies and demand response signals;" and that "such voluntary standards should incorporate appropriate manufacturer lead time."

[26] U. S. Department of Energy, Office of Electricity Delivery and Energy Reliability**,** Recovery Act Financial Assistance Funding Opportunity Announcement, Smart Grid Investment Grant Program, DE-FOA-0000058, June 25, 2009.

[27] U.S. Department of Energy, *Smart Grid System Report*, July 2009.

[28] Quotes in the bulleted list are from the Energy Independence and Security Act of 2007 [Public Law No: 110-140] Title XIII, Sec. 1305.

2.2 Importance to National Energy Policy Goals

The Smart Grid is a vital component of President Obama's comprehensive energy plan, which aims to reduce U.S. dependence on foreign oil, to create jobs, and to help U.S. industry compete successfully in global markets for clean energy technology. The President has set ambitious short- and long-term goals, necessitating quick action and sustained progress in implementing the components, systems, and networks that will make up the Smart Grid. For example, the President's energy policies are intended to double renewable energy generating capacity to 10 percent by 2012[29]—an increase in capacity that is enough to power 6 million American homes. By 2025, renewable energy sources are expected to account for 25 percent of the nation's electric power consumption.

The American Recovery and Reinvestment Act (ARRA) of 2009 included $11 billion for smart grid technologies, transmission system expansion and upgrades, and other investments to modernize and enhance the electric transmission infrastructure to improve energy efficiency and reliability.[30] These investments and associated actions to modernize the nation's electricity grid ultimately will result, for example, in more than 3,000 miles of new or modernized transmission lines and 40 million "smart meters" in American homes, [31]as well as almost 700 automated substations and more than 850 sensors (phasor measurement units) that will cover 100 percent of the electric grid, which will enable operators to detect minor disturbances and prevent them from cascading into local or regional power outages or blackouts[32]. In addition, progress toward realization of the Smart Grid will contribute to accomplishing the President's goal of putting one million plug-in hybrid vehicles on the road by 2015.[33] A DOE study found that the idle capacity of today's electric power grid could supply 70 percent of the energy needs of today's cars and light trucks without adding to generation or transmission capacity—*if the vehicles charged during off-peak times.*[34]

---

[29] Vice-President Biden, Memorandum for the President, "Progress Report: The Transformation to a Clean Energy Economy," December 15, 2009. See http://www.whitehouse.gov/administration/vice-president-biden/reports/progress-report-transformation-clean-energy-economy.

[30] The White House, "American Recovery and Reinvestment Act: Moving America Toward a Clean Energy Future." Feb. 17, 2009. See: http://www.whitehouse.gov/assets/documents/Recovery_Act_Energy_2-17.pdf.

[31] Ibid.

[32] The White House, Office of the Press Secretary, "President Obama Announces $3.4 Billion Investment to Spur Transition to Smart Energy Grid," Oct. 27, 2009. See: http://www.whitehouse.gov/the-press-office/president-obama-announces-34-billion-investment-spur-transition-smart-energy-grid.

[33] The White House, Office of the Press Secretary, "President Obama Announces $2.4 Billion in Funding to Support Next Generation Electric Vehicles." March 19, 2009.

[34] M. Kintner-Meyer, K. Schneider, and R. Pratt, "Impacts Assessment of Plug-in Hybrid Vehicles on Electric Utilities and Regional U.S. Power Grids." Part 1: Technical Analysis. Pacific Northwest National Laboratory, U.S. Department of Energy, 2006.

Anticipated Smart Grid Benefits

- Improves power reliability and quality
- Optimizes facility utilization and averts construction of back-up (peak load) power plants
- Enhances capacity and efficiency of existing electric power networks
- Improves resilience to disruption
- Enables predictive maintenance and "self-healing" responses to system disturbances
- Facilitates expanded deployment of renewable energy sources
- Accommodates distributed power sources
- Automates maintenance and operation
- Reduces greenhouse gas emissions by enabling electric vehicles and new power sources
- Reduces oil consumption by reducing the need for inefficient generation during peak usage periods
- Presents opportunities to improve grid security
- Enables transition to plug-in electric vehicles and new energy storage options
- Increases consumer choice

Over the long term, the integration of the power grid with the nation's transportation system has the potential to yield huge energy savings and other important benefits. Estimates of associated potential benefits[35] include:

- Displacement of about half of our nation's net oil imports;
- Reduction in U.S. carbon dioxide emissions by about 25 percent; and
- Reductions in emissions of urban air pollutants of 40 percent to 90 percent.

While the transition to the Smart Grid may unfold over many years, incremental progress along the way can yield significant benefits (see box on left). In the United States, electric-power generation accounts for about 40 percent of human-caused emissions of carbon dioxide, the primary greenhouse gas.[36] The Electric Power Research Institute has estimated that, by 2030, Smart Grid-enabled (or facilitated) applications—from distribution voltage control to broader integration of intermittent renewable resources to electric transportation vehicles—could reduce the nation's carbon-dioxide emissions (60 to 211) million metric tons annually.[37] The opportunities are many and the returns can be sizable. If the current power grid were just 5 percent more efficient, the resultant energy savings would be equivalent to permanently eliminating the fuel consumption and greenhouse gas emissions from 53 million cars.[38]

---

[35] Ibid.

[36] Energy Information Administration, U.S. Department of Energy, "U.S. Carbon Dioxide Emissions from Energy Sources, 2008 *Flash* Estimate." May 2009.

[37] Electric Power Research Institute, *The Green Grid: Energy Savings and Carbon Emissions Reductions Enabled by a Smart Grid*, 1016905 Technical Update, June 2008.

[38] U.S. Department of Energy, *The Smart Grid: an Introduction*, 2008. See http://www.oe.energy.gov/SmartGridIntroduction.htm .

In its National Assessment of Demand Response Potential, FERC estimated the potential for peak electricity demand reductions to be equivalent to up to 20 percent of national peak demand—enough to eliminate the need to operate hundreds of backup power plants.[39]

ants, 2009

Category	$ Million
Integrated/Crosscutting	2,150
AMI	818
Distribution	254
Transmission	148
Customer Systems	32
Manufacturing	26
Total	3,429

18 million smart meters
1.2 million in-home display units
206,000 smart transformers
177,000 load control devices
170,000 smart thermostats
877 networked phasor measurement units
671 automated substations
100 PEV charging stations

Geographic Coverage of Selected Projects

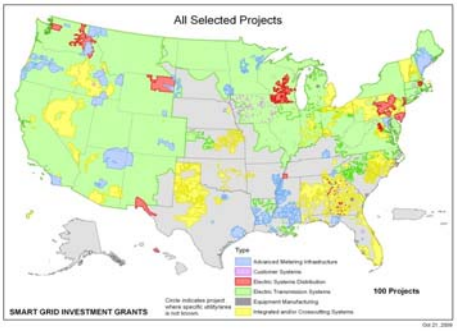


Figure 2-1 Department of Energy Smart Grid Investment Grants, 2009. [40]

President Obama has called for a national effort to reduce, by 2020, the nation's greenhouse gas emissions to 14 percent below the 2005 level and to about 83 percent below the 2005 level by 2050.[41] Reaching these targets will require an ever more capable Smart Grid with end-to-end interoperability.

The transition to the Smart Grid already is under way, and it is gaining momentum, spurred by ARRA investments. In late October, President Obama announced 100 awards under the Smart Grid Investment Grant Program.[42] Totaling $3.4 billion and attracting an additional $4.7 billion in matching funding, the grants support manufacturing, purchasing, and installation of existing Smart Grid technologies that can be deployed on a commercial scale (Figure 2-1). The DOE required project plans to include descriptions of technical approaches to "addressing interoperability," including a "summary of how the project will support compatibility with

[39] Federal Energy Regulatory Commission, *A National Assessment Of Demand Response Potential*. Staff report prepared by the Brattle Group; Freeman, Sullivan & Co; and Global Energy Partners, LLC, June 2009.

[40] http://www.energy.gov/news2009/8216.htm.

[41] Office of Management and Budget, *A New Era of Responsibility, Renewing America's Promise.* U.S. Government Printing Office, Washington, D.C. 2009.

[42] The White House, "President Obama Announces $3.4 Billion Investment to Spur Transition to Smart Energy Grid," Oct, 27, 2009.

NIST's emerging Smart Grid framework for standards and protocols."[43]

Other significant federal investments include $60 million in ARRA funding, awarded by DOE on December 18, 2009, to "support transmission planning for the country's three interconnection transmission networks."[44] The six awards will support a "collaborative long-term analysis and planning for the Eastern, Western, and Texas electricity interconnections, which will help states, utilities, grid operators, and others prepare for future growth in energy demand, renewable energy sources, and Smart Grid technologies."[45]

2.3 Key Attributes

The Smart Grid effort is unprecedented in its scope and breadth, and thus it will demand significant levels of cooperation to achieve the ultimate vision. Efforts directed toward enabling interoperability among the many diverse components of the evolving Smart Grid must address the following issues and considerations.

2.3.1 Defined Architectures

An architecture models the structure of a system and describes the entities and interactions within the system. A defined architecture helps enable technical and management governance and can be used to direct ongoing development work as well as to guide decision making on how to achieve a functional fit within a system (in this case, the modernized electric power infrastructure). An architecture is also a tool used to help developers and users understand a system.

For the Smart Grid, which like the Internet is a loosely coupled system of systems, a single, all-encompassing architecture is not practical. Rather, the Smart Grid architecture will be a composite of many system and subsystem architectures developed independently or in concert with other systems. This will allow for maximum flexibility during implementation and will simplify interfacing with other systems.

Thus, it is not the intent of this framework to prescribe an architecture with the intent of constraining how the Smart Grid is implemented, but to describe what is being done to help stakeholders understand Smart Grid interoperability needs. The framework describes a conceptual reference model for discussing the characteristics, uses, behavior, and other elements of Smart Grid domains and the relationships among these elements. The model is a tool for identifying the standards and protocols needed to ensure interoperability and cyber security, and defining and developing architectures for systems and subsystems within the Smart Grid.

Ultimately, these architectures must be well-defined, well-documented and robust. Desired attributes of architectures for the Smart Grid include:

---

[43] U.S. Department of Energy, Office of Electricity Delivery and Energy Reliability, Recovery Act Financial Assistance Funding Announcement (DE-FOA-0000058), June 25, 2009.

[44] U.S. Department of Energy, "Secretary Chu Announces Efforts to Strengthen U.S. Electric Transmission Networks,"Dec. 18, 2009. See: http://www.energy.gov/news2009/8408.htm .

[45] Ibid.

- Support a broad range of technology options— both legacy and new. (Architectures should be flexible enough to incorporate evolving technologies. They also must support interfacing with legacy applications and devices in a standard way, avoiding as much additional capital investment and/or customization as possible.)
- Employ well-defined interfaces that are useful across industries and include appropriate security.
- Are developed with modern system-modeling tools and techniques that are used to manage the documentation and complexity of the Smart Grid.
- Architectural elements are appropriate for the applications that reside within the architecture. (The architectures must support development of massively scaled, well-managed, and secure networks with life spans appropriate for the type of associated network, which range from 5 years to 30 years depending on the type of network.)
- Support third-party products that are interoperable and can be integrated into the management and cyber security infrastructures.
- Achieve appropriate balance between top-down and bottom-up approaches to system design. (In other words, the goals and requirements defined in the top organizational layers of the GWAC stack shown in Figure 2-2 need to be implemented using the building blocks available today—or in the near future—as defined in the bottom technical levels of the stack.)
- Are based on proven enterprise architecture, software, and systems design methodologies.

2.3.2 Different Layers of Interoperability

Large, integrated, complex systems require different layers of interoperability, from a plug or wireless connection to compatible processes and procedures for participating in distributed business transactions. In developing the conceptual model described in the next chapter, the high-level categorization approach developed by GWAC was considered.[46]

[46] GridWise Architecture Council, *GridWise Interoperability Context-Setting Framework.* March 2008.

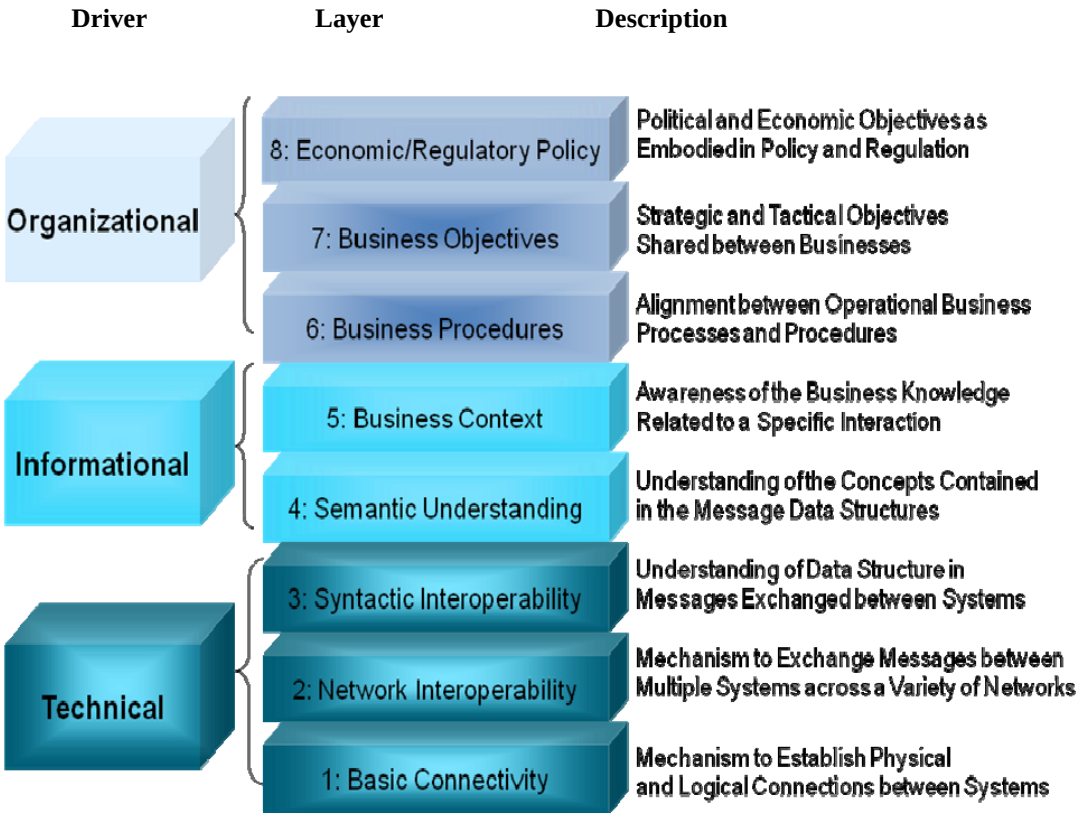


Figure 2-2 The GridWise Architecture Council's eight-layer stack provides a context for determining Smart Grid interoperability requirements and defining exchanges of information**.**

Referred to as the "GWAC stack," the eight layers comprise a vertical cross-section of the degrees of interoperation necessary to enable various interactions and transactions on the Smart Grid. Very simple functionality—such as the physical equipment layer and software for encoding and transmitting data—might be confined to the lowest layers. Communication protocols and applications reside on higher levels with the top levels reserved for business functionality. As functions and capabilities increase in complexity and sophistication, more layers of the GWAC stack are required to interoperate to achieve the desired results. Each layer typically depends upon—and is enabled by—the layers below it.

The most important feature of the GWAC stack is that the layers define well-known interfaces: establishing interoperability at one layer can enable flexibility at other layers. The most obvious example of this is seen in the Internet: with a common Network Interoperability layer, the Basic Connectivity Layer can vary from Ethernet to WiFi to optical and microwave links, but the different networks can exchange information in the same common way.

As shown in Figure 2-2, the eight layers are divided among three "drivers," each requiring a different level of interoperability:

- **Informational:** Emphasizes the semantic aspects of interoperation, focusing on what information is exchanged and its meaning.

- **Informational:** Emphasizes the semantic aspects of interoperation, focusing on what information is exchanged and its meaning.
- **Organizational:** Emphasizes the pragmatic (business and policy) aspects of interoperation, especially those pertaining to the management of electricity.

2.3.3 Standards and Conformance

Standards are critical to enabling interoperable systems and components. Mature, robust standards are the foundation of mass markets for the millions of components that will have a role in the future Smart Grid. Standards enable innovation where components may be constructed by thousands of companies. They also enable consistency in systems management and maintenance over the life cycles of components. Criteria for Smart Grid interoperability standards are discussed further in Chapter 4.

The evidence of the essential role of standards is growing. A recent Congressional Research Service report, for example, cited the ongoing deployment of smart meters as an area in need of widely accepted standards. The U.S. investment in smart meters is predicted to be at least $40 billion to $50 billion over the next several years.[47] Globally, 100 million new smart meters are predicted to be installed over the next five years.[48]

Sound interoperability standards are needed to ensure that sizable public and private sector technology investments are not stranded. Such standards enable diverse systems and their components to work together and to securely exchange meaningful, actionable information.

Clearly, there is a need for concerted action and accelerated efforts to speed the development of high-priority standards. But the standards process must be systematic, not *ad hoc*.

Moreover, while standards are necessary for achieving interoperability, they are not sufficient. A conformance testing and certification regime is essential. NIST, in consultation with industry, government, and other stakeholders, has started work to develop an overall framework for conformance testing and certification and plans to initiate steps toward implementation in 2010.

[47] S. M. Kaplan, *Electric Power Transmission: Background and Policy Issues.* Congressional Research Service, April 14, 2009.

[48] ON World, "100 Million New Smart Meters within the Next Five Years," June 17, 2009. See http://www.onworld.com/html/newssmartmeter.htm.

3 Conceptual Reference Model

3.1 Overview

The conceptual model presented in this chapter supports planning and organization of the diverse, expanding collection of interconnected networks that will compose the Smart Grid. For this purpose, NIST adopted the approach of dividing the Smart Grid into seven domains, as described in Table 3-1 and shown graphically in Figure 3-1.

Each domain—and its sub-domains—encompass Smart Grid *actors* and *applications*. Actors include devices, systems, or programs that make decisions and exchange information necessary for performing applications: smart meters, solar generators, and control systems represent examples of devices and systems. Applications, on the other hand, are tasks performed by one or more actors within a domain. For example, corresponding applications may be home automation, solar energy generation and energy storage, and energy management. The appendix describes the seven Smart Grid domains in more detail. It contains domain-specific diagrams intended to illustrate the type and scope of interactions within and across domains. Figure 3.2 is a composite 'box" diagram that combines attributes of the seven domain-specific diagrams.

Table 3-1. Domains and Actors in the Smart Grid Conceptual Model

Domain	Actors in the Domain
Customers	The end users of electricity. May also generate, store, and manage the use of energy. Traditionally, three customer types are discussed, each with its own domain: residential, commercial, and industrial.
Markets	The operators and participants in electricity markets.
Service Providers	The organizations providing services to electrical customers and utilities.
Operations	The managers of the movement of electricity.
Bulk Generation	The generators of electricity in bulk quantities. May also store energy for later distribution.
Transmission	The carriers of bulk electricity over long distances. May also store and generate electricity.
Distribution	The distributors of electricity to and from customers. May also store and generate electricity.

In general, actors in the same domain have similar objectives. To enable Smart Grid functionality, the actors in a particular domain often interact with actors in other domains, as shown in Figure 3.1. However, communications within the same domain may not necessarily have similar characteristics and requirements. Moreover, particular domains also may contain components of other domains. For instance, the ten Independent System Operators and Regional Transmission Organizations (ISOs/RTOs) in North America have actors in both the Markets and Operations domains. Similarly, a distribution utility is not entirely contained within the

Distribution domain—it is likely to contain actors in the Operations domain, such as a distribution management system, and in the Customer domain, such as meters.

Underlying the conceptual model is a legal and regulatory framework that includes policies and requirements that apply to various actors and applications and to their interactions. Regulations, adopted by the Federal Energy Regulatory Commission at the federal level and by public utility commissions at the state and local levels, govern many aspects of the Smart Grid.

Such regulations are intended to ensure that electric rates are fair and reasonable and that security, reliability, safety, privacy, and other public policy requirements are met.[49] The transition to the Smart Grid introduces new regulatory considerations, which may transcend jurisdictional boundaries and require increased coordination among federal, state, and local lawmakers and regulators. The conceptual model must be consistent with the legal and regulatory framework and support its evolution over time. The standards and protocols identified in the framework also must align with existing and emerging regulatory objectives and responsibilities. The conceptual model is intended to be a useful tool for regulators at all levels to assess how best to achieve public policy goals that, along with business objectives, motivate investments in modernizing the nation's electric power infrastructure and building a clean energy economy.

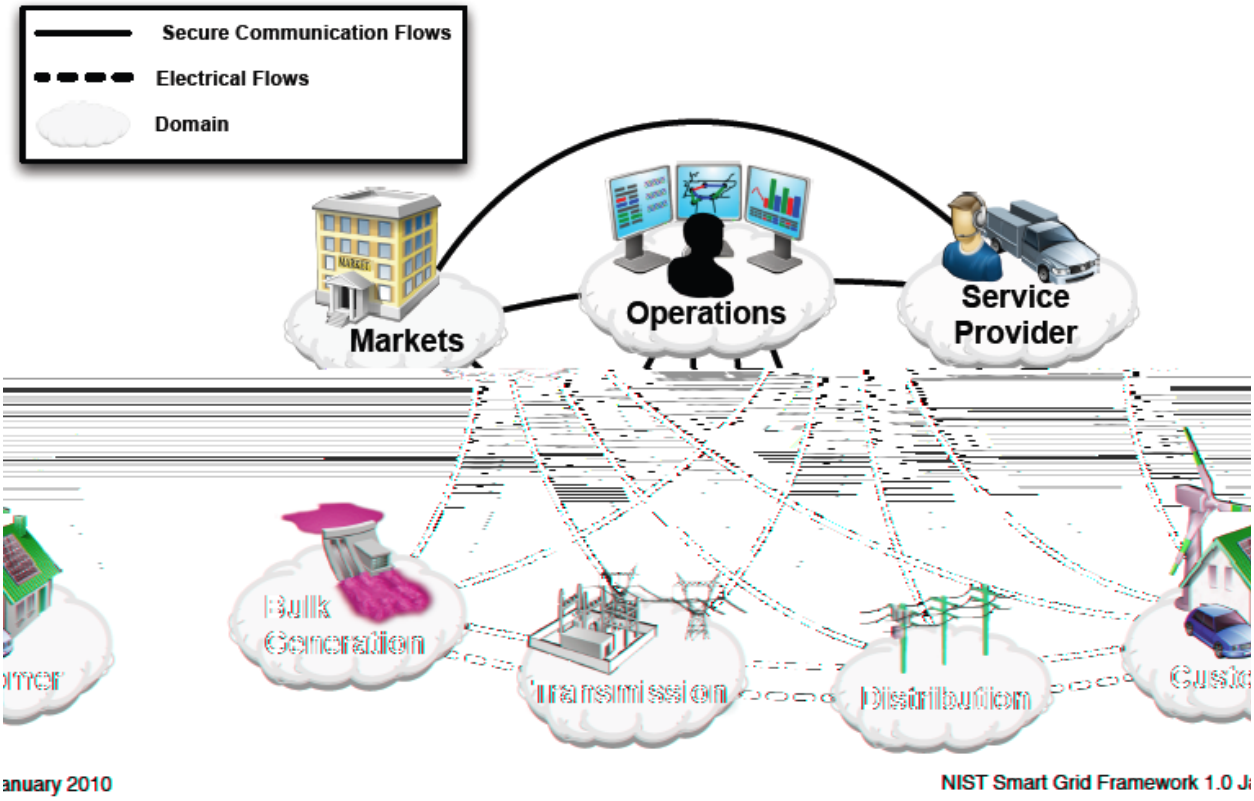


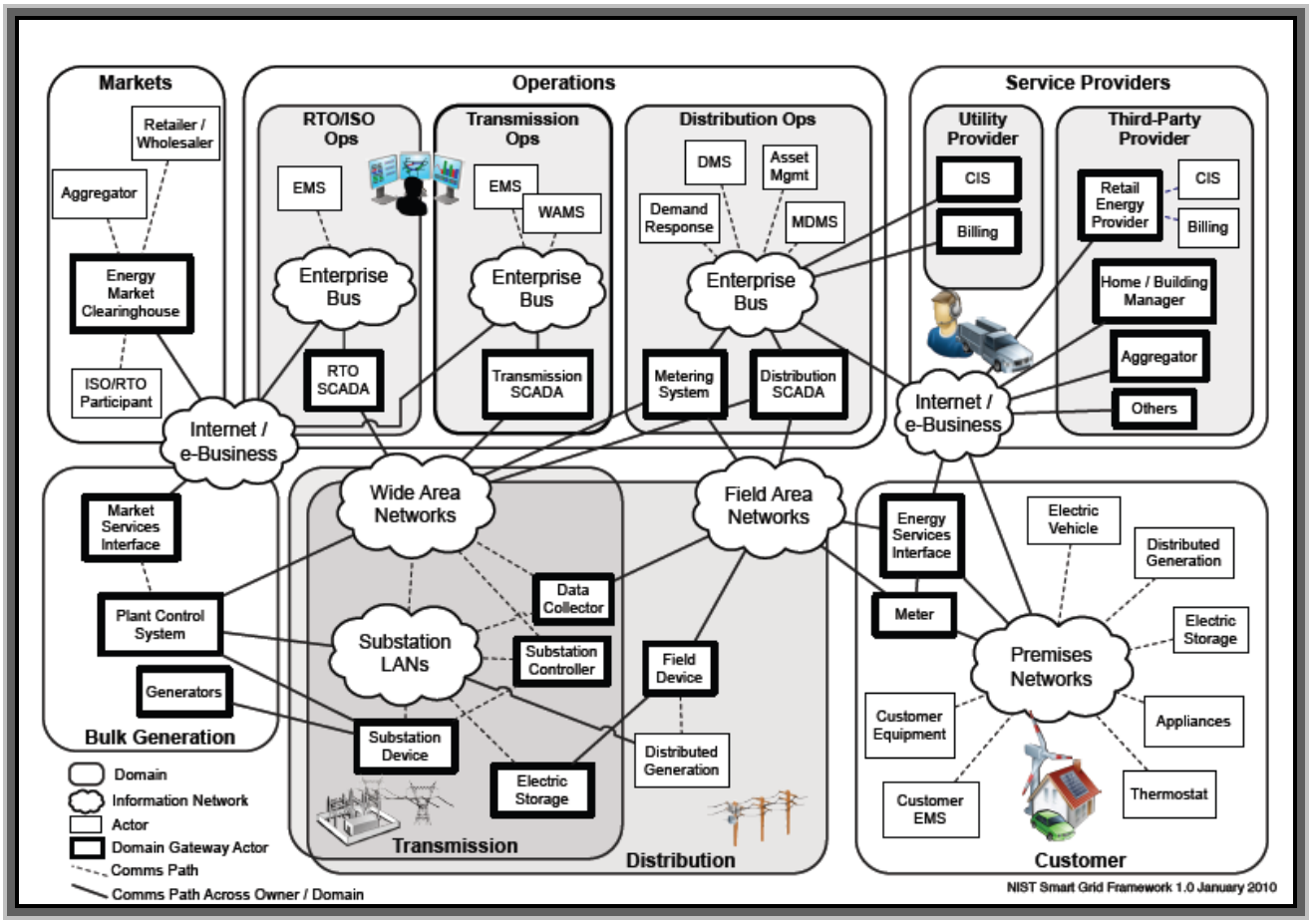
Figure 3-1 Interaction of actors in different Smart Grid Domains through Secure Communication Flows and Electrical Flows.

[49] See, for example, the mission statements of NARUC (http://www.naruc.org/about.cfm) and FERC (http://www.ferc.gov/about/about.asp).

3.2 Description of Conceptual Model

The conceptual model described here provides a high-level, overarching perspective. It is not only a tool for identifying actors and possible communications paths in the Smart Grid, but also a useful way for identifying potential intra- and inter-domain interactions and potential applications and capabilities enabled by these interactions. The conceptual model represented in Figure 3-1 and Figure 3-2 is intended to aid in analysis; it is ***not*** a design diagram that defines a solution and its implementation. In other words, the conceptual model is descriptive and not prescriptive. It is meant to foster understanding of Smart Grid operational intricacies but not prescribe how the Smart Grid will be implemented.

Figure 3-2. **Conceptual Reference Diagram for Smart Grid Information Networks.**



Domain: Each of the seven Smart Grid domains (Table 3-1) is a high-level grouping of organizations, buildings, individuals, systems, devices or other *actors* that have similar objectives and that rely on—or participate in—similar types of applications. Communications among actors in the same domain may have similar characteristics and requirements. Domains may contain sub-domains. Moreover, domains have much overlapping functionality, as in the case of the transmission and distribution domains. Transmission and distribution often share networks and, therefore, are represented as overlapping domains.

Actor: An actor is a device, computer system, software program, or the individual or organization that participates in the Smart Grid. Actors have the capability to make decisions and to exchange information with other actors. Organizations may have actors in more than one domain. The actors illustrated here are representative examples but are by no means all of the actors in the Smart Grid. Each actor may exist in several different varieties and may actually contain other actors within them.

Gateway Actor: An actor in one domain that interfaces with actors in other domains or in other networks. Gateway actors may use a variety of communication protocols; therefore, it is possible that one gateway actor may use a different communication protocol than another actor in the same domain, or use multiple protocols simultaneously.

Information Network: An information network is a collection, or aggregation, of interconnected computers, communication devices, and other information and communication technologies. Technologies in a network exchange information and share resources. The Smart Grid consists of many different types of networks, not all of which are shown in the diagram. The networks include: the Enterprise Bus that connects control center applications to markets, generators, and with each other; Wide Area Networks that connect geographically distant sites; Field Area Networks that connect devices, such as Intelligent Electronic Devices (IEDs) that control circuit breakers and transformers; and Premises Networks that include customer networks as well as utility networks within the customer domain. These networks may be implemented using public (e.g., the Internet) and nonpublic networks in combination. Both public and nonpublic networks will require implementation and maintenance of appropriate security and access control to support the Smart Grid. Examples of where communications may go through the public networks include: customer to third-party providers, bulk generators to grid operators, markets to grid operators, and third-party providers to utilities.

Comms (Communications) Path: Shows the logical exchange of data between actors or between actors and networks. Secure communications are not explicitly shown in the figure and are addressed in more detail in Chapter 6.

3.3 Models for Smart Grid Information Networks

Figure 3-2 shows many comunication paths between and within domains. Currently, various functions are supported by independent and, often, dedicated networks. Examples range from enterprise data and business networks, typically built on the IP family of network layer protocols, to supervisory control and data acquisition (SCADA) systems utilizing specialized protocols. However, to fully realize the Smart Grid goals of vastly improving the control and management of power generation, distribution, and consumption, the current state of information network interconnectivity must be improved so that information can flow securely between the various actors in the Smart Grid. The following sections discuss some of the key outstanding issues that need to be addressed in order to support this vision of network interconnectivity across the Smart Grid.

Given that the Smart Grid will not only be a system of systems, but also a network of information networks, a thorough analysis of network and communications requirements for each subnetwork is needed. This analysis should differentiate among the requirements pertinent to different Smart Grid applications, actors, and domains. One component of this analysis is to identify the security constraints and issues associated with each network interface and the impact level (low, moderate, or high) of a security compromise of confidentiality, integrity, and availability. This information is being used by the Smart Grid Cyber Security Coordination Task Group (CSCTG) in the selection and tailoring of security requirements. (See Chapter 6.)

3.3.1 Information Networks

The Smart Grid is a network of many systems and subsystems, as well as a network of networks. That is, many systems with various ownership and management boundaries are interconnected to provide end-to-end services between and among stakeholders as well as between and among intelligent devices.

Figure 3-3 is a high-level vision for the information network for the Smart Grid. The clouds represent the networks handling two-way communications between the network end points of seven different domains (Table 3-1), as represented by rectangular boxes in Figure 3-3. As shown in the innermost clouds in Figure 3-3, each domain is a unique distributed computing environment and may have its own sub-network to meet the special communication requirements for the domain. Within each network, a hierarchical structure consisting of network technologies, such as Home Area Networks, Personal Area Networks, Wireless Access Networks, Local Area Networks, and Wide Area Networks, may be implemented. On the basis of Smart Grid functional requirements, the network should provide the capability to enable an application in a particular domain to communicate with an application in any other domain over the information network, with proper management control as to who and where applications can be interconnected. Security is required to ensure that the confidentiality, integrity, and availability of Smart Grid information, control systems, and related information systems are properly protected.

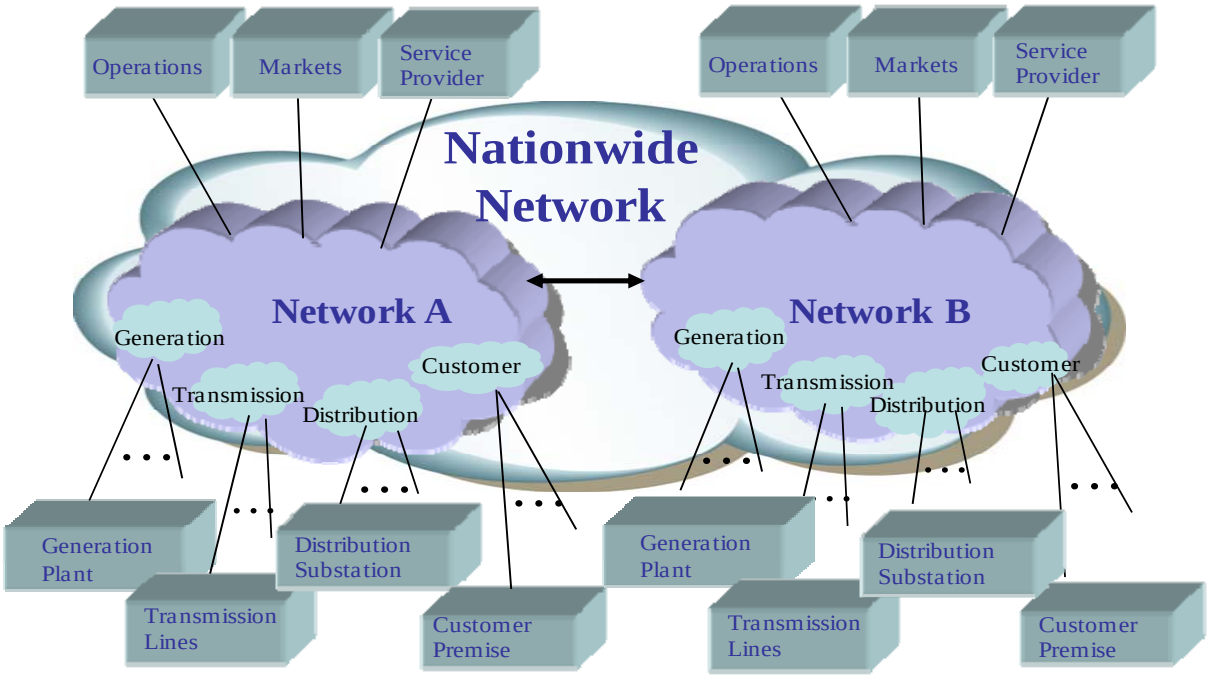


Figure 3-3. Smart Grid Networks for Information Exchange.

Because the Smart Grid will include networks from the diverse information technology, telecommunications, and energy sectors, security is required to ensure that a compromise in one network does not compromise security in other, interconnected systems. A security compromise could impact the availability and reliability of the entire electric grid. In addition, information within each specific system also needs to be protected. Security includes the confidentiality,

integrity, and availability on all related systems. The CSCTG is currently identifying and assessing the Smart Grid logical interfaces to determine the impact of a loss of confidentiality, integrity, or availability. The objective is to select security requirements to mitigate the risk of cascading security breaches.

Devices and applications in each domain are network end points. Examples of applications and devices in the Customer domain include smart meters, appliances, thermostats, energy storage, electric vehicles, and distributed generation. Applications and devices in the Transmission or Distribution domain include phasor measurement units (PMUs) in a transmission line substation, substation controllers, distributed generation, and energy storage. Applications and devices in the Operations domain include SCADA systems and computers or display systems at the operation center. Applications in the Operations, Market, and Service Provider domains are similar to those in Web and business information processing. Thus, their networking function may not be distinguishable from normal information processing networks; therefore, no unique clouds are illustrated.

This information network may consist of multiple interconnected networks, represented by two backbone networks, A and B, in Figure 3-3. Each of these represents the network in the service region of a power utility or service. The physical or logical links within and between these networks, and the links to network end points could utilize any appropriate communication technology currently available or those to be developed and standardized in the future. Note that Figure 3-3 represents a vision for networks supporting Smart Grid control and information exchange.

Additional information network requirements include:

- network management functionality, network activities, and network devices, including status monitoring, fault detection, isolation, and recovery;
- ability to uniquely identify and address elements in the network and devices attached to it;
- routing capability to all network end points; and
- quality-of-service support for a wide range of applications with different bandwidths and different latency and loss requirements.

3.3.2 Security for Smart Grid Information Systems and Control Systems Networks

Because Smart Grid information and controls flow through many networks with various owners, it is critical to properly secure the information and controls, along with the respective networks. This means reducing the risk of intrusion while, at the same time, allowing access for the relevant stakeholders.

Security for the Smart Grid information and control networks must include requirements for:

- security policies, procedures, and protocols to protect Smart Grid information and commands in transit or residing in devices and systems;
- authentication policies, procedures, and protocols; and
- security policies, procedures, protocols, and controls to protect infrastructure components and the interconnected networks.

An overview of the Smart Grid cyber security strategy is included in Chapter 6.

3.3.3 IP-Based Networks

Among Smart Grid stakeholders, there is a wide expectation that Internet Protocol (IP) -based networks will serve as a key element for the Smart Grid information networks. While IP may not address all Smart Grid communications requirements, there are a number of aspects that make it an important Smart Grid technology. Benefits of using IP-based networks include the maturity of a large number of IP standards, the availability of tools and applications that can be applied to Smart Grid environments, and the widespread use of IP technologies in both private and public networks. In addition, IP technologies serve as a bridge between applications and the underlying communication medium. They allow applications to be developed independent of both the communication infrastructure and the various communication technologies to be used, be they wired or wireless.

Furthermore, IP-based networks enable bandwidth sharing among applications and increased reliability with dynamic routing capabilities. For Smart Grid applications that have specific quality-of-service requirements (such as minimum access delay, maximum packet loss or minimum bandwidth constraints), other technologies, such as Multi Protocol Label Switching (MPLS), can be used for the provisioning of dedicated resources.

IP-based network by design is easily scalable; any new Smart Grid devices, such as smart meters, smart home appliances, and data concentrators in neighborhoods, could be added to the network.

As the scale of IP-based network for Smart Grid expands, the numbers of devices connected to the network will increase substantially, as will the number of addresses needed in the IP network to uniquely identify these devices. The fact that the available pool of IPv4 addresses will be exhausted soon should be considered carefully. Even though an alternative addressing scheme in conjunction with translation/mapping into IP addresses might work, we encourage the use of IPv6 for new systems to be developed and deployed. IPv6 was specifically developed to solve the address space issue and to provide enhancements for the IP network.

For each set of Smart Grid requirements, an analysis is necessary to determine whether IP is appropriate and whether cyber security and desired performance characteristics can be assured. For the correct operation of IP networks in Smart Grid environments, a suite of protocols must be identified and developed on the basis of standards defined by the Internet Engineering Task Force (IETF), commonly referred to as Request for Comments (RFCs). The definition of the necessary suite of RFCs will be dictated by the networking requirements yet to be fully determined for Smart Grid applications. Given the heterogeneity and the large number of devices and systems that will be interconnected within the Smart Grid, multiple IP protocol suites may be needed to satisfy a wide range of network requirements. In addition, protocols and guidelines must be developed for the initiation of Smart Grid applications and the establishment and management of Smart Grid connections, in addition to the packetization of Smart Grid application-specific data traffic over IP.

3.3.4 Smart Grid and the Public Internet – Security Concerns

One of the advantages of the Smart Grid is the ability to better manage energy loads and the consumption of energy within many domains. Many of the Smart Grid use cases describe how utilities can work with customers to control and manage home energy consumption. To enable

this functionality, information may flow back and forth between the utility and the customer. The presence of both Smart Grid networks and public Internet connections at the customer site (e.g., within the home) may introduce security concerns that must be addressed. With the customer potentially having access to utility-managed information or information from a third party, safeguards are required to prevent access to the utility control systems that manage power grid operations. These security risks are being assessed by the CSCTG as described in Chapter 6.

3.3.5 Technologies for Standards for Smart Grid Communication Infrastructure

There are a number of mature technologies available to support Smart Grid information networks. Network requirements determined in support of Smart Grid applications will guide the choice of the communication technologies to be used. Standards relevant to physical network infrastructure are too numerous to list and include standards endorsed by the Alliance for Telecommunications Industry Solutions (ATIS), GSM Association (GSMA), the Institute of Electrical and Electronics Engineers Standards Association (IEEE-SA), the Telecommunication Industry Association (TIA), the Third Generation Partnership Project (3GPP), the Third Generation Project 2 (3GPP2), and the IETF.

3.4 Use Case Overview

The conceptual reference model provides a useful tool for constructing use cases. A use case describes the interaction between a Smart Grid actor and a system when the actor is using the system to accomplish a specified goal. Use cases can be classified as “black box” or “white box.” The black box variety describes the user/system interaction and the functional requirements to achieve the goal, but it leaves the details of the inner workings of the system to the implementer. In contrast, white box use cases also describe the internal details of the system, in addition to the interaction and associated requirements, and are therefore prescriptive because they do not allow the implementer to change the internal system design.

For this interoperability standards framework and roadmap, the focus is on the black box use cases that describe how systems within the Smart Grid interact. Because white box use cases describing the details of a particular solution are prescriptive, they are not covered by the framework and are left to the stakeholders to create. The focus on black box use cases will allow maximum innovation in Smart Grid applications while ensuring their ready deployment and interoperability within the Smart Grid as it evolves.

Individually and collectively, these use cases are helpful when scoping out interoperability requirements for specific areas of functionality—such as on-premises energy management or predictive maintenance for grid equipment. When viewed from a variety of stakeholder perspectives and application domains, combining the actors and interactions from multiple use cases permits the Smart Grid to be rendered as a collection of transactional relationships, within and across domains, as illustrated in Figure 3-2.

Many Smart Grid intra- and inter-domain use cases already have been developed, and the number will grow substantially. The scope of the body of existing use cases also cover cross-cutting requirements, including cyber security, network management, data management, and

application integration, as described in the *GridWise Architecture Council Interoperability Context-Setting Framework.*[50]

Developing black box use cases and interface requirements was a major activity at the second NIST Smart Grid interoperability standards public workshop (May 19-20, 2009), which was attended by more than 600 people. This activity was focused on six Smart Grid functionalities: wide-area situational awareness, demand response, energy storage, electric transportation, advanced metering infrastructure, and distribution grid management. The cross-cutting cyber security task group utilized use cases in the priority areas, in addition to those it is developing to supplement the priority area use cases.

The detailed use cases can be found on the NIST Smart Grid Collaboration Web site.[51]

3.5 Smart Grid Interface to the Customer Domain

The interface between the Smart Grid and the customer domain is of special importance. It will be the most visible part of the Smart Grid to the consumer. The conceptual reference model (see Figure 3-2) depicts two distinct elements that, together, provide the interface to the Customer Domain: the Meter and the Energy Services Interface (ESI), which serves as the gateway to the Customer Premises Network. It is through these interfaces that electricity usage is measured, recorded, and communicated; service provisioning and maintenance functions are performed (such as remote connection and disconnection of service); and pricing and demand response signaling occurs. New and innovative energy-related services, which we may not even imagine today, will be developed and may require additional data streams between the Smart Grid and the customer domain. Extensibility and flexibility are important considerations. The interface must be interoperable with a wide variety of energy-using devices and controllers, such as thermostats, water heaters, appliances, consumer electronics, and energy management systems. The diversity of communications technologies and standards used by devices in the customer domain presents a significant challenge to achieving interoperability. In addition, ensuring cyber security is a critical consideration.

3.5.1 Distinction between the Meter and the Energy Services Interface

The meter and the ESI have very different characteristics and functions. The logical separation of the meter and the ESI is a very important forward-looking aspect of the reference model. The meter's essential functions are to measure, record, and communicate energy usage; communicate information for outage management; and enable automated provisioning and maintenance functions, such as connection or disconnection of service. Meters also measure the flow of power into the grid from distributed generation or storage resources located at the customer's premises. Meters have historically been designed with a service life measured in decades, and the cost recovery period set by regulators is at least a decade. Thus, once a meter is installed, it remains there for a very long time as the interface to the electric utility. The meter is owned by the utility and is at the interface between the distribution and customer domains. In the conceptual reference model, it is shown in the customer domain because that is where it physically resides.

[50] http://www.gridwiseac.org/pdfs/interopframework_v1_1.pdf .

[51] http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/IKBUseCases

The ESI serves as the information management gateway through which the customer domain interacts with energy service providers. The service provider may be an electric utility, but that is not necessarily the case. In some states, such as Texas, the market has been restructured so that the service provider is a company entirely separate from the electric utility. Customers have a choice of competing service providers. There also may be third-party service providers that offer demand response aggregation, energy management services, and other such offerings. A telephone company, cable company, or other nontraditional provider might wish to offer their customers energy management services. The standards associated with the ESI need to be flexible and extensible to allow for innovation in market structures and services. Basic functions of the ESI include demand response signaling (for example, communicating price information or critical peak period signals) as well as provision of customer energy usage information to residential energy management systems or in-home displays. However, the possibilities for more advanced services are virtually limitless, so standards associated with the ESI must facilitate rather than impede innovation. The ESI interfaces with the service provider, which, as discussed above, may or may not be the same company as the electric utility.

While the ESI and meter are logically viewed as separate devices, this does not preclude the possibility for manufacturers to implement the meter and ESI in one physical device, provided that the flexibility and extensibility to support the Smart Grid vision can be achieved. Most smart meters currently integrate the ESI and meter functionality in one device due to cost considerations. Looking forward, logical separation of the two functions, even if physically integrated, is essential to avoid having the meter become an impediment to innovation in energy services enabled by the Smart Grid.

3.5.2 The ESI and the Home Area Network

One of the differences between residential environments and commercial/industrial environments is the level of sophistication and customer participation that can be assumed in configuring premises networks to achieve interoperability and security in Smart Grid communications.

Many homes already have one or more data networks that interconnect computers or consumer electronic devices. However, this is not universally the case. Furthermore, even in homes that have data networks, consumers who lack the expertise may not wish to spend time or money configuring an appliance like a clothes dryer to communicate over their home network. It should be possible for consumers to obtain the energy saving benefits of Smart Grid-enabled appliances without requiring that they have a home area network or expertise in configuring data networks. Ideally, a consumer would purchase, for example, a Smart Grid-enabled clothes dryer, plug it in, and register it with their service provider through a Web portal or toll-free phone call. That is all that should be necessary to enable a “smart” appliance to operate on the basis of electricity price information and other demand response signals received from the Smart Grid. To avoid undue expense and complexity for the consumer, the ESI should be able to communicate with Smart Grid-enabled appliances either with or without a separate data network in the home, and such communication should be “plug and play” and “auto-configuring,” requiring no technical expertise.

Another issue that must be addressed is the need for manufacturers of appliances and consumer electronics goods to cost-effectively mass-produce products that will be interoperable with the

Smart Grid anywhere in the country. EISA provides guidance on this issue. Section 1305 of the law advises that the Smart Grid interoperability framework be designed to "consider the use of voluntary uniform standards for certain classes of mass-produced electric appliances and equipment for homes and businesses that enable customers, at their election and consistent with applicable State and Federal laws, and are manufactured with the ability to respond to electric grid emergencies and demand response signals." EISA also advises that "such voluntary standards incorporate appropriate manufacturer lead time."

There are a large number of physical data communication interfaces—wireless and wired—available for use in the home environment, and there will be more in the future. Mass-produced appliances and consumer electronics devices can only support a limited number of interfaces on each device. To minimize costs while maximizing flexibility, the ESI should support, at minimum, a defined subset of widely used standard data communication standards chosen from among those discussed in Section 3.3.5 and listed in Tables 4-1 and 4-2 in Chapter 4. Appliance manufacturers can select from this minimum subset and be assured of interoperability in most environments without the need for separate adapters. Additional interfaces that are less widely used can be supported through adapters.

Many consumers and businesses are located in multiunit buildings. Any data communication interface supported by the ESI should be capable of coexisting with other data communications technologies that may be used in the customer premises without interfering with each other. The use of IP as a network layer protocol for the ESI may provide a cost-effective solution to achieve interoperability between the ESI and appliances and other energy-using devices in the home. Further definition of a minimum set of interfaces to be supported by the ESI will be addressed by the Smart Grid Interoperability Panel in a new Priority Action Plan in early 2010 in order to enable the appliance industry and other industries to offer Smart Grid-compatible products in late 2011, as planned by several manufacturers.

4 Standards Identified for Implementation

4.1 Guiding Principles Used for Identifying Interoperability Standards

The EISA assigns NIST the responsibility to coordinate development of an interoperability framework including model standards and protocols. The identification of the standards and protocol documents that support interoperability of the Smart Grid is therefore a key element of the framework.

There are two lists presented in this chapter. The first, Table 4-1 in Section 4.2, is a list of identified Smart Grid standards and specifications for which NIST believes stakeholder consensus exists. Requirements documents and guidelines are also included in this table. The confidence that there is stakeholder consensus on applicability for Smart Grid for the items in Table 4-1 is based on the outcomes of several workshops, individual stakeholder inputs, NIST Domain Expert Working Group (DEWG) discussions and work products, and public comments solicited on both the standards and this framework document. The second list, Table 4-2 in Section 4.3, contains documents that have or are likely to have applicability to the Smart Grid, subject to further review and consensus development being carried out through plans identified in this roadmap. Again, this conclusion is based upon the comments received from the workshops, stakeholder inputs, and public review. With the establishment of the SGIP and its Governing Board and Architectural Committee, additional mechanisms will be explored to document and where possible increase the level of support for standards and specifications deemed necessary to support the Smart Grid.

There are several guiding principles that led to the two lists of documents presented in this chapter. The major principles that NIST used to select the documents were: 1) they support interoperability of the Smart Grid as it evolves from the existing grid with new utility deployments, Smart Grid programs, and consumer investments in Smart Grid equipment and appliances; and 2) they have a demonstrably high level of consensus support. Since the Smart Grid is evolving from the existing power grid, NIST also included standards that support widely deployed legacy systems. The intent is for Priority Action Plans (PAPs) to be established with the goal of resolving interoperability issues between the standards for legacy equipment and those others identified for the Smart Grid. For example, PAP12 seeks to harmonize the Distribution Network Protocol, DNP3.0, with the IEC 61850 standard (see Section 5.12 and the PAP12 Website, PAP12: DNP3 Mapping to IEC 61850 Objects).

In addition to the major principles, additional nonexclusive guiding principles used in the selection of standards for the framework are given in the inset frames in this section, entitled "Guiding Principles for Identifying Standards for Implementation." NIST used the criteria listed in these inset frames to evaluate standards, specifications, requirements, and guidelines for inclusion in the current version of the *NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0*, and will use them for subsequent versions. This set of criteria is extensive, and the complete list does not apply to each standard, specification, or guideline listed in Tables 4-1 and 4-2. Judgments as to whether each item merits inclusion is made on the basis of combinations of relevant criteria.

The items included in Table 4-1, are in most cases, voluntary consensus standards developed and maintained by accredited Standards Development Organizations (SDOs). The phrases Standards/Specification-Setting Organizations (SSOs) and Standards-Developing Organizations (SDOs) are used loosely and interchangeably within the documentary standards-related literature. However, for the purpose of this document, NIST is using the phrase SSOs to define the broader universe of organizations and groups – formal or informal – that develop standards, specifications, user requirements, guidelines, etc. The term SDOs is used to define standards-developing organizations that develop standards in processes marked by openness, balance, transparency, and characterized by due processes to address negative comments. NIST is using these two terms to address the wide variations in types of organizations that are developing standards, specifications, user guidelines, and other input that is being identified and considered for use in the Smart Grid framework.

Also, in this document, NIST uses the definition of voluntary consensus standards given in OMB Circular A-119, on *Federal Participation in the Development and Use of Voluntary Consensus Standards and in Conformity Assessment Activities*,[52] where such standards are defined as developed and adopted by voluntary consensus standards bodies. In these standards, there are provisions that require that the relevant intellectual property owners have agreed to make that intellectual property available on a nondiscriminatory, royalty-free, or reasonable royalty basis to all interested parties. Voluntary consensus standards bodies are "domestic or international organizations which plan, develop, establish, or coordinate voluntary consensus standards using agreed-upon procedures,"[53] and have the following attributes: 1) openness, 2) balance of interest, 3) due process, 4) a process for appeals, and 5) consensus. Consensus is defined as general agreement, but not necessarily unanimity, and includes a process for attempting to resolve objections by interested parties including the following attributes: all comments are fairly considered, each objector is advised of the disposition of his or her objection(s) and the reasons why, and the consensus body members are given an opportunity to change their votes after reviewing the comments.

As a general rule, however, NIST believes that Smart Grid interoperability standards should be *open*; that is, *developed and maintained through a collaborative, consensus-driven process that is open to participation by all relevant and materially affected parties and not dominated or under the control of a single organization or group of organizations, and readily and reasonably available to all for Smart Grid applications*.[54] In addition, Smart Grid interoperability standards should be developed and implemented internationally, wherever practical.

Because of the massive investment and accelerated timeline for deployment of Smart Grid devices and systems along with the consequent accelerated timetable for standards development and harmonization, NIST did not limit the lists of both identified and candidate standards to

---

[52] OMB Circular A-119, *Federal Participation in the Development and Use of Voluntary Consensus Standards and in Conformity Assessment Activities*, February 10, 1998, http://www.whitehouse.gov/omb/rewrite/circulars/a119/a119.html#5.

[53] Ibid.

[54] *ANSI Essential Requirements: Due process requirements for American National Standards*, Edition: January, 2009, http://www.ansi.org/essentialrequirements/ .

SDO-developed voluntary consensus standards. Rather, Tables 4-1 and 4-2 include specifications, requirements, and guidelines developed by other Standards-Setting Organizations (SSOs). This was done to ensure that the interoperability framework would be established as quickly as possible to support current and imminent deployments of Smart Grid equipment. These SSO documents were developed by user groups, industry alliances, consortia, and other organizations, but ultimately it is envisioned that these specifications and other documents will be used for development of SDO standards.

In making the selections of SSO documents listed in this section, NIST attempted to ensure that documents were consistent with the guiding principles, including that they be open and accessible. This does not mean that all of the standards and specifications are available for free, or that access can be gained to them without joining an organization (including those organizations requiring a fee). It does mean that they will be made available on fair, reasonable, and nondiscriminatory terms and conditions, which may include monetary compensation. To facilitate the development of the Smart Grid and the interoperability framework, NIST is working with SSOs to find ways to make the interoperability documents more accessible so that cost and other factors that may be a barrier to some stakeholders are made less burdensome.

Guiding Principles for Identifying Standards for Implementation

For *Release 1.0,* a standard, specification, or guideline was evaluated on whether it:

- Is well-established and widely acknowledged as important to the Smart Grid.
- Is an open, stable and mature industry-level standards developed in consensus processes from a standards development organization (SDO).
- Enables the transition of the legacy power grid to the Smart Grid.
- Has, or is expected to have, significant implementations, adoption, and use.
- Is supported by an SDO or Users Group to ensure that it is regularly revised and improved to meet changing requirements and that there is strategy for continued relevance.
- Is developed and adopted internationally, wherever practical.
- Is integrated and harmonized, or there is a plan to integrate and harmonize it with complementing standards across the utility enterprise through the use of an industry architecture that documents key points of interoperability and interfaces.
- Enables one or more of the framework characteristics as defined by EISA[*] or enables one or more of the six chief characteristics of the envisioned Smart Grid[†]
- Addresses, or is likely to address, anticipated Smart Grid requirements identified through the NIST workshops and other stakeholder engagement.
- Is applicable to one of the priority areas identified by FERC[‡] and NIST:
    - Demand Response and Consumer Energy Efficiency,
    - Wide Area Situational Awareness,
    - Electric Storage,
    - Electric Transportation,
    - Advanced Metering Infrastructure,
    - Distribution Grid Management.
    - Cyber Security
    - Network Communications

---

[*]Energy Independence and Security Act of 2007 [Public Law No: 110-140] Title XIII, Sec. 1305.

[†] U.S. Department of Energy, Smart Grid System Report, July 2009.

[‡] Federal Energy Regulatory Commission, *Smart Grid Policy*, 128 FERC ¶ 61,060 [Docket No. PL09-4-000] July 16, 2009.

Guiding Principles for Identifying Standards for Implementation (cont'd)

- Focuses on the semantic understanding layer of GWAC stack, which has been identified as most critical to Smart Grid interoperability.
- Is openly available under fair, reasonable, and nondiscriminatory terms.
- Has associated conformance tests or a strategy for achieving them.
- Accommodates legacy implementations.
- Allows for additional functionality and innovation through:
    - *Symmetry* – facilitates bi-directional flows of energy and information.
    - *Transparency* – supports a transparent and auditable chain of transactions.
    - *Composition* – facilitates building of complex interfaces from simpler ones.
    - *Extensibility* – enables adding new functions or modifying existing ones.
    - *Loose coupling* – helps to create a flexible platform that can support valid bilateral and multilateral transactions without elaborate pre-arrangement.*
    - *Layered systems* – separates functions, with each layer providing services to the layer above and receiving services from the layer below.
    - *Shallow integration* – does not require detailed mutual information to interact with other managed or configured components.

* While loose coupling is desirable for general applications, tight coupling often will be required for critical infrastructure controls.

4.2 Overview of the Standards Identification Process

The process used to establish the lists presented in Tables 4-1 and 4-2 is described in the next section. During the first phase of the NIST three-phase plan for Smart Grid interoperability, NIST's approach to accelerating the development of standards was to 1) identify existing standards that could be immediately applied to meet Smart Grid needs, or are expected to be available in the near future, and 2) identify gaps and establish priorities and action plans to develop additional needed standards to fill these gaps.

Of the three public workshops that NIST convened in 2009, two were devoted, in part, to identifying existing standards—or those under development—that stakeholders suggested as relevant and potentially important to current and future development of the Smart Grid. Following the first of these workshops, held on April 28-29, 2009, NIST published a list of 16 existing standards and other specifications that it felt were appropriate for inclusion in its initial release of Smart Grid interoperability standards.

The list of 16 specifications was published for public review and comment. In a notice published in the *Federal Register*, [55] NIST advised that the list was neither complete, nor exclusionary.

[55] 74 FR 27288 (June 9, 2009).

Other existing standards, it said, "have not been eliminated from consideration, [and] standards that currently appear on the list ultimately may not be included." [56] In all, NIST received comments from 97 individuals and organizations on the 16 standards and specifications. The majority of the comments were positive, and several additional standards were recommended for inclusion on the initial list.

NIST reviewed all comments submitted in response to its notice in the *Federal Register* as well as other inputs received during its many interactions with stakeholders. After reviewing and evaluating all the inputs received, the list was expanded from the initial 16 to include an additional 15 standards. A second list of standards for further consideration was also added to indicate which standards were being considered for future additions to the first list. These lists were both included in a draft version of this document that was posted for a 30-day public comment period during which extensive comments from over 90 individuals and organizations were received.[57]

4.3 Revised List of Standards Identified by NIST

Table 4-1 lists the standards identified by NIST at the conclusion of the process defined above. The list includes the initial 16 specifications, plus 9 standards that NIST added after reviewing and evaluating the inputs it received. Based upon the inputs received and further evaluation of the 15 standards initially added to the list, it was deemed necessary to move some of the standards on the extended list to the second list because they require further evaluation. The list of standards in Table 4-1 was also reordered to better group the documents into families, such as the IETF standards, and the standards were further identified as standards and specifications, requirements, and guidelines. Cyber security standards are also grouped together in each of Tables 4-1 and 4-2.

[56] 74 FR 27288 (June 9, 2009).

[57] Ibid. p. 27288.

Table 4-1. Standards Identified by NIST.

	Standard	Application	Comments
Standards and Specifications			
1	ANSI/ASHRAE 135-2008/ISO 16484-5 BACnet - A Data Communication Protocol for Building Automation and Control Networks http://resourcecenter.ashrae.org/store/ashrae/newstore.cgi?itemid=30853&view=item&page=1&loginid=39839941&priority=none&words=135-2008&method=and&	BACnet defines an information model and messages for building system communications at a customer's site. BACnet incorporates a range of networking technologies to provide scalability from very small systems to multi-building operations that span wide geographic areas using IP protocols.	Open, mature standard with conformance testing developed and maintained by an SDO. BACnet is adopted internationally as EN ISO 16484-5 and used in more than 30 countries. This standard serves as a customer side communication protocol at the facility interface and is relevant to the Price, DR/DER, and Energy Usage PAPs (see Sec. 5.5 - http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/PAP03PriceProduct , Sec. 5.4 - http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/PAP09DRDER, and Sec. 5.3- http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/PAP10EnergyUsagetoEMS).
2	ANSI C12 Suite : ANSI C12.1 http-p://webstore.ansi.org/RecordDetail.aspx?sku=ANSI+C12.1-2008 ANSI C12.18/IEEE P1701/MC1218 http://webstore.ansi.org/FindStandards.aspx?SearchString=c12.18&SearchOption=0	Performance and safety type tests for revenue meters. Protocol and optical interface for measurement devices.	Open, mostly mature standards. It is recognized that ANSI C12.19 is an extremely flexible revenue metering model that allows such a wide range of options that requests for actionable information from a meter, such as usage in kilowatt hours, requires complex programming to secure this information. ANSI C12.19 2008 has a mechanism by which table choices can be described, termed Exchange Data Language (EDL), that can be used to constrain oft-utilized information into a well-known form. A Priority Action Plan (PAP) has been set up to establish common data tables for meter information that will greatly reduce the time for

	&PageNum=0&SearchTermsArray=null|c12.18|null ANSI C12.19/MC1219 http://webstore.ansi.org/RecordDetail.aspx?sku=ANSI+C12.19-2008 ANSI C12.20 http://webstore.ansi.org/FindStandards.aspx?SearchString=c12.20&SearchOption=0&PageNum=0&SearchTermsArray=null|c12.20|null ANSI C12.21/IEEE P1702/MC1221 http://webstore.ansi.org/FindStandards.aspx?SearchString=c12.21&SearchOption=0&PageNum=0&SearchTermsArray=null|c12.21|null	Revenue metering End Device Tables. Revenue metering accuracy specification and type tests. Transport of measurement device data over telephone networks.	utilities and others requiring meter data to implement Smart Grid functions, such as demand response and real-time usage information (see Sec.5.2, http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/PAP05MeterProfiles). It is recognized that C12.22 is an important standard relevant to the transport of C12.19 tables and many comments on the draft framework document recommending it were received. However, it is not included here, but rather in Table 4.2 for further review because it is not clear that sufficient consensus exists for it. Several issues were raised in other comments received, including concerns about layering, security, and the need for better alignment with Internet Protocol and harmonization with the IEC 62056(Device Language Message Specification (DLMS)/Companion Specification for Energy Metering (COSEM)) standard (see #21 in Table 4.2). This further review may require a PAP to be established by the SGIP.

3	ANSI/CEA 709 and CEA 852.1 LON Protocol Suite: ANSI/CEA 709.1-B-2002 Control Network Protocol Specification http://www.ce.org/Standards/browseByCommittee_2543.asp ANSI/CEA 709.2-A R-2006 Control Network Power Line (PL) Channel Specification http://www.ce.org/Standards/browseByCommittee_2545.asp ANSI/CEA 709.3 R-2004 Free-Topology Twisted-Pair Channel Specification http://www.ce.org/Standards/browseByCommittee_2544.asp ANSI/CEA-709.4:1999 Fiber-Optic Channel	This is a general purpose local area networking protocol in use for various applications including electric meters, street lighting, home automation and building automation. This is a specific physical layer protocol designed for use with ANSI/CEA 709.1-B-2002. This is a specific physical layer protocol designed for use with ANSI/CEA 709.1-B-2002. This is a specific physical layer protocol designed for use with ANSI/CEA 709.1-B-2002. This protocol provides a way to tunnel local operating network messages through an IP network using the User Datagram Protocol (UDP), thus providing a way to create larger internetworks	Widely used, mature standards, supported by the LonMark International users group. Proposed for international adoption as part of ISO/IEC 14908, Parts 1, 2, 3, and 4. These standards serve on the customer side of the facility interface and are relevant to the Price, DR/DER, and Energy Usage PAPs; see Sec. 5.5- http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/PAP03PriceProduct , Sec. 5.4 - http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/PAP09DRDER, and Sec. 5.3- http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/PAP10EnergyUsagetoEMS.

	Specification http//www.ce.org/Standards/browseByCommittee_2759.asp CEA-852.1:2009 Enhanced Tunneling Device Area Network Protocols Over Internet Protocol Channels http://www.ce.org/Standards/browseByCommittee_6483.asp		
4	DNP3 http://www.dnp.org/About/Default.aspx	This standard is used for substation and feeder device automation as well as for communications between control centers and substations.	An open, mature, widely implemented specification developed and supported by a group of vendors, utilities and other users. IEEE recommends the use of this protocol, and work is underway to have it adopted as an IEEE standard. A Priority Action Plan (PAP12) was established to support transport of Smart Grid data and management functions over existing DNP3 networks. This PAP is intended to coordinate actions on development of mapping between 61850 and DNP3 objects that will allow presently-communicated SCADA information to be used in new ways, while also providing the ability to create new applications using the existing DNP3 infrastructure (see Sec. 5.12 and PAP12: DNP3 Mapping to IEC 61850 Objects).
5	IEC 60870-6 / TASE.2 http://webstore.iec.ch/webstore/webstore.nsf/artnum/034	This standard defines the messages sent between control	Open, mature standard that is widely implemented with compliance testing. This is part of the IEC

	806	centers of different utilities.	60870 Suite included in PAP14 (Sec 5.11, http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/PAP14TDModels).
6	IEC 61850 Suite http://webstore.iec.ch/webstore/webstore.nsf/artnum/033549!opendocument	This standard defines communications within transmission and distribution. substations for automation and protection. It is being extended to cover communications beyond the substation to integration of distributed resources and between substations.	Open standard that is starting to be adopted in North America. Developed for field device communications within substations, this set of standards is now being extended to communications between substations and including DER. Several PAPs are dedicated to further develop information models for electric transportation Integrate 61850 with DNP3 (Sec 5.12. PAP12: DNP3 Mapping to IEC 61850 Objects) C37.118 (Sec.5.13 PAP13: Harmonization of IEEE C37.118 with IEC 61850 and Precision Time Synchronizatation) Harmonization with CIM and Multispeak (Sec. 5.10, http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/PAP08DistrObjMultispeak)).
7	IEC 61968/61970 Suites http://webstore.iec.ch/webstore/webstore.nsf/artnum/031109!opendocument http://webstore.iec.ch/webstore/webstore.nsf/artnum/035316!opendocument	These families of standards define information exchanged among control center systems using common information models. They define application-level energy management system interfaces and messaging for distribution grid management in the utility space.	Open standards that are starting to become more widely implemented, developed and maintained by an SDO with support from a users group. They are part of PAPs relating to integration with IEC 61850 and Multispeak (Sec. 5.10, http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/PAP08DistrObjMultispeak).

8	IEEE C37.118 https://sbwsweb.ieee.org/ecustomercme_enu/start.swe?SWECmd=GotoView&SWEView=Catalog+View+(eSales)_Standards_IEEE&mem_type=Customer&SWEHo=sbwsweb.ieee.org&SWETS=1192713657	This standard defines phasor measurement unit (PMU) performance specifications and communications.	Open standards, widely implemented, developed and maintained by an SDO. Standard includes some requirements for communications and measurement and is currently being updated by IEEE Power System Relaying Committee (PSRC) Relaying Communications Subcommittee Working Group H11. Some items not covered in C37.118 include communication service modes, remote device configuration, dynamic measurement performance and security. The protocol will not map to very large systems that include more than a couple hundred PMU devices. They are part of PAP13 relating to integration with IEC 61850 and C37.118 (Sec. 5.13, PAP13: Harmonization of IEEE C37.118 with IEC 61850 and Precision Time Synchronizatation).
9	IEEE 1547 Suite https://sbwsweb.ieee.org/ecustomercme_enu/start.swe?SWECmd=GotoView&SWEView=Catalog+View+(eSales)_Standards_IEEE&mem_type=Customer&SWEHo=sbwsweb.ieee.org&SWETS=1192713657	This family of standards defines physical and electrical interconnections between utility and distributed generation (DG) and storage.	Open standards, with significant implementation for the parts covering physical/electrical connections. The parts of this suite of standards that describe messages are not as widely deployed as the parts that specify the physical interconnections. Many utilities and regulators require their use in systems. Revising and extending the IEEE 1547 family is a focus of the PAP covering energy storage interconnections (Sec. 5.14, http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/PAP07Storage).
10	IEEE 1588 http://ieee1588.nist.gov/	Standard for time management and clock synchronization across the Smart Grid for equipment	Open standard. Version 2 is not widely implemented for power applications, developed and maintained by an SDO.

		needing consistent time management.	IEEE PSRC Subcommittee Working Group H7 is developing PC37.238 (IEEE Standard Profile for the Application of IEEE 1588 (Ver. 2) for Applications in Power. Version 2 of the standard is part of the PAP13, which covers precision time synchronization and harmonization of IEEE and IEC standards for communications of phasor data (Sec. 5.13, PAP13: Harmonization of IEEE C37.118 with IEC 61850 and Precision Time Synchronizatation).
11	Internet Protocol Suite including, but not limited to :IETF RFC 2460 (IPv6) http://www.ietf.org/rfc/rfc2460.txt IETF RFC 791 (IPv4) http://www.ietf.org/rfc/rfc791.txt Core Protocol in the Internet Suite, draft-baker-ietf-core-04 http://tools.ietf.org/html/draft-baker-ietf-core-04	The foundation protocol for delivery of packets in the Internet network,.IPv6 is new version of the Internet Protocol that provides enhancements to IPv4 and allows a larger address space. Core Protocols in the Internet Suite applicable for Smart Grid.	A set of open, mature standards produced by IETF for Internet technologies. As part of the tasks for PAP01for IP (Sec 5.7), IETF is to produce an RFC listing of IETF standards applicable for Smart Grid.: http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/PAP01InternetProfile.
12	Multispeak http://www.multispeak.org/About/specifications.htm	A specification for application software integration within the utility operations domain; a candidate for use in an Enterprise Service Bus.	An open, mature specification developed and maintained by a consortium of electric utilities and industry vendors, with an interoperability testing program. It is part of PAP08 for harmonization of CIM and Multispeack (Sec. 5.10, http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/PAP08DistrObjMultispeak).

13	OpenADR http://openadr.lbl.gov/pdf/cec-500-2009-063.pdf	The specification defines messages exchanged between utilities and commercial/industrial customers for price-responsive and direct load control.	Developed by Lawrence Berkeley National Laboratory, used primarily in California. It is part of PAP09 to develop standard demand response signals (Sec. 5.4, http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/PAP09DRDER).
14	OPC-UA Industrial http://www.opcfoundation.org/Downloads.aspx?CM=1&CN=KEY&CI=283	A platform-independent specification for a secure, reliable, high-speed data exchange based on a publish/subscribe mechanism. Modern SOA designed to expose complex data and metadata defined by other information model specifications (e.g. IEC 61850, BACnet, OpenADR). Works with existing binary and XML schema defined data.	Widely supported open standard, with compliance testing program.
15	Open Geospatial Consortium Geography Markup Language (GML) http://www.opengeospatial.org/standards/gml	A standard for exchange of location-based information addressing geographic data requirements for many Smart Grid applications.	An open standard, GML encoding is in compliance with ISO 19118 for the transport and storage of geographic information modeled according to the conceptual modeling framework used in the ISO 19100 series of International Standards and is in wide use with supporting open source software. Also used in Emergency Management, building, facility, and equipment location information bases (http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=32554).
16	ZigBee/HomePlug Smart Energy Profile 2.0 http://www.zigbee.org/Products/TechnicalDocumentsDo	Home Area Network (HAN) Device Communications and Information Model.	A profile under development, but anticipated to be technology-independent and useful for many Smart Grid applications.

	wnload/tabid/237/Default.aspx		
Requirements and Guidelines			
17	OpenHAN http://osgug.ucaiug.org/utilityami/openhan/HAN%20Requirements/Forms/AllItems.aspx	A specification for home area network (HAN) to connect to the utility advanced metering system including device communication, measurement, and control.	A specification developed by a users group, UCAIug, that contains a "checklist" of requirements that enables utilities to compare the many available HANs.
18	AEIC Guidelines v2.0	A guideline comprising a - framework and testing criteria for vendors and utilities who desire to implement standards-based AMI (StandardAMI) as the choice for Advanced Metering Infrastructure (AMI) solutions.	The guidelines in this document were created in order to assist utilities in specifying implementations of ANSI C12.19 typical metering and AMI devices. Intended to constrain the possible options chosen when implementing the ANSI C12 standards and therefore improve interoperability.

Cyber Security			
19	*Security Profile for Advanced Metering Infrastructure, v 1.0*, Advanced Security Acceleration Project – Smart Grid, December 10, 2009 http://osgug.ucaiug.org/utilisec/amisec/Shared%20Documents/AMI%20Security%20Profile%20(ASAP-SG)/AMI%20Security%20P	This document provides guidance and security controls to organizations developing or implementing AMI solutions. This includes the meter data management system (MDMS) up to and including the HAN interface of the smart meter.	The Advanced Metering Infrastructure Security (AMI-SEC) Task Force was established under the Utility Communications Architecture International Users Group (UCAIug) to develop consistent security guidelines for AMI.

	rofile%20-%20v1_0.pdf.		
20	Department of Homeland Security, National Cyber Security Division. 2009, September. Catalog of Control Systems Security: Recommendations for Standards Developers. http://www.us-cert.gov/control_systems/pdf/FINAL-Catalog_of_Recommendations_Rev4_101309.pdf	The catalog presents a compilation of practices that various industry bodies have recommended to increase the security of control systems from both physical and cyber attacks.	This is a source document for the DRAFT NIST Interagency Report NISTIR 7628 Smart Grid Cyber Security Strategy and Requirements (http://csrc.nist.gov/publications/drafts/nistir-7628/draft-nistir-7628.pdf).
21	DHS Cyber Security Procurement Language for Control Systems http://www.us-cert.gov/control_systems/pdf/FINAL-Procurement_Language_Rev4_100809.pdf	The National Cyber Security Division of the Department of Homeland Security (DHS) developed this document to provide guidance to procuring cyber security technologies for control systems products and services - it is not intended as policy or standard. Because it speaks to control systems, its methodology can be used with those aspects of Smart Grid systems.	This is a source document for the DRAFT NIST Interagency Report NISTIR 7628 Smart Grid Cyber Security Strategy and Requirements (http://csrc.nist.gov/publications/drafts/nistir-7628/draft-nistir-7628.pdf).
22	IEC 62351 Parts 1-8 http://webstore.iec.ch/webstore/webstore.nsf/artnum/037996!opendocument	This family of standards defines information security for power system control operations.	Open standard, developed and maintained by an SDO, but not widely used yet.

23	IEEE 1686-2007 https://sbwsweb.ieee.org/ecustomercme_enu/start.swe?SWECmd=GotoView&SWEView=Catalog+View+(eSales)_Standards_IEEE&mem_type=Customer&SWEHo=sbwsweb.ieee.org&SWETS=1192713657	The IEEE 1686-2007 is a standard that defines the functions and features to be provided in substation intelligent electronic devices (IEDs) to accommodate critical infrastructure protection programs. The standard covers IED security capabilities including the access, operation, configuration, firmware revision, and data retrieval.	Open standard, developed and maintained by an SDO, not widely implemented yet.
24	NERC CIP 002-009 http://www.nerc.com/page.php?cid=2|20	These standards cover physical and cyber security standards for the bulk power system.	Mandatory for the bulk electric system. Currently being revised by NERC.
25	NIST Special Publication (SP) 800-53, NIST SP 800-82 http://csrc.nist.gov/publications/drafts/800-82/draft_sp800-82-fpd.pdf; http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final-errata.pdf.	These standards cover cyber security standards and guidelines for federal information systems, including those for the bulk power system.	Open standards developed by NIST. SP800-53 defines security measured required for all U.S. government computers. SP800-82 is in draft form. It defines security specifically for industrial control systems, including the power grid.

While there is strong stakeholder consensus on the relevance of the standards listed in Table 4-1, many of the specifications require enhancements or other changes necessary to fully address Smart Grid requirements. Many of the necessary modifications to these standards and related specifications will be driven by the PAPs described in the next chapter. In addition, the Cyber Security Coordination Task Group, whose ongoing efforts are summarized in Chapter 6, is also addressing some of these needed modifications.

4.4 Additional Standards Identified by NIST Subject to Further Review

NIST and its contractor, the Electric Power Research Institute (EPRI), convened a second workshop held on May 19-20, 2009, where more than 600 participants engaged in sessions focused on analyzing and enhancing use cases, locating key interfaces, determining Smart Grid interoperability requirements, and identifying additional standards for consideration. Many of the use cases discussed during this workshop referenced standards in addition to those in Table 4-1. Altogether, the use cases, which concentrated on the six priority areas, yielded more than 70 candidate standards and emerging specifications, which were compiled in the EPRI's *Report to NIST on the Smart Grid Interoperability Standards Roadmap.*[58] The additional candidate standards that are not covered by those in Table 4-1 are presented in Table 4-2.

Four "non-exclusive criteria" were used in the May 19-20, 2009 workshop for identification of standards to be included in the list:

- Standard is supported by a Standards-Development Organization (SDO) or via an emergent SDO process.
- Standard is supported by a users' community.
- Standard is directly relevant to the use cases analyzed for the Smart Grid.
- Consideration was given to those standards with a viable installed base and vendor community.

EPRI's *Report to NIST on the Smart Grid* also was submitted for public review and comment. However, the standards listed were only a portion of a lengthy report. **NIST used the public review process for this document as an opportunity to solicit further public comments and recommendations on existing standards or emerging specifications for standards listed in the document.** The list of standards in Table 4-2 was revised based on the public comments obtained through the *Federal Register* notice.

[58] *Report to NIST on the Smart Grid Interoperability Standards Roadmap* (Contract No. SB1341-09-CN-0031—Deliverable 7) Prepared by the Electric Power Research Institute (EPRI), June 17, 2009.

Table 4-2. Additional Standards, Specifications, Profiles, Requirements, Guidelines, and Reports for Further Review.

	Standards, Specifications, Requirements, Guidelines, Reports	Application	Comments
1	ANSI C12.22-2008/IEEE P1703/MC1222 http://webstore.ansi.org/FindStandards.aspx?SearchString=c12.22&SearchOption=0&PageNum=0&SearchTermsArray=null|c12.22|null	End Device Tables communications over any network.	It is recognized that C12.22 is an important standard relevant to the transport of C12.19 tables and many comments on the draft framework document recommending it were received. However, it is identified for further review because it is not clear that sufficient consensus exists for it. Several issues were raised in other comments received, including concerns about layering, security, and the need for better alignment with Internet Protocol and harmonization with the IEC 62056(Device Language Message Specification (DLMS)/Companion Specification for Energy Metering (COSEM)) standard (see #21 in this list). This further review may require a PAP to be established by the SGIP.
	ANSI C12.23	Compliance Testing for Standard Protocols (C12.18, C12.19, C12.21 and C12.22)	Draft standard for compliance testing of ANSI C12 communication standards
	ANSI C12.24	A catalog of calculation algorithms for VAR/VA that is in draft form. It may ultimately become a report instead of a standard.	VAR and VA have multiple formulas that can be used and depending on the waveform, do not give the same result. This document is a catalog of the present algorithms used to implement the formulas in order for all parties to know what

			algorithm the meter has implemented. This document should be considered once it is completed.
2	CableLabs PacketCable Security Monitoring and Automation Architecture Technical Report http://www.cablelabs.com/specifications/PKT-TR-SMA-ARCH-V01-081121.pdf	A technical report describing a broad range of services that could be provided over television cable, including remote energy management.	This report contains a security, monitoring, and automation architecture for home networks and should be re-evaluated by the SGIP.
3	Global Positioning System (GPS) Standard Positioning Service (SPS) Signal Specification http://pnt.gov/public/docs/1995/signalspec1995.pdf	Standard for using GPS to establish accurate geospatial location and time.	This specification defines the publicly available service provided by GPS and specifies GPS SPS ranging signal characteristics and SPS performance. See also Open Geospatial Consortium listing in this chapter.
4	HomePlug AV	Entertainment networking content distribution for consumer electronic equipment.	This specification uses Power Line Communications, harmonization and coexistence with other PLC standards is being addressed by PAP15 (Sec. 5.9, http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/PAP15PLCForLowBitRates).
5	HomePlug C&C	Control and management of residential equipment for whole-house control products: energy management, lighting, appliances,	This specification uses Power Line Communications, harmonization and coexistence with other PLC standards is being addressed by PAP15 for PLC (Sec. 5.9,

		climate control, security, and other devices.	http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/PAP15PLCForLowBitRates).
6	IEEE 61400-25 http://www.iec.ch/cgi-bin/procgi.pl/www/iecwww.p?wwwlang=E&wwwprog=sea22.p&search=iecnumber&header=IEC&pubno=61400&part=&se=	Communication and control of wind power plants.	This set of standards is being considered for addition to the "61850 Suite" because it uses 61850 modeling principles to address wind power applications. However, it goes further to recommend multiple protocol mappings, some of which cannot transport all of the basic services of 61850.
7	ITU Recommandation G.9960 (G.hn) http://www.itu.int/ITU-T/aap/AAPRecDetails.aspx?AAPSeqNo=1853	In-home networking over power lines, phone lines, and coaxial cables.	This harmonization and coexistence of this standard with other PLCs is being addressed by PAP15 for PLC (Sec. 5.9, http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/PAP15PLCForLowBitRates).
8	IEEE P1901	Broadband communications over Powerline medium access control (MAC) and physical layer (PHY) protocols.	This harmonization and coexistence of this standard with other PLCs is being addressed by PAP15 for PLC (Sec. 5.9, http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/PAP15PLCForLowBitRates).
9	ISO/IEC 8824 ASN.1 (Abstract Syntax Notation)	Used for formal syntax specification of data; used in (e.g.) X.400.	Any SDO may decide to use ASN.1 notation when defining the syntax of data structures.
10	ISO/IEC 12139-1	High speed power line communications medium access control (MAC) and physical layer (PHY) protocols.	This harmonization and coexistence of this standard with other PLC standards is being addressed by PAP15 for PLC (Sec. 5.9, http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/PAP15PLCForLowBitRates).
11	IEEE 802 Family	This includes standards developed by the IEEE 802 Local Area and Metropolitan Area Network	A set of open, mature standards for wired and wireless LLC/MAC/PHY protocols developed by IEEE 802. Other related specifications

		Standards Committee.	include those developed by Industry fora such as WiFi Alliance, WiMAX Forum, and Zigbee Alliance to promote the use of these standards and to provide implementation testing and certification. PAP02 for wireless will produce guidelines and attributes for wireless protocols. (http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/PAP02Wireless).
12	TIA TR-45/3GPP2 Family of Standards	Standards for cdma2000® Spread Spectrum and High Rate Packet Data Systems.	A set of open standards for cellular phone networks. PAP02 for wireless will produce guidelines and attributes for wireless protocols.(http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/PAP02Wireless).
13	3GPP Family of Standards - Including 2G (CSD, HSCSD, GPRS, EDGE, EDGE Evolution), 3G (UMTS/FOMA, W-CDMA EUTRAN, HSPA, HSPA+, 4G (LTE Advanced)	2G, 3G, and 4G cellular network protocols for packet delivery.	A set of open international standards for cellular phone networks. PAP02 for wireless will produce guidelines and attributes for wireless protocols. (http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/PAP02Wireless).
14	ETSI GMR-1 3G Family of standards	GMR-1 3G is a satellite-based packet service equivalent to 3GPP standards.	ETSI and TIA Geo-Mobile Radio Air Interface standards for mobile satellite radio interface, evolved from the GSM terrestrial cellular standard.
15	ISA SP100	Wireless communication standards intended to provide reliable and secure operation for non-critical monitoring, alerting, and control applications specifically focused to	Standards developed by ISA-SP100 Standards Committee, Wireless Systems for Automation.

		meet the needs of industrial users.	
16	Network Management Standards - including Internet based standards such as DMTF, CIM, WBEM, ANSI INCITS 438-2008, SNMP v3, netconf, STD 62, and OSI-based standards including CMIP/CMIS)	Protocols used for management of network components and devices attached to the network.	A future PAP may be needed to produce guidelines on which protocol to use under specific network technology.
17	NIST SP 500-267	A profile for IPv6 in the U.S. Government.	A version of IPv6 profile for Smart Grid will be produced.
18	Z-wave http://www.z-wave.com/modules/ZwaveStart/	A wireless mesh networking protocol for home area networks.	Technology developed by the Z-Wave Alliance.
19	IEEE P2030	Draft Guide for Smart Grid Interoperability of Energy Technology and Information Technology Operation with Electric Power System (EPS) and End-Use Applications and Loads.	Standards, guidelines to be developed by IEEE P2030 Smart Grid Interoperability.
20	IEC 60929 AC-supplied electronic ballasts for tabular fluorescent lamps – performance requirements	Standard specifies communications of information to and from lighting ballasts for Energy Management Systems.	Appendix E of this standard defines the Digital Addressable Lighting Interface (DALI), which is a protocol for the control of lighting in buildings.
21	IEC 62056 Device Language Message Specification	Energy metering communications.	This suite of standards contains specifications for the application layers of the DLMS for energy metering. It is supported by a user group, the

	(DLMS)/Companion Specification for Energy Metering (COSEM)) Electricity metering - Data exchange for meter reading, tariff and load control		DLMS User Association.
22	IEC PAS 62559 http://webstore.iec.ch/preview/info_iecpas62559%7Bed1.0%7Den.pdf	Requirements development method covers all applications.	This specification describes the EPRI Intelligrid[SM] methodology for requirements development. It is a pre-standard that is gaining acceptance by early Smart Grid and AMI implementing organizations and has been used the NIST May workshop and is used in several PAP tasks.
23	IEEE C37.2-2008 IEEE Standard Electric Power System Device Function Numbers	Protective circuit device modeling numbering scheme for various switchgear.	Open standard. The latest revision contains cross-references between C37.2 numbers and IEC 61850-7-4 logical nodes.
24	IEEE C37.111-1999 IEEE Standard Common Format for Transient Data Exchange (COMTRADE) for Power Systems (COMTRADE)	Applications using transient data from power system monitoring, including power system relays, power quality monitoring field and workstation equipment.	Open standard to facilitate monitoring of instabilities in the power grid.
25	IEEE C37.232 Recommended Practice for Naming Time Sequence Data Files	Naming time sequence data files for substation equipment requiring time sequence data.	Recommended practice that resolves issues with reporting, saving, exchanging, archiving and retrieving large numbers of substation data files. The recommended practice has been adopted by

			utilities and manufacturers and is recommended by the North American Energy Reliability Corporation (NERC) and the Northeast Power Coordinating Council.
26	IEEE 1159.3 Recommended Practice for the Transfer of Power Quality Data	Applications using of power quality data.	It is a recommended practice for a file format suitable for exchanging power quality-related measurement and simulation data in a vendor-independent manner.
27	IEEE 1379-2000	Substation Automation - Intelligent Electronic Devices (IEDs) and remote terminal units (RTUs) in electric utility substations.	Recommends the use of DNP3 or IEC 60870-5 for substation IED communications.
28	ISO/IEC 15045, "A Residential gateway model for Home Electronic System." http://www.iso.org/iso/catalogue_detail.htm?csnumber=26313	Specification for a residential gateway (RG) that connects home network domains to network domains outside the house. This standard will be evaluated in the discussions of Home Area Networks.	This should be considered as standards for residential networks are established under present and future PAPs.
29	ISO/IEC 15067-3 "Model of an energy management system for the Home Electronic System." http://webstore.iec.ch/preview/info_isoiec15067-3%7Bed1.0%7Den.pdf	A model for energy management that accommodates a range of load control strategies.	This should be reconsidered as standards for the residential networks are established under present and future PAPs.
30	ISO/IEC 18012, "Guidelines for Product Interoperability."	Specifies requirements for product interoperability in the home and building automation systems.	This should be reconsidered as standards for the residential networks are established under present and future PAPs.

	http://www.iso.org/iso/catalogue_detail.htm?csnumber=30797 http://www.iso.org/iso/catalogue_detail.htm?csnumber=46317		
31	North American Energy Standards Board (NAESB) Open Access Same-Time Information Systems (OASIS)	Utility business practices for transmission service.	Practices are mandated by FERC, it specifies the methods and information that must be exchanged between market participants and market Operators for transactions in wholesale electric power industry.
32	NAESB WEQ 015 Business Practices for Wholesale Electricity Demand Response Programs	Utility business practices for demand response.	Current standardized business practices for DR/DER communications. It is part of PAP09 to develop standard demand response signals (Sec. 5.4, http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/PAP09DRDER).
33	NEMA Smart Grid Standards Publication SG-AMI 1-2009 – Requirements for Smart Meter Upgradeability http://www.nema.org	This standard will be used by smart meter suppliers, utility customers, and key constituents, such as regulators, to guide both development and decision making as related to smart meter upgradeability.	This standard serves as a key set of requirements for smart meter upgradeability. These requirements should be used by Smart Meter suppliers, utility customers, and key constituents, such as regulators, to guide both development and decision making as related to smart meter upgradeability. The Purpose of this document is to define requirements for smart meter firmware upgradeability in the context of an AMI system for industry stakeholders such as regulators, utilities, and vendors.
34	OASIS EMIX (Energy Market Information eXchange)	Exchange of price, characteristics, time, and related information for markets, including market makers,	This common price and product definition communication standard is under development as part of the common price communications PAP

		market participants, quote streams, premises automation, and devices	03 (see Sec. 5.5, http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/PAP03PriceProduct).
35	Fix Protocol, Ltd. FIXML Financial Information eXchange Markup Language http://www.fixprotocol.org/specifications/fix4.4fixml	FIXML is a Web services implementation of FIX (Financial Information Exchange). FIX is the most widely used protocol for financial trading today.	This standard serves as a reference point for OASIS EMIX (see above) in the PAP 03 effort (see Sec. 5.5, http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/PAP03PriceProduct).
36	OASIS oBIX	General Web service specification for communicating with control systems.	This open specification is an integration interface to and between control systems and to a growing extent, between enterprises and building systems.
37	OASIS WS-Calendar	XML serialization of IETF iCalendar for use in calendars, buildings, pricing, markets, and other environments. A communication specification used to specify schedule and interval between domains.	This standard is the primary deliverable of the common schedules PAP04 (see Section 5.6 http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/PAP04Schedules) and will be incorporated into EMIX and other standards.
38	SAE J1772 Electrical Connector between PEV and EVSE	Electrical connector between Plug-in Electric Vehicles (PEVs) and Electric Vehicle Supply Equipment (EVSE).	This will be considered when it is finalized along with other relevant plug standards.
39	SAE J2836/1-3 Use Cases for PEV Interactions	J2836/1: Use Cases for Communication between Plug-in Vehicles and the Utility Grid. J2836/2: Use Cases for Communication between Plug-in Vehicles and the Supply Equipment (EVSE). J2836/3: Use Cases for Communication between	This will be considered when it is updated based on PAP11 task 1.

		Plug-in Vehicles and the Utility Grid for Reverse Power Flow.	
40	SAE J2847/1-3 Communications for PEV Interactions	J2847/1 Communication between Plug-in Vehicles and the Utility Grid. J2847/2 Communication between Plug-in Vehicles and the Supply Equipment (EVSE). J2847/3 Communication between Plug-in Vehicles and the Utility Grid for Reverse Power Flow.	This will be considered when it is finalized.
41	W3C Simple Object Access Protocol (SOAP)	XML protocol for information exchange.	SOAP is a published standard for structured Web services communication. As such it should be considered for use in the smart grid domain when such functionality is required.
42	W3C WSDL Web Service Definition Language	Definition for Web services interactions.	WSDL is a standard for defining Web services interactions. As such it should be considered for use in the smart grid domain when such functionality is required.
43	W3C XML eXtensible Markup Language	Self-describing language for expressing and exchanging information.	XML is a core standard for structuring data. As such it should be considered for use in the Smart Grid domain when such functionality is required.
44	W3C XSD (XML Definition)	Description of XML artifacts, which used in WSDL (q.v.) and Web Services as well as other XML applications.	XSD is a standard for defining XML data instances. As such it should be considered for use in the Smart Grid domain when such functionality is required.
45	W3C EXI	Efficient XML interchange.	EXI is an alternate binary encoding for XML. As such it should be considered for use in the smart grid domain when such functionality is required.

46	US Department of Transportation's Federal Highway Administration's Intelligent Transportation System (ITS) Standard NTCIP 1213, "Electrical Lighting and Management Systems (ELMS) http://www.ntcip.org/library/documents/pdf/1213v0219d.pdf	Addresses open protocol remote monitoring and control of street, roadway and highway based electrical assets including lighting, revenue grade metering, power quality, and safety equipment including remote communicating ground fault and arc fault interrupters.	Development began development in 1992 by the NEMA 3-TS Transportation Management Systems and Associated Control Devices; transferred initial work from an ad hoc committee of the Illuminating Engineering Society of North America (IESNA) in 2002 and formed the ELMS Working Group to further develop the control objects based on NTCIP.
Cyber Security			
47	ISA SP99 http://www.isa.org/MSTemplate.cfm?MicrositeID=988&CommitteeID=6821	Cyber security mitigation for industrial and bulk power generation stations. International Society of Automation (ISA) Special Publication (SP) 99 is a standard that explains the process for establishing an industrial automation and control systems security program through risk analysis, establishing awareness and countermeasures, and monitoring and improving an organization's cyber security management system. Smart Grid contains many control systems that require cyber security management.	This will be used in the development of the DRAFT NIST Interagency Report NISTIR 7628 Smart Grid Cyber Security Strategy and Requirements: (http://csrc.nist.gov/publications/drafts/nistir-7628/draft-nistir-7628.pdf).

48	ISO27000 http://www.27000.org/	The ISO 27000 series of standards have been specifically reserved by ISO for information security matters.	This will be used in the development of the DRAFT NIST Interagency Report NISTIR 7628 Smart Grid Cyber Security Strategy and Requirements (http://csrc.nist.gov/publications/drafts/nistir-7628/draft-nistir-7628.pdf).
49	NIST FIPS 140-2 http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf	U.S. government computer security standard used to accredit cryptographic modules.	Required for the federal government. As such it should be considered for use in the Smart Grid domain when such functionality is required.
50	OASIS WS-Security and OASIS suite of security standards	Toolkit for building secure, distributed applications, applying a wide range of security technologies. The toolkit includes profiles for use of tokens applying SAML, Kerberos, X.509, Rights Expression Language, User Name, SOAP profiles for security, and others.	Broadly used in eCommerce and eBusiness applications. Fine-grained security. WS-Security is -part of an extended suite using SAML, XACML, and other fine-grained security standards. As such it should be considered for use in the Smart Grid domain when such functionality is required.

4.5 Process for Future Smart Grid Standards Identification

In all, it is anticipated that hundreds of standards will be required to build a safe and secure Smart Grid that is interoperable, end to end. Identification and selection of standards will be aided by useful, widely accepted criteria or guidelines. Clearly, any set of guidelines for evaluating candidate standards will have to evolve as the Smart Grid is developed, new needs and priorities are identified, and new technologies emerge. For example, NIST concentrated on six priority areas for the first phase of its standards-coordination effort. As this effort proceeds, new priorities will be established and standards applicable to these priorities will be emphasized.

In evaluating standards for inclusion, NIST also recommends considering principles put forward by the World Trade Organization's Committee on Technical Barriers to Trade "Decision of the Committee - Principles for the Development of International Standards, Guides and Recommendations (Annex 4)." These are summarized below:

1. Transparency in the standards development process;
2. Openness of the standardizing body to all interested parties;
3. Impartiality and consensus in the standards development process;
4. Relevance and effectiveness in responding to regulatory and market needs, as well as scientific and technological developments;
5. Coherence, such that standards minimize duplication and overlap with other existing international standards; and
6. Developmental dimensions have been adequately addressed by the standards-developing body.

5 Priority Action Plans

5.1 Overview

NIST has identified an initial set of priorities for developing and improving standards necessary to build an interoperable Smart Grid. Among the criteria for inclusion on this initial list were 1) immediacy of need, 2) relevance to high-priority Smart Grid functionalities,[59] 3) availability of existing standards to respond to the need, and 4) the extent and stage of the deployment of affected technologies. In assembling this list, NIST considered stakeholder input received at three public workshops and other public interactions, as well as reviews of research reports and other relevant literature.

The August 3-4, 2009, NIST Smart Grid workshop engaged more than 20 standards-setting organizations (SSOs) as well as user groups to address these priorities through the establishment of priority action plans (PAPs). At the workshop, SSOs and other Smart Grid stakeholders agreed on many individual and collaborative responsibilities for addressing standards issues and gaps. They also defined tasks and set aggressive timelines for accomplishing many of them. The ongoing PAP prioritization, resource identification and oversight, and timelines for addressing remaining gaps and overlaps, as well as other standardization needs that will inevitably emerge, will be determined in consultation with the Smart Grid Interoperability Panel (SGIP) that has been established to provide an open process for stakeholders to participate in providing input and cooperating with NIST in the ongoing coordination, acceleration and harmonization of standards development for the Smart Grid..

In addition to parallel efforts on cyber security (described in the next chapter), the creation and development of PAPs is proceeding rapidly, but these plans will continue to be improved and refined in order to incorporate new developments and to reflect the current status of plan implementation. Complete and updated versions of the PAPs, which are summarized below, can be found on-line on the NIST Smart Grid Collaboration Site.[60]

Please note that while the PAPs are individually numbered (PAP 01, PAP 02, …) to help organize and reference these efforts, the PAP summaries in this section are grouped together by subject area and are not presented in numerical PAP order. The organization of the PAP summaries below is as follows:

- PAPs supporting metering: Meter Upgradeability Standard (PAP 00); Standard Meter Data Profiles (PAP 05);

[59] NIST is focusing initial standardization efforts on six Smart Grid functionalities: wide-area situational awareness; demand response; electric storage; electric transportation; advanced metering infrastructure; and distribution grid management; in addition to cyber security and network communications. See Chapter 1 for a discussion of these priorities.

[60] http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/WebHome.

- PAPs supporting enhanced customer interactions with the Smart Grid: Standards for Energy Usage Information (PAP 10); Standard Demand Response Signals (PAP 09); Develop Common Specification for Price and Product Definition (PAP 03); and Develop Common Scheduling Communication for Energy Transactions (PAP 04);

- PAPs supporting smart grid communications: Guidelines for the Use of IP Protocol Suite in the Smart Grid (PAP 01); Guidelines for the Use of Wireless Communications (PAP 02); and Harmonize Power Line Carrier Standards for Appliance Communications in the Home (PAP 15)

- PAPs supporting distribution and transmission: Develop Common Information Model (CIM) for Distribution Grid Management (PAP 08); Transmission and Distribution Power Systems Model Mapping (PAP 14); IEC 61850 Objects/DNP3 Mapping (PAP 12); and Harmonization of IEEE C37.118 with IEC 61850 and Precision Time Synchronization (PAP13); and

- PAPs supporting new smart grid technologies: Energy Storage Interconnection Guidelines (PAP 07); Interoperability Standards to Support Plug-in Electric Vehicles (PAP 11).

The initial PAPs reflect just the beginning of an accelerated development and sustained standardization effort that will span a number of years. New PAPs will be developed over time as existing PAPs are completed to encompass the larger scope of standardization efforts that will be required as the nation pursues the vision of a fully interoperable Smart Grid. In collaboration with NIST, the SGIP also will be responsible for creating new PAPs to address gaps that are identified in the future. To facilitate this process, NIST has directed EnerNex, which is assisting NIST under an ARRA-funded contract, to develop a formalized template for categorizing, defining, and assigning new action plans.

Meter Upgradeability Standard—A Completed Priority Action Plan (PAP 00)

To support the development and deployment of a Smart Grid, many electric utilities are looking to make their Advanced Metering Infrastructure (AMI) and smart meter investments now as a precursor or enabler to additional Smart Grid, energy management, and consumer participation initiatives.

One of the critical issues facing these electric utilities and their regulators is the need to ensure that technologies or solutions that are selected by utilities will be interoperable and comply with the yet-to-be-established national standards. Further, many utilities want to ensure that the system they select will allow for evolution and growth as Smart Grid standards evolve. To manage change in a dynamically growing Smart Grid, it is essential to be able to upgrade firmware, such as meters, in the field without replacing the equipment or "rolling a truck" to manually upgrade the meter firmware. Remote image download capability, common practice today in many embedded computing devices, will permit certain characteristics of the meter to be substantially altered on an as needed basis.

For investment in and deployment of smart metering to continue at an aggressive pace, industry requires standards to accommodate upgradeability requirements. These standards are needed to allow utilities to mitigate risks associated with "predicting the future" and to install systems that are flexible and upgradeable to comply with emerging requirements for the Smart Grid.

NIST identified this need for a meter upgradeability standard as a high priority requiring immediate attention. The objective was to define requirements for smart meter firmware upgradeability in the context of an AMI system for industry stakeholders, such as regulators, utilities, and vendors. The National Electrical Manufacturers Association (NEMA) accepted the challenge to lead this effort to develop a standard set of requirements for smart meter upgradeability on an exceptionally rapid schedule. The standard was completed in less than 90 days with the help of a team of meter manufacturers and electric utilities. The standard has been approved by NEMA's Codes & Standards Committee, and is titled NEMA Smart Grid Standards Publication SG-AMI 1-2009 – Requirements for Smart Meter Upgradeability. This standard will be used by smart meter suppliers, utility customers, and key constituents, such as regulators, to guide both development and decision making as related to smart meter upgradeability. The final standard is available from NEMA's Web site (www.nema.org) at no cost. In total, the standard was produced in roughly 90 days from start to final NEMA approval, which is a truly accelerated standards development.

5.2 Standard Meter Data Profiles (PAP 05)

What

This action plan will define meter data in standard profiles. The common profiles will benefit not only the utility company, but also customers and the devices they use to manage their energy consumption, such as thermostats and building automation systems. Other potential clients exist inside and outside of the customer premises.

Action plan tasks include completion of AEIC Guidelines v2.0, mapping utility requirements expressed via AEIC Guidelines v2.0 to ANSI C12.19 device classes by March 2010, and expressing AEIC Guidelines v2.0 in terms of one or more additional ANSI C12.19 device classes by May 2010. Other tasks include socializing the existence of additional tables within ANSI C12.21-2006 and C12.22-2008 and socializing the existence and application of existing default sets, and the definition of new default sets, device classes, and profiles via Web conferences, all by fourth quarter 2010.

Why

Consumers will be better able to reduce energy consumption when they have easy access to usage data. Different meter vendors report meter data in tables that are not uniform across all vendors. The reason for this is that ANSI C12.19, the relevant standard for this purpose, is a flexible revenue metering data structure. In effect, it allows such a wide range of options that a request for actionable information from a meter, such as usage in kilowatt hours, requires complex programming to secure this information. Exchange Data Language (EDL) from the ANSI C12.19 2008 standard offers a mechanism by which table choices can be constrained into a well-known form for oft-utilized information.

Meter information that can be made available in common data tables will greatly reduce the time for utilities and others requiring meter data to implement Smart Grid functions, such as demand response and real-time usage information. It was decided to wait until completion of this priority action plan before proceeding with tasks for PAP 06 “Translate ANSI C12.19 to the Common Semantic Model of CIM.” This translation will facilitate use of meter information to support back office functions and grid operations. Once the common data tables created under PAP 05 are completed, they can then be expressed in terms of IEC 61968 (CIM) as part of PAP 06, and appropriate tasks will be defined at that time. PAP 06 is not included in this document, but the description can be found at: http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/PAP06Meter.

Major Plan Objectives

- Define common meter Device Classes by building upon the work performed by the AEIC for defining the common meter data tables that are required to enable Smart Grid applications.
- Deliver these meter Device Classes to ANSI C12 SC17 for inclusion in ANSI C12.19-2008.
- Revise ANSI C12.19 and publish by July 2010.

- Publish these meter Device Classes in ANSI C12.19 and make these meter Device Classes readily available for use by all vendors and software implementers.

Project Team

NIST lead: Tom Nelson

Collaborators:

Association of Edison Illuminating Companies (AEIC)

American National Standards Institute (ANSI) C12 SC12.1; C12 SC17

ANSI C12 SC17 WG1; C12 SC17 WG2; C12 SC17 WG3; C12 SC17 WG4

International Electrotechnical Commission (IEC) TC13; TC57 Smart Grid TF

Institute of Electrical and Electronic Engineers (IEEE) SCC31; SCC31 End Devices SC

MultiSpeak

National Electrical Manufacturers Association (NEMA)

UCA International Users Group (UCAIug) AMI-NET TF

Measurement Canada

The full plan can be found at: http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/PAP05MeterProfiles.

5.3 Standards for Energy Usage Information (PAP 10)

Customers will benefit from energy usage information that enables them to make better decisions and take other actions consistent with the goals of Sections 1301 and 1305 of EISA. An understanding of energy usage informs better decisions about energy use and conservation, and is the basis for performance feedback on the operation of customer-owned energy management systems and understanding device energy usage and management.

Some states have already mandated customer access to meter-based usage information. As part of this action plan, a limited set of requirements are driving a specification which is expected in February 2010.

Subsequent work in the first half of 2010 will drive a standardized information model for broader exchange of usage information. This model for cross-domain interaction needs the characteristics of integration models as described elsewhere in this document.

What

This action plan will lead to data standards to exchange fine-grained and timely information about energy usage. The first goal is agreement on a core information set to enable integration of usage information throughout facility decision processes. Customers and customer-authorized third-party service providers will use these standards to access energy usage information from the Smart Grid and meter, enabling them to make better decisions about energy use and conservation. Consumers and premises-based systems will use these standards to provide real-

time feedback on present and projected performance. Using the Smart Grid infrastructure, this information will be shared with the facility: a home, building, or industrial installation. Two-way flows of usage information will improve collaboration and thereby energy efficiency.

The data standards will enable immediate and widespread benefit. They will support access to monthly usage information, which may already be available, as well as near-real-time information as smart meters and other devices are deployed. The standards will enable innovation by third-party service and software providers in providing novel ways to help consumers and operations manage their energy usage. In the absence of these standards, software developers and utilities would have to negotiate pair-wise interfaces, an impractical situation. The standards will also promote more responsive facilities. Devices that deliver and understand common usage information can be deployed more quickly.

These standards must be developed on an aggressive timetable. States such as California and Texas have mandated that consumers have electronic access to such data in 2010. This action plan will result in both an initial specification of narrower information to satisfy regulatory mandates by February 2010 and a requirements-based definition for standard energy usage within the facility as well as to and from the Smart Grid by mid-2010.

Why

Attempts to encourage consumers of electricity to conserve energy are enhanced when consumers have the means to track their actual energy use. Real-time, or near real-time, information supports energy management decisions and actions far more effectively than after-the-fact billing. Today, limited access to information already collected hinders customer-focused energy management. Making understandable, actionable energy usage information readily available to consumers requires widely adopted data standards. Such standards will support innovation in automated energy management services and products, help to build national and global markets for these technologies, and help to conserve energy.

The on-premises meter can provide information about energy consumption. This information can also be made available through energy delivery systems (such as those operated by utilities or aggregating service providers) and through consumer devices. In larger facilities, customer-owned sub-meters are common, but accurate meter information at the boundary of the facility is still critical information. Anticipated initial users of this information model will be utilities and other service providers, which will provide energy usage information to customers via the World Wide Web, or public Internet. The model also will support development of on-premises devices that can access meters and provide usage information directly to the occupant.

Device and facility usage is the other target—sharing of usage and load and demand historical and projected information inside a facility makes that facility more valuable to the Smart Grid, as aggregated projections can be passed on to the Smart Grid operations domain, making forecasting and management better. Inside the facility, the energy efficiency goals of EISA and Department of Energy initiatives are better served by consistent usage information exchange.

This effort will support information standards for load curtailment, load shaping, and energy market operations. The initial focus, however, is on immediate steps to define and standardize energy usage information up through the existing Smart Grid infrastructure and to make it more readily available.

Major Plan Objectives

- Develop a summary of initial information needs for various means of customer access to metering and billing information. These initial requirements and use cases have been developed (October 2009).
- Vet these requirements among standards organizations (including IEC, NEMA, OASIS, and ZigBee) and identify potential harmonization opportunities. UCAIug has committed to developing a statement of support for extending their process to include additional stakeholders. This work is in progress.
- Carry out an initial effort to meet upcoming state public utility commission mandates (including California's) to provide the customer electronic access to energy usage data (from both smart meters and legacy meters). This effort must plan for a transition to the broader energy usage effort, so applications designed to use the initial release will function properly in the presence of data from later, more extensive releases. The goal is to have useable definitions in place by February 2010 to meet Public Utilities Commissions' (PUC) mandates.
- Define a framework for sharing energy usage information with and within the premise with minimal changes to existing Smart Grid or legacy meters, during the first half of 2010.
- Develop an information model that can be easily transformed and transported via standards and specifications including but not limited to those from IETF, W3C, OASIS, IEC61970/61968, IEC61850, ANSI C12.19/22, ASHRAE 135, and ZigBee Smart Energy Profile (SEP).
- Implement a plan to expedite harmonized standards development and adoption within the associated standards bodies.

Project Team:

NIST lead: David Wollman

Lead organization: UCAIug – OpenSG

Coordinating organizations:

International Electrotechnical Commission (IEC) (61850; 61970/61968)

National Electrical Manufacturers Association (NEMA) (ANSI C12 Secretariat)

Organization for the Advancement of Structured Information Standards (OASIS)

Open DeviceNet Vendors Association (ODVA)

American Society of Heating, Refrigerating and Air Conditioning Engineers (ASHRAE)

EIS Alliance

LonMark International

International Society of Automation (ISA)

ZigBee

The full plan can be found at: http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/PAP10EnergyUsagetoEMS.

5.4 Standard Demand Response Signals (PAP 09)

Demand Response (DR) communications cover interactions between wholesale markets and retail utilities and aggregators, as well as between these entities and the end-load customers who reduce demand in response to grid reliability or price signals. Given the rapid deployment of smart meters, DR standards are widely acknowledged as a top priority, with a draft DR specification expected by January 2010.

What

While the value of DR is generally well understood, the interaction patterns, semantics, and information conveyed vary. Price (often with the time that the price is effective), grid integrity signals (e.g., event levels of low, medium, high), and possibly environmental signals (e.g., air quality) are components of DR communications. Defining consistent signal semantics for DR will make the information conveyed more consistent across Smart Grid domains.

The swift deployment of smart meters and the integration of distributed energy resources (DER) into the grid require DR standards. As represented in this plan, the focus of the DR standards effort is to integrate the standards work in OpenADR, OpenSG, IEC TC57, and NAESB efforts, along with the input of other stakeholders to deliver a draft DR specification in January 2010. The initial emphasis is on meeting utility DR requirements, while developing an extensible signaling framework that allows continued development of DER semantics.

Why

DR has evolved over the years. Previous mechanisms included calling or paging plant managers to advise them to curtail energy use at their facilities; current mechanisms support varying levels of automation. Technologies such as Open Automated Demand Response (OpenADR) have demonstrated rapid, automated curtailment based on price or grid integrity signals, so that aggregators have a clearer understanding of what loads customer facilities can shed at what times. Unfortunately, lack of widely accepted signals across the entire DR signaling and validation chain hinders widespread deployment of these technologies. Consistent signals will allow further automation and improve DR capabilities across the grid.

Integration of renewable and other intermittent resources increases the need for balancing reserve, spinning reserve, and other techniques to take advantage of lower operating costs for renewable resources. However, the responsiveness of the entire power generation and delivery system needs to improve in correlation with the extent and degree of intermittency. DER integration raises interoperation issues related to distribution automation, signals and information exchanges, and profiles; some of these (e.g. storage) are being addressed specifically in other action plans. Although all domains are affected to some extent, markets, operations, distribution, distribution-related capital costs, and the customer domains are primarily affected.

Major Plan Objectives

- Collect, analyze, and consolidate use cases and gather stakeholder user requirements.
- Define a framework and common terminology (message semantics) for: price communication (including schedules, import from other PAPs); grid safety or integrity signals; DER support; and other signals and/or extensibility mechanism.
- Address safety of interconnection and resale issues.
- Address common vocabulary across existing DR specifications.

Project Team

NIST Lead: David Holmberg

Collaborators:

Association of Home Appliance Manufacturers (AHAM)

American Society of Heating Refrigeration and Air-conditioning Engineers (ASHRAE)

Independent System Operator-Regional Transmission Organization (ISO-RTO) Council (IRC)

California ISO (CAISO)

Electric Power Research Institute (EPRI) (appliances)

GridWise Architecture Council (GWAC)

International Electrotechnical Commission (IEC) TC57 WG14 International Organization for Standardization (ISO)/IEC JTC 1 WG15

Independent System Operator-Regional Transmission Organization (ISO-RTO) Council (IRC)

Lawrence Berkeley National Labs (LBNL) Open Automated Demand Response (OpenADR)

LONMark International

MultiSpeak Initiative

North American Energy Standards Board (NAESB)

Organization for the Advancement of Structured Information Standards (OASIS)

Utility Communications Architecture International Users Group (UCAIug) Advanced Metering Infrastructure Enterprise Task Force (AMI-ENT TF) and Smart Grid Sub-Committee

ZigBee/ HomePlug Smart Energy Profile 2.0 (SEP2)

The full plan can be found at: http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/PAP09DRDER.

5.5 Develop Common Specification for Price and Product Definition (PAP 03)

A common specification for price is critical for applications used across the Smart Grid. The price and product specification development is proceeding on a rapid time scale. A draft specification will be ready in April 2010. This definitive effort is drawing on input from a wide

group of stakeholders as well as existing work. It focuses on meeting the immediate needs of utilities and demand response program mandates while building an extensible foundation for a market-based Smart Grid.

What

Actions under this plan will result in a common specification for price and product definition. This specification will be used in demand response applications, market transactions, distributed energy resource integration, meter communications, and many other inter-domain communications. Businesses, homes, electric vehicles, and the power grid will benefit from automated and timely communication of energy prices, characteristics, quantities, and related information.

Price is a number associated with product characteristics, including delivery schedule, quality (reliability, power quality, source, etc.), and environmental and regulatory characteristics. Price also is a common abstraction for abundance, scarcity, and other market conditions. A common price model will define how to exchange data on energy characteristics, availability, and schedules to support efficient communication of information in any market.

Why

Coordination of energy supply and demand requires a common understanding of supply and demand. A simple quotation of price, quantity, and characteristics in a consistent way across markets enables new markets and integration of distributed energy resources. Price and product definition are key to transparent market accounting.

A consistent information model will reduce implementation costs. A consistent model for market information exchange simplifies communication flow and improves the quality and efficiency of actions taken by energy providers, distributors, and consumers.

Better communication of actionable energy prices facilitates effective dynamic pricing and is necessary for net-zero-energy buildings, supply-demand integration, and other efficiency and sustainability initiatives. Common, up-to-the-moment pricing information is also an enabler of local generation and storage of energy, such as electric-charging and thermal-storage technologies for homes and buildings.

Major Plan Objectives

- Develop a summary of power reliability and quality characteristics that affect price and availability (supply side) and desirability (demand side).
- Survey existing price communications and develop harmonized specification (draft specification by April 2010).
- Engage the broad group of stakeholders into the effort.
- Build on existing work in financial energy markets and existing demand response programs.
- Integrate with schedule and interval specifications under development.

Project Team

NIST Lead: David Holmberg

Collaborators:

Association of Home Appliance Manufacturers (AHAM)

American Society of Heating Refrigeration and Air-conditioning Engineers (ASHRAE)

BAE Systems

Cazalet Group

Financial Information Exchange (FIX) Protocol, Ltd. (FPL)

GridWise Architecture Council (GWAC)

International Electrotechnical Commission (IEC)

Independent System Operator-Regional Transmission Organization (ISO-RTO) Council (IRC)

JP Morgan

Lawrence Berkeley National Labs

LONMark International

Multispeak

North American Energy Standards Board (NAESB)

New England ISO

Organization for the Advancement of Structured Information Standards (OASIS)

The full plan can be found at: http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/PAP03PriceProduct.

5. 6 Develop Common Scheduling Communication for Energy Transactions (PAP 04)

The coordination of supply and demand is already of critical importance on the Smart Grid. With an expected future increase of distributed energy resources, including both distributed energy generation and demand response, this coordination becomes more critical.

What

Already important, coordination of supply and demand in the grid will be critical as distributed energy resources increase and as renewable energy resources account for a growing share of electric power. Beyond electromechanical devices and equipment, it is necessary to coordinate enterprise activities, home operations and family schedules, and market operations. Thus, a

common schedule specification is required for the Smart Grid and the many sectors that interact with the grid.

Under this plan, NIST and collaborators are surveying existing calendaring specifications. They will develop a standard for how schedule and event information is passed between and within services. The output will be a micro-specification that can then be incorporated into price, demand-response, and other specifications. Easy integration of the specification will facilitate a common scheduling operation across different domains and diverse contracts.

A draft is scheduled for completion by the end of April 2010 so that it can be included in the Common Specification for Price and Product Definition plan.

Why

Services operate—and are negotiated—on the basis of schedules. Some services may stem from almost instantaneous transactions while others may require significant lead times and coordination with other services, processes, or actors. Central coordination of such services reduces interoperability, as it requires the coordinating agent to know the lead time of each service. The Smart Grid relies on coordinating processes in homes, offices, and industry with projected and actual power availability, including different prices at different times. In addition, regularly updated weather observations and forecasts are increasingly important to projecting energy availability. Energy use in buildings can be reduced if building-system operations are coordinated with the schedules of the occupants. A common standard for transmitting calendaring information will enable the coordination necessary to improve energy efficiency and overall performance.

In the evolving transactive power grid, market communications will involve energy consumers, producers, and transmission and distribution systems. Coordinated scheduling will enable aggregation for both consumption and curtailment resources. With information in consistent formats, building and facility agents can make decisions about energy production, sale, purchase, and use that fit the goals and requirements of their home, business, or industrial facility.

Major Plan Objectives

- The Calendar Consortium will complete its current work on XML serialization of ICalendar into a Web-service component (WS-Calendar) by early 2010.
- ISO20022 will comment on and coordinate with the Calendar Consortium on schedule semantics across enterprise, energy, and financial information.
- Ongoing work in price and product definition standards development and in grid end node interactions (OASIS Energy Interoperability) will incorporate a schedule component pending completion of this work.

Project Team

NIST Lead: David Holmberg

Collaborators: CalConnect Financial Information Exchange (FIX) Protocol, Ltd. (FPL) International Organization for Standardization (ISO)

North American Energy Standards Board (NAESB)

Organization for the Advancement of Structured Information Standards (OASIS)

Open Standards Consortium for Real Estate (OSCRE)

Pacific Northwest National Laboratory (PNNL)

Software and Information Industry Association (SIIA)

Utility Communications Architecture International Users Group (UCAIug)

The full plan can be found at: http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/PAP04Schedules.

5.7 Guidelines for the Use of IP Protocol Suite in the Smart Grid (PAP 01)

What

Given that Internet technologies play an important role in support of the Smart Grid information networks, it is critical to identify the appropriate Internet standards or Internet Engineering Task Force "requests for comments" (RFCs) that are suitable for use in the context of the Smart Grid. This action plan presents steps for developing guidelines for the use of the IP protocol suite by working with key SDO committees to determine the characteristics of Smart Grid application areas and domain types and the applicable IP protocols that are suitable for use by these applications and domains. The networking standards identified under this action plan will define a significant portion of the interfaces to Smart Grid equipment and systems for both intra-domain and inter-domain applications.

NIST expects the initial guidelines, based on the existing Smart Grid requirements, to be completed by mid-year 2010.

Why

The Smart Grid will use a variety of different networking environments across Smart Grid domains and sub-domains as identified in the Smart Grid applications and conceptual models. The suitability of the proposed protocol suites or profiles in specific application contexts should be analyzed against the requirements emerging for Smart Grid applications and the proposed scale and scope of Smart Grid networks. The analysis should identify which IP-based protocols are clearly applicable in specific application contexts and protocols for network control, management, and security, in addition to identifying any existing gaps.

Major Plan Objectives

- Review Smart Grid use cases and application domains and devise a taxonomy for applications with similar network requirements.
- Define a core suite of IP-based protocols required for Smart Grid networks.
- Identify additional protocols or protocol enhancements beyond the core suite required by specific classes of applications and develop guidelines for IP-based Smart Grid deployment.
- Identify key networking issues, including issues related to addressing, management, security, and those surrounding IPv4 vs. IPv6.

- Determine appropriate Smart Grid network architectures and technologies appropriate for basic transport and security requirements (e.g., shared IP networks, virtual private networks, MPLS switching, traffic engineering, and resource control mechanisms).
- Determine which transport layer security protocol(s) (e.g., TLS, DTLS, SCTP, and IPsec) are most appropriate for securing Smart Grid applications. Identify higher-layer security mechanisms (e.g., XML, S/MIME) to secure transactions.
- Identify new protocol or protocol enhancement standardization activities required to fully support Smart Grid in the future.
- Develop an action plan for development of necessary usage guides, profiles, and remaining work.

Project Team

NIST Lead: David Su

Lead SSO: Internet Engineering Task Force (IETF)

Collaborators:

Alliance for Telecommunications Industry Solutions (ATIS)

Institute of Electrical and Electronic Engineers (IEEE)

National Electrical Manufacturers Association (NEMA)

Telecommunications Industry Association (TIA)

UCA International Users Group (UCAIug)

The full plan can be found at: http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/PAP01InternetProfile.

5.8 Guidelines for the Use of Wireless Communications (PAP 02)

What

Wireless technologies can be used in field environments across the Smart Grid, including generation plants, transmission systems, substations, distribution systems, and customer premises communications. The choice of wireless, type of wireless, or non-wireless must be made with full knowledge of the appropriate use of the technology.

This plan will investigate the use of wireless communications for different Smart Grid applications by assessing the strengths, weaknesses, capabilities, and constraints of existing and emerging standards-based technologies for wireless communications. The approach is to work with key SDO committees to determine the characteristics of each technology for Smart Grid application areas and types. Results will be used in evaluations of the appropriateness of wireless communications technologies for Smart Grid applications.

NIST expects the initial guidelines, based on the existing Smart Grid requirements, to be completed by mid-year 2010.

Why

Wireless technologies are candidates for meeting Smart Grid requirements, especially those for which alternative media are too costly or not workable. However, different types of wireless technologies also have different availability, time sensitivity, and security characteristics that may limit their suitability for certain applications. Therefore, the capabilities and weaknesses of specific wireless technologies must be assessed in all possible conditions of Smart Grid operations. This work includes reviewing existing documentation and ongoing work to assess wireless technologies operating in both licensed and unlicensed bands. This review is necessary before developing guidelines for safe, effective use of wireless technologies in different Smart Grid applications.

Specific tasks include:

1) Segmenting the Smart Grid domains into wireless environments/groups with similar sets of requirements.

2) Developing a common set of terminologies and definitions for use by the wireless and Smart Grid communities.

3) Compiling and communicating Smart Grid requirements and use cases in a standardized format mapped into categories identified in Task 1.

4) Creating an attribute list and performance metrics for wireless standards.

5) Creating an inventory of wireless technologies and standards that are identified by each SDO in accordance with the metrics developed in Task 4.

6) Performing the mapping and conducting an evaluation of the wireless technologies based on the criteria and metrics developed in Task 4 and identify gaps where appropriate.

Major Plan Objectives

- Identify key issues to be addressed in wireless assessments and development for the Smart Grid.

- Identify requirements for use of wireless technologies for different Smart Grid applications.

- Identify approaches to define the strengths and weaknesses of candidate wireless technologies to assist Smart Grid design decisions.

- Analyze both intentional and unintentional interference issues and develop coexistence guidelines for deployment and operation.

- Identify guidelines for effectively, safely, and securely employing wireless technologies for different Smart Grid applications.

Project Team

NIST Lead: David Su

Collaborators:

Alliance for Telecommunications Industry Solutions (ATIS)

Institute of Electrical and Electronic Engineers (IEEE) 802; P2030

Internet Engineering Task Force (IETF)

International Society of Automation (ISA) SP100

Telecommunications Industry Association (TIA)

WiFi Alliance

UCA International Users Group (UCAIug)

Utility Telecom Council (UTC)

ZigBee Alliance

WiMAX Forum

The full plan can be found at: http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/PAP02Wireless.

5.9 Harmonize Power Line Carrier Standards for Appliance Communications in the Home (PAP 15)

What

Several power line-based communications technologies are being considered for appliances, meters, and PEV communications in and across the customer premises. Relevant standards include ITU G.Hn (HomeGrid), IEEE P1901 (HomePlug™), and ANSI/CEA 709.2 (Lonworks™). However, these technologies are currently not interoperable and may not coexist successfully, and their operation in proximity may cause harmful mutual interference. Given the cost, complexity, and physical constraints of the medium, it is imperative that coexistence and some interoperability be achieved. The purpose of this PAP is to achieve that resolution.

Why

Smart home appliances represent a major part of the Smart Grid vision aimed at increasing energy efficiency; to achieve that goal, home appliances need to communicate with entities and players in other Smart Grid domains via home networks. The implementation of such home networks must enable *plug-n-play* of appliances from the same or different vendors, requiring no manual configurations by homeowners.

Power line communications (PLCs) are potential technologies that could be used in home networks; however, the lack of international standard specifications impedes the effective use of

this technology. There are multiple standards being developed by SDOs, but none are currently interoperable.

Thus, a PLC PAP was formed to facilitate the harmonization of different standard specifications currently developed by different SDOs including IEEE and ITU-T. The goal of this PAP is to enable the development of an interoperable profile containing common features for low bit rate applications where the resulting implementation of this profile leads to interoperable products.

Major Plan Objectives

- Determine range of potential acceptable outcomes – coexistence or selection or convergence.
- Agree on an acceptable outcome for achieving coexistence among multiple PLC protocols.
- Formulate a PAP for moving forward.

Project Team

NIST Lead: David Su

SSOs:

Institute of Electrical and Electronic Engineers (IEEE) P1901 and P2030

International Telecommunication Union ITU-T Study Group 15

Collaborators:

Association of Home Appliance Manufactures

Consumer Electronics Powerline Communication Alliance

HD-PLC Alliance

HomeGrid Forum

HomePlug Powerline Alliance

Universal Powerline Association

U-SNAP Alliance

The full plan can be found at: http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/PAP15PLCForLowBitRates.

5.10 Develop Common Information Model (CIM) for Distribution Grid Management (PAP 08)

Standards are urgently needed to enable the rapid integration of wind, solar, and other renewable resources, and to achieve greater reliability and immunity to grid instabilities resulting from wide-scale deployment. A CIM will also create a more reliable and efficient grid. The accelerated timeline calls for creation of an interoperability test team; development of integrated models for Multispeak, a standard that is widely used by rural cooperative electric utilities; and

development of requirements and common models for data and information used in distribution systems and back-office equipment by the end of 2010.

What

This action plan intends to ensure that new Smart Grid equipment for distribution grid operations, currently deploying in many different grid environments, can readily communicate with new and legacy equipment and act on the information exchanged. To ensure the interoperability of new equipment, the strategy calls for defining the key distribution applications that will enable Smart Grid functions for substation automation, integration of distributed energy resources, equipment condition monitoring, and geospatial location; evaluating existing standards; and coordinating the necessary standards development work. This work will enable the integration of data and information from equipment in the distribution grid with information used for enterprise back-office systems.

Efforts are focusing on three standards used in North American distribution systems. The standards differ in the type of data models they use. Their integration will enable many new Smart Grid applications and will lower technical barriers to the implementation of these applications. Currently, none of these standards has a complete data model for distributed energy resources, equipment condition monitoring data, geospatial location, and other information that will underpin Smart Grid technologies and applications. It is critical to act quickly on the initial tasks defined in this action plan since deployments, particularly those funded by the Department of Energy Smart Grid grants and demonstration projects, are under way.

Why

This work is developing an approach for integrating application-level communications from three standards. IEC 61968, which is beginning to be used in the North American grid, and Multispeak, which is widely used by rural cooperative utilities, provide the structure and semantics for integrating a variety of back-office applications. In addition, IEC 61850 defines semantics for communications with substation equipment, including exchanging data on real-time operations as well as nonoperational data, such as for condition monitoring. Integrating these standards provides a basis for powerful integration for both real-time operations for status monitoring and control of substation equipment (circuit breakers, relays, transformers) that will lead to fewer, shorter, or completely prevented outages as well as support for a variety of back-office applications for more efficient and powerful management of equipment assets, validation and analysis of metering data, billing, forecasting, distribution planning and operations that realize the full potential of Smart Grid capabilities.

Major Plan Objectives

- Develop strategies to integrate and expand IEC 61970-301, IEC 61968, Multispeak, and IEC 61850 for Smart Grid applications.
- Create a scalable strategy to integrate other identified standards.

- Evaluate the contents of each standard for a "best fit" to meet the requirements of key applications that span the environments of these standards. Agree on an approach to integrate domain knowledge represented in each standard.

Project Team

NIST Lead: Jerry FitzPatrick

SSO Leads: International Electrotechnical Commission (IEC) TC57 WG14, WG17; MultiSpeak

Collaborators:

International Electrotechnical Commission (IEC) TC57 WG10; TC57 WG13; TC57 WG15; TC57 WG19

Institute of Electrical and Electronic Engineers (IEEE) Power Systems Relay Communications Committee

IEEE Power and Energy Society Distribution Automation Working Group

North American Energy Standards Board (NAESB)

OpenGeospatial Consortium (OGC)
Transmission & Distribution Domain Expert Working Group

Utility Communication Architecture International users' group (UCAIug)

Utilities Standards Board (USB)

The full plan can be found at: http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/PAP08DistrObjMultispeak.

5.11 Transmission and Distribution Power Systems Model Mapping (PAP 14)

Advanced protection, automation, and control applications that will improve the reliability, robustness, and resilience of the power grid are all goals of the Smart Grid. For envisioned applications to meet these goals, information requirements must be identified and standardized to the level necessary to achieve interoperability. Transmission and distribution power system information models defined in existing standards must be modified as needed to meet these requirements. These modifications are expected to be completed by the end of 2010.

What

This plan will define strategies for integrating standards across different utility environments to support various real-time grid operations (relay, circuit breaker, transformer operations) and back-office applications for customer services, meter data and billing, and other business operations. The work must be completed on an aggressive schedule to enable ready interoperability of ongoing Smart Grid deployments funded by federal and industry investments. Modeling of the electric power system, multifunctional Intelligent Electronic Devices (IEDs),

and definition of standard methods for reporting events and exchanging relay settings will enable improving the efficiency of many protection, control, engineering, commissioning, and analysis tasks. Tasks include identifying issues that stand in the way of harmonizing potentially conflicting standards and identifying information requirements for relay settings in the Smart Grid. Some of the tasks identified for this action plan overlap with those in PAP 08 "Develop Common Information Model (CIM) for Distribution Grid Management," and are covered by it as noted in the objectives given below.

Why

Advanced protection, automation, and control applications will benefit from a utility-wide communication infrastructure. Many of today's applications require manual conversion between different proprietary formats. A standards-based approach for system models, protection settings, and event-reporting data exchange will improve the efficiency of many Smart Grid-related tasks. This integration can enable many new applications.

The information requirements of Smart Grid protection, automation, and control applications must be identified and, then, standardized to the level required to achieve interoperability. Use cases describing the applications will be developed, and information needs will be mapped to existing transmission and distribution power system models, which will be extended as required.

This work develops an approach for integrating the application-level communications from several standards. The IEC 61850 standard provides a basis for field equipment communications, including semantics, and encompasses real-time operations as well as nonoperational data, such as condition monitoring. The IEC 61968 and IEC 61970 standards provide the structure and semantics for integrating a variety of back-office applications. Models of the transmission and distribution power system are available in IEC 61970 and IEC 61968-11. Some of the information to be added may be retrieved from devices supporting IEC 61850. An extension of the IEC 61850 models may be required as well.

Automated verification of the different settings of the components of a power system will be essential to preventing system failures due to misconfiguration. To enable these applications across the power system, standardization of protection-setting information is required. Beyond the settings of individual devices, applications also may require more information about the power network, such as line characteristics or topology. The IEEE Power and Energy Society (PES) Power Systems Relaying Committee (PSRC) Working Group H5 is in the process of completing the protection settings object models and defining a common data format for exchange between applications.

Other standards to be considered are IEEE PC37.239, which defines a Standard Common Format for Event Data Exchange (COMFEDE) for Power Systems, and IEEE PC37.237, which defines a Recommended Practice for Time Tagging of Power System Protection Events.

Major Plan Objectives

- Develop strategies to expand and integrate MultiSpeak, IEC 61850, IEC 61968, IEC 61970, IEEE PC37.237 (Time Tagging), IEEE PC37.239 (COMFEDE), and the future IEEE Common Settings File Format for Smart Grid Applications.

- Develop a summary of information required from the power system for various Smart Grid applications. (Covered by the PAP tasks described in Section 5.10.)
- Map that information with the already-defined models from MultiSpeak, IEC 61970, IEC 61968-11, and IEC 61850 (June 2010). (Covered by the PAP tasks described in Section 5.10.)
- Coordinate with the SDOs to extend the existing models. (Covered by the PAP tasks described in Section 5.10.)
- Identify power equipment setting information that is required for performing an automatic verification of the power system configuration to prevent failures due to misconfigurations. This information shall include both settings in the devices as well as parameters of the power network that need to be available for verification.
- Coordinate with SDOs to extend the existing standards to include the necessary setting information (year-end 2010).

Project Team

NIST Lead: Jerry FitzPatrick

Lead SSO: International Electrotechnical Commission (IEC) TC57, WG10

Collaborators:

Electric Power Research Institute (EPRI)

Institute of Electrical and Electronic Engineers (IEEE) PSRC H7; PSRC H5; PSRC H16; PSRC Communications Subcommittee

International Electrotechnical Commission (IEC) TC57 WG13; TC 57 WG14

UCA International Users Group (UCAIug)

The full plan can be found at: http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/PAP14TDModels.

5.12 DNP3 Mapping to IEC 61850 Objects (PAP 12)

DNP3 (the Distributed Network Protocol 3) is the de facto communication protocol used at the distribution and transmission level in the North American power grid. However, DNP3 is not fully capable of enabling all foreseen Smart Grid functions. Nevertheless, the Smart Grid must accommodate and build upon the legacy systems of today's power grid including DNP3 and IEC 61850. Mapping documents, including guidelines for achieving interoperable integration of equipment using DNP3 with equipment using IEC 61850 Smart Grid standards will be completed in 2010.

What

There is an urgent need for distribution and transmission communication networks currently using the legacy DNP3 protocol to support the exchanges of larger volumes of data (with low latency/time delays) necessary to achieve new Smart Grid capabilities. This action plan focuses on developing the means to enable transport of select Smart Grid data and related services over legacy DNP3 networks. This will be accomplished, in part, by defining a method to map the exchange of certain data types and services between DNP3 and the newer IEC 61850 Standard for Communication Networks and Systems in Substations. IEC 61850 is considered to be a standard better suited to support Smart Grid functions. IEC 61850 is a comprehensive standard for substation automation that supports monitoring and control of grid equipment (relays, circuit breakers, transformers) as well as renewable energy resources. Many of the new Smart Grid deployments, including those funded under Department of Energy Smart Grid grants programs, will require rapid, high-bandwidth communications that are better supported by IEC 61850. The tasks of this action plan include performing a gap analysis to identify the extent to which DNP3 meets Smart Grid requirements. Guidelines for achieving interoperable integration of DNP3 with IEC 61850 and other Smart Grid standards will be produced in 2010.

Why

Data acquisition consists of three types of data: binary (digital) inputs, analog inputs, and counters. Supervisory control consists of commands for both digital and analog equipment. DNP3 was designed for low-bandwidth supervisory control and data acquisition (SCADA) operations that control grid equipment. Although this protocol allows any DNP data to be transported between two points, the semantic content of the messages depends upon lists of tables, which are not machine-readable. In addition, mapping of objects in each direction presents difficult challenges. The goal is to ensure that select data are seamlessly transported between devices and readily used by them, even when there are communication constraints imposed by the DNP3 protocol.

Major Plan Objectives

- Agree upon a consistent definition and/or algorithm to map a selected subset of IEC 61850 information objects to corresponding DNP3 data objects (May 2010).
- Provide a method to map between DNP3 data objects and IEC 61850 information objects. Because DNP3 uses less specific semantics than IEC 61850, this is only an approximate mapping. The DNP3 specification (Volume 8 clause 8.4 and its Appendix 1 clause 2) presents the approach recommended by the DNP3 Technical Committee, which uses XML to perform this mapping. This DNP mapping approach is referenced in Annex E of IEC 61400-25-4 (June 2010).
- Define a proposed migration path forward from current DNP only systems to hybrid implementations and ultimately to IEC 61850-only systems.

Project Team

NIST Leads: Jerry FitzPatrick, Tom Nelson

SSO Leads:

Distributed Network Protocol (DNP) Technical Committee

International Electrotechnical Commission (IEC) TC57 WG10

UCA International Users Group (UCAIug) Technical Committee

Collaborators:

Distributed Network Protocol (DNP) User Group

EnerNex Corporation

International Electrotechnical Commission (IEC) TC57 WG03

UCA International Users Group (UCAIug) Testing Committee

Utility Representatives

The full plan can be found at: http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/PAP12DNP361850.

5.13 Harmonization of IEEE C37.118 with IEC 61850 and Precision Time Synchronization (PAP 13)

Synchrophasor measurements are key information needed by system operators to assess the status of the power grid. Using data from Phasor Measurement Units (PMUs), received by phasor data concentrators (PDCs), grid operators will be able to have better visibility of power grid operations and respond to grid disturbances earlier to prevent major blackouts. The current primary standard for the communications of PMU and PDC data and information is the IEEE Standard C37.118, which was published in 2005. This standard also includes requirements for the measurement and determination of phasor values. IEC 61850 is seen as a key standard for all substation and field equipment operating under both real-time and non-real-time applications. The use of IEC 61850 for wide-area communication is discussed in IEC 61850-90-1 (draft technical report) in the context of communication between substations. It appears possible to use a similar approach for the transmission of PMU and PDC data but the capability needs to be formally defined in IEC 61850. This action plan seeks to assist and accelerate the integration of standards that can impact phasor measurement and applications depending on PMU- and PDC-based data and information.

Common time synchronization is the key to many Smart Grid applications for real-time operation necessary to make the Smart Grid highly robust and resilient to disturbances ("self-healing"), either from natural events such as earthquakes or large variations in wind or solar power availability, or from potential terrorist actions. Guidelines on how to achieve that synchronization and addressing different issues related to that synchronization are required. A standard (IEEE 1588) is available to achieve highly accurate synchronization over a communication network; however, an implementation profile for power system applications is required.

What

For the integration of PMU and PDC data based on IEEE C37.118 into IEC 61850, a new work item has already been issued as a joint work item for IEEE and IEC. The work has been circulated within IEC TC57. Within the IEC, a task force as part of working group 10 may be created to support that work from the IEC side. In IEEE, the Power System Relaying Committee (PSRC) H11 Working Group (WG) is responsible for C37.118. These will be the key SDOs for that part of the work. From a procedural viewpoint, the integration of PMU and PDC data into IEC 61850 cannot be considered as an independent standard. Integration will affect several parts of the existing IEC 61850 standard. Therefore, NIST recommends the development of a technical report (similar to IEC 61850-90-1) that addresses all the issues related to the problem. While the final responsibility of the work will be in the joint IEEE/IEC task force, the PAP collaborators will provide technical input to the SDO, will interact with the stakeholders like NASPI, and support demonstration activities.

For time synchronization, this action plan focuses on ensuring that Smart Grid deployments use a common format and have common meaning for time data so that the applications are readily interoperable. The approach will determine detailed requirements for Smart Grid applications and in particular, for synchrophasor measurements used to monitor conditions in the transmission grid. Additionally, the plan tasks cover harmonizing the differences in time data formats used by Smart Grid standards, promoting rapid prototype development and interoperability testing, and developing guidelines on how to achieve uniform time stamping throughout the Smart Grid. Since the IEEE PSRC WG H7 work on developing a profile for accurate time synchronization for power system applications is supported by IEC TC57 WG10, no harmonization is required here. The current activities in the WG are driven on one side by the requirements of PMUs and on the other side by the requirements for accurate synchronization of instrument transformers in a substation that are transmitting sampled values as a stream of data for protection and control applications. The PAP13 WG will interact with the IEEE working group by developing the requirements for the different applications of Smart Grid, by contributing technical work and by supporting demonstration activities. In addition, several other aspects need to be considered like loss of synchronization, dealing with synchronization islands and resynchronization. Calendar models are required. Also, other mechanisms for time synchronization using the global positioning system (GPS) or inter-range instrumentation group (IRIG-B) approaches need to be discussed.

Why

Two standards are related to communications of PMU and PDC data and information. IEEE C37.118 was published in 2005 for PMUs. IEC 61850 has been substantially developed for substations but is seen as a key standard for all field equipment operating under both real-time and non-real-time applications. Integrating IEEE C37.118 with IEC 61850 will help to remove overlaps between the standards, which may impede development of interoperable equipment and systems.

There are significant differences in scope and content of the two standards. IEEE C37.118 includes communication as well as measurement requirements and is also intended to support applications such as protection. IEC 61850 is suitable for system-wide applications that require higher publishing rates. The use of IEC 61850 for wide-area communication is already discussed

in IEC 61850-90-1 (draft technical report) in the context of communication between substations. It appears possible to use a similar approach for the transmission of PMU and PDC data. The approach, including possible models for PMU data, needs to be defined in IEC 61850.

With IEEE 1588, a standard is available to achieve highly accurate synchronization over communication networks. Several applications related to Smart Grid require time synchronization, and many aspects, such as loss of synchronization, dealing with synchronization "islands," and resynchronization after loss, must be considered. Calendar models are required and other mechanisms for time synchronization such as GPS or IRIG-B are considered. A standards-based approach for time synchronization that addresses the requirements from all applications will support interoperability and facilitate implementation of new Smart Grid applications.

Major Plan Objectives

- Develop contributing technical work to integrate IEEE C37.118 and IEC 61850 under a Dual IEEE/IEC Logo Standard (January 2010).
- Participate with SDO working groups to work out technical issues related to the standard integration (ongoing).
- Support prototyping activities (ongoing).
- Facilitate interoperability demonstrations of prototypes (at the next Plugfest).
- Validate detailed requirements from Smart Grid applications using common time synchronization and time management.
- Develop, in cooperation with SDO working groups, guidelines for application and role-based time synchronization.
- Develop contributing technical work to prepare standard profiles for IEEE 1588 (January 2010).
- Ensure NASPI-NET and NERC timing requirements are encompassed by work of this group.
- Resolve differences between time stamp format and time semantic of C37.118 and 61850 (perhaps add a second timestamp to message).

Project Team

NIST Lead: Jerry FitzPatrick

Lead SSOs:

International Electrotechnical Commission (IEC) TC 57 WG 10 6185090

Institute of Electrical and Electronic Engineers (IEEE) Power Systems Relaying Committee (PSRC) H1; PSRC H7*Collaborators:*

Electric Power Research Institute (EPRI)

EnerNex Corporation

International Electrotechnical Commission (IEC) TC57 WG19; TC57 WG15; TC38 WG37

Institute of Electrical and Electronics Engineers (IEEE) Power Systems Relaying Committee (PSRC) H11; PSRC H7; PSRC H3; PSRC Communications Subcommittee, PSRC H4 C37.11 COMTRADE

North American Synchrophasor Initiative (NASPI)

NASPI, Performance and Standards Committee

North American Electric Reliability Corporation (NERC) CSSWG

PJM

Utility Communication Architecture International users' group (UCAIug)

The full plan can be found at: http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/PAP1361850C27118HarmSynch.

5.14 Energy Storage Interconnection Guidelines (PAP 07)

Although still in their infancy, energy storage (ES) technologies will play an increasingly important role in the evolution of the power grid, particularly in providing a solution that will enable large penetration of intermittent renewable energy sources while also enhancing the stability of the grid. Indeed, the Federal Energy Regulatory Commission has identified energy storage as a key Smart Grid functionality[61]. Initial specifications, standards and guidelines for interconnection of ES and ES combined with renewables are planned to be completed by the middle of 2010.

What

Energy storage is required to accommodate the increasing penetration of intermittent renewable energy resources and to improve Electric Power System (EPS) performance. Consistent, uniformly applied interconnection and information model standards, supported by implementation guidelines, are required for energy storage devices (ES), power electronics interconnection of distributed energy resources (DER), hybrid generation-storage systems (ES-DER), and plug-in electric vehicles (PEV) used as storage. A broad set of stakeholders and SDOs have been enlisted to address this need.

Significant progress has been made in meeting the objectives of the Energy Storage PAP. The first draft of a Scoping Document defining interconnection requirements across a broad range of anticipated ES-DER scenarios (including islanding[62]) has been completed and posted on the

[61] Federal Energy Regulatory Commission, Smart Grid Policy, 128 FERC ¶ 61,060 [Docket No. PL09-4-000] July 16, 2009.

[62] Islanding in a DER system can be intentional, such as when a customer disconnects his building from the grid and draws power from his own distributed generator, or unintentional/forced, caused by an outage on the grid. In the latter case, rather than supplying energy to the grid, the distributed generator is isolated from the grid and supplies electricity to power the building.

NIST Smart Grid Collaboration Site. The Scoping Document describes EPS applications of dispatchable ES-DER, multifunctional operational interface capabilities of mechanical generators (rotating machines) and electronic generators (power electronics-based inverters), business and regulatory issues influencing the deployment of ES-DER devices, and emerging storage and power electronics technologies that will influence the timeline for introduction of ES-DER devices. A process has also been initiated to identify and develop ES-DER use cases (UCs), and to prioritize and roadmap the standards development required to meet urgent near-term deployments while ensuring consistency of standards for the broad spectrum of future ES-DER applications.

The Scoping Document and the prioritized timeline for ES-DER applications will expedite the formation of new standards projects for Smart Grid dispatchable ES-DER extensions of the IEEE 1547 series of standards, which define the physical and electrical interconnection of DERs with the grid. The Scoping Document and UCs will also be used by a similar fast-tracking effort focused on defining ES-DER object models in the IEC 61850-7-420 standards to accommodate Smart Grid requirements. Collaborations with UL, SAE, NEC-NFPA70, and CSA also have been initiated to focus on specifications for safe and reliable implementation.

Why

Due to the initial limited applications of the use of power electronics for grid interconnection of ES and DER, there are few standards that exist to capture how it could or should be utilized as a grid-integrated operational asset on the legacy grid and Smart Grid. For example, no standards address grid-specific aspects of aggregating large or small mobile energy storage units, such as Plug-in Electric Vehicles (PEVs). ES-DER is treated as a distributed energy resource in some standards, but there may be distinctions between energy storage and connected generation. In particular, storage systems such as PEVs may function as a load more than half of the time. Interoperability standards must reckon with the diversity in functionality of ES-DER systems.

At the same time, we are moving toward large penetration of renewables into the grid. While desirable, this trend poses grid operational difficulties and stability concerns. First, because of their intermittent nature, renewables are generally unsuitable as a dispatchable resource under the control of the utility. Second, the present interconnection regulations and standards themselves require the DER devices to trip off in response to minor variations in grid voltage or frequency, which may actually increase the underlying disturbance leading to an instability (for large penetration of renewables) as other DER devices trip off in a cascading manner.

ES-DER is being considered as a preferred means of shifting the time that electricity is delivered to better follow the demand, and to eliminate congestion on transmission systems. ES-DER systems based on photovoltaic, wind, and other intermittent/variable renewable energy sources are also exploring the use of storage to help smooth their intermittency, to augment their ability to respond to distribution power grid management requirements, and to compensate for the variability of these resources due, for example, to diurnal cycles of wind and solar energy. Appropriate interconnection standards, Smart Grid communication, and storage are all key elements of the solution that will enable large penetration of renewables while also enhancing rather than diminishing the stability of the grid.

An assortment of ES-DER systems are emerging. They vary in abilities to respond to power grid management requests, and they use different technologies and system parameters for forecasting

their available power generation reserve. Furthermore, the EPS needs for storage (power, energy, duty cycle, and functionality) also depend on the grid domain where the storage is used (e.g., transmission, distribution, and consumer). These considerations need to be included in the storage and hybrid generation-storage interconnection and information model standards.

Major Plan Objectives

- A broad set of stakeholders has been convened to address ES-DER electrical interconnection issues, including utilities from different regions, the international community, groups addressing similar issues (such as wind turbine interconnection), vendors, and researchers.
- A Scoping Document defining interconnection requirements across a broad range of anticipated ES-DER scenarios has been completed and posted on the NIST Smart Grid Collaboration Site. The Scoping Document includes ES-DER interconnection and operational interface requirements for the full spectrum of application issues, including high penetration of ES-DER, ride-through of power system anomalies, plug-in electric vehicles, and all sizes of ES-DER systems, including those at customer sites, within distribution systems, and at transmission level.
- UCs are being identified and developed to prioritize interconnection and object modeling requirements for ES-DER before electrical interconnection standards are developed. Initial UCs have been identified and posted on the NIST Smart Grid Collaboration Site, and a process has been described to develop further UCs and to prioritize and roadmap the standards development required to meet urgent near-term deployments while ensuring consistency of standards for the broad spectrum of future ES-DER applications. Both NEMA and IEEE IGCC (Intelligent Grid Coordinating Committee) have agreed to lead the collection and development of additional ES-DER UCs.
- Update or augment the IEEE 1547 distribution-level standards series, as appropriate, to accommodate the wide range of ES-DER system requirements, including new IEEE SCC21 projects to be initiated in Spring 2010.
- Augment the IEC 61850-7-420 object models for ES-DER based on the project descriptions for IEEE 1547 extensions (to be completed within a few months following the corresponding project descriptions).
- Initiate development of transmission-level standards for ES-DER. These should build on the FERC wind plant interconnect (LGIP) guidelines and European practice (e.g., e-on, ESB).
- Harmonize the distribution and transmission-level standards, where possible.

Project Team

NIST Lead: Al Hefner

SSO Leads:

Institute of Electrical and Electronic Engineers (IEEE) SCC21

International Electrotechnical Commission (IEC) TC57 WG17

Collaborators:

A123Systems

ABB

American Electric Power (AEP)

Altairnano

BuildingSmart

CSA-Standards

DTE Energy

Electric Power Research Institute (EPRI)

Florida Solar Energy Center (FSEC)

GMATC

Institute of Electrical and Electronic Engineers (IEEE)

National Electrical Code (NEC) - National Fire Protection Association (NFPA)

National Electrical Manufacturers Association (NEMA)

Novus Energy

National Renewable Energy Laboratory (NREL)

Oak Ridge National Laboratory (ORNL)

Open Standards Consortium for Real Estate (OSCRE)

SAE International

Satcon

Sandia National Laboratory

S&C

Underwriters Laboratory (UL)

The full description of PAP 7 can be found at the following link:
http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/PAP07Storage.

5.15 Interoperability Standards to Support Plug-in Electric Vehicles (PAP 11)

Interoperability standards that will define data standards to enable the charging of plug-in electric vehicles (PEVs) will support the adoption of PEVs and related benefits. Standards are anticipated to be available by the end of 2010.

What

This action plan will define data standards to enable the charging of plug-in electric vehicles (PEVs). The specifications will cover charging at home or away from home using a special rate schedule, discharging of PEV energy storage for demand response purposes, and administration and monitoring. The standards will allow the charging flexibility necessary for PEVs to meet customer needs. They also will encourage the adoption of electric vehicles for general-purpose transportation. This anticipated trend would favorably affect the nation's energy portfolio. The standards developed under this action plan will benefit electric utilities by supporting charging during off-peak, low-demand periods and enabling energy stored in PEVs to be returned to the grid during high-demand periods. The objectives described below are expected to be completed by December 2010.

These standards must be developed on an aggressive timetable. One of the cornerstones of the current administration's energy policy is to encourage PEV manufacturing and use to reduce the nation's dependence on foreign oil. Goals include 1 million plug-in hybrid and electric vehicles on U.S. roads by 2015.[63] Achieving this goal requires implementing the charging infrastructure prior to this date. Additionally, auto manufacturers must have some confidence that the necessary charging infrastructure will be established before they can justify developing and producing these vehicles on a large scale.

Why

Hybrid and electric vehicle owners will need to charge their vehicles, both at home and at sites along their local and extended travels. These travels might take them to work, to the grocery store, or on a cross-country trip. PEVs have the potential to significantly burden utilities. They also have the ability to be used as strategically important energy storage assets that can smooth out power demand. By providing intelligent charging capabilities and giving customers the control and the price incentives to charge during off-peak hours and to return stored power during periods of high demand, the nation can better leverage existing resources to support this new source of load and distributed storage.

Major Plan Objectives

- Gather and normalize all the existing use cases and derive requirements so that each element of prospective standards meets a particular stakeholder need, by early 2010.
- Draft common high-level information models in Unified Modeling Language (UML) to be used as a basis for specific models needed for different SDO projects (to be completed by February 2010).
- Facilitate productive collaboration among the many different SDOs involved in the PEV infrastructure. These SDOs represent a variety of domains and, traditionally, most have not

[63] http://www.whitehouse.gov/the_press_office/President-Obama-Announces-24-Billion-in-Funding-to-Support-Next-Generation-Electric-Vehicles

worked together. Currently, there are few—or no—mechanisms for the different standards groups to work together.

- Once the common high-level model is developed in the objective in the second bullet above, specific implementation models must be developed for each standard. The common UML model will be used to create this standards-specific view of the model for IEC 61968/61850. These standards-specific implementation models will form the basis for the standards documents (to be completed by December 2010).
- Identify regulatory impediments to achieving the goals defined in the PEV use cases. Review the current regulatory/use case conflicts to determine areas where changes are needed; advise regulatory bodies of the identified obstacles and develop options for solutions (to be completed by April 2010).
- Ensure that other standards involving safety, interconnection, and certification support the PEV use cases (to be completed by April 2010).

Project Team

NIST lead: Eric Simmon

Lead SSO: SAE International

Collaborators:

American National Standards Institute (ANSI)

International Electrotechnical Commission (IEC) 61850; 61970/61968)

Institute of Electrical and Electronic Engineers (IEEE)

National Electrical Manufacturers Association (NEMA)

ZigBee

The full plan can be found at: http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/PAP11PEV.

6 Cyber Security Strategy[64]

With the implementation of the Smart Grid, the information technology (IT) and telecommunications infrastructures have become more important to ensure the reliability and security of the electric sector. Therefore, the security of systems and information in the IT and telecommunications infrastructures must also be addressed by an increasingly diverse electric sector. Security must be included at the design phase to ensure adequate protection.

Cyber security must address not only deliberate attacks, such as from disgruntled employees, industrial espionage, and terrorists, but also inadvertent compromises of the information infrastructure due to user errors, equipment failures, and natural disasters. Vulnerabilities might allow an attacker to penetrate a network, gain access to control software, and alter load conditions to destabilize the grid in unpredictable ways. The need to address potential vulnerabilities has been acknowledged across the federal government, including NIST[65], the Department of Homeland Security (DHS),[66] DOE,[67] and FERC.[68]

Additional risks to the grid include:

- Increasing the complexity of the grid could introduce vulnerabilities and increase exposure to potential attackers and unintentional errors;
- Interconnected networks can introduce common vulnerabilities;
- Increasing vulnerabilities to communication disruptions and introduction of malicious software could result in denial of service or compromise the integrity of software and systems;
- Increased number of entry points and paths for potential adversaries to exploit; and
- Potential for compromise of data confidentiality, including the breach of customer privacy.

[64] This section is extracted from NISTIR 7628, *Smart Grid Cyber Security Strategy and Requirements*. NISTIR 7628 provides all the supporting material used in selecting and tailoring the cyber security requirements for the Smart Grid. The NISTIR is a companion document to this framework.

[65] Testimony of Cita M. Furlani, Director, Information Technology Laboratory, NIST, before the United States House of Representatives Homeland Security Subcommittee on Emerging Threats, Cyber security, and Science and Technology, March 24, 2009.

[66] Statement for the Record, Sean P.McGurk, Director, Control Systems Security Program, National Cyber Security Division, National Protection and Programs Directorate, Department of Homeland Security, before the U.S. House of Representatives Homeland Security Subcommittee on Emerging Threats, Cyber security, and Science and Technology, March 24, 2009.

[67] U.S. Department of Energy, Office of Electricity Delivery and Energy Reliability, Smart Grid investment Grant Program, Funding Opportunity: DE-FOA-0000058, Electricity Delivery and Energy Reliability Research, Development and Analysis, June 25, 2009.

[68] Federal Energy Regulatory Commission, Smart Grid Policy, 128 FERC ¶ 61,060 [Docket No. PL09-4-000] July 16, 2009.

With the ongoing transition to the Smart Grid, the IT and telecommunication sectors will be more directly involved. These sectors have existing cyber security standards to address vulnerabilities and assessment programs to identify known vulnerabilities in their systems. These same vulnerabilities need to be assessed in the context of the Smart Grid infrastructure. In addition, the Smart Grid will have additional vulnerabilities due to its complexity, large number of stakeholders, and highly time-sensitive operational requirements.

NIST leads a Smart Grid Cyber Security Coordination Task Group (CSCTG), which now has more than 300 volunteer members from the public and private sectors, academia, regulatory organizations, and federal agencies. Cyber security is being addressed using a thorough process that will result in a comprehensive set of cyber security requirements. As explained more fully later in this chapter, the cyber security requirements are being developed using a high-level risk assessment process. NIST has published a preliminary report, NIST Interagency Report (NISTIR) 7628 *Smart Grid Cyber Security Strategy and Requirements*[69] that describes the CSCTG's overall cyber security strategy for the Smart Grid. The preliminary report distills use cases collected to date, requirements and vulnerability classes identified in other relevant cyber security assessments and scoping documents, and other information necessary for specifying and tailoring security requirements to provide adequate protection for the Smart Grid. The requirements included in the NIST report will form the basis for the standards and guidelines developed with coordination by NIST and the Smart Grid Interoperability Panel (SGIP). The document is summarized below.

6.1 Cyber Security and the Electric Sector

The critical role of cyber security in ensuring the effective operation of the Smart Grid is documented in legislation and in the Department of Energy (DOE) Energy Sector Plan.

Section 1301 0f the Energy Independence and Security Act of 2007 (P.L. 110-140) states that, "It is the policy of the United States to support the modernization of the Nation's electricity transmission and distribution system to maintain a reliable and secure electricity infrastructure that can meet future demand growth and to achieve each of the following, which together characterize a Smart Grid:

1. Increased use of digital information and controls technology to improve reliability, security, and efficiency of the electric grid.
2. Dynamic optimization of grid operations and resources, with full cyber-security. ...."

Cyber security for the Smart Grid supports both the reliability of the grid and the confidentiality of the information that is transmitted.

DOE's *Energy Sector-Specific Plan*[70] "envisions a robust, resilient energy infrastructure in which continuity of business and services is maintained through secure and reliable information sharing, effective risk management programs, coordinated response capabilities, and trusted

[69] The document is available at: http://csrc.nist.gov/publications/PubsDrafts.html#NIST-IR-7628

[70] Department of Energy, *Energy, Critical Infrastructure and Key Resources, Sector-Specific Plan as input to the National Infrastructure Protection Plan*, May 2007

relationships between public and private security partners at all levels of industry and government."

6.2 Scope and Definitions

The following definition of cyber infrastructure from the National Infrastructure Protection Plan (NIPP) is included to ensure a common understanding.

- **Cyber Infrastructure:** Includes electronic information and communications systems and services and the information contained in these systems and services. Information and communications systems and services are composed of all hardware and software that process, store, and communicate information, or any combination of all of these elements. Processing includes the creation, access, modification, and destruction of information. Storage includes paper, magnetic, electronic, and all other media types. Communications include sharing and distribution of information. For example: computer systems; control systems (e.g., SCADA); networks, such as the Internet; and cyber services (e.g., managed security services) are part of cyber infrastructure.

A traditional IT-focused understanding of cyber security is that it is the protection required to ensure confidentiality, integrity, and availability of the electronic information communication system. For the Smart Grid, this definition of cyber security needs to be more inclusive. Cyber security in the Smart Grid includes both power and cyber system technologies and processes in IT and power system operations and governance. These technologies and processes provide the protection required to ensure confidentiality, integrity, and availability of the Smart Grid cyber infrastructure, including, for example, control systems, sensors, and actuators.

As described below, NISTIR 7628 provides guidance to organizations that are addressing cyber security for the Smart Grid, e.g., utilities, regulators, power equipment manufacturers and vendors, retail service providers, and electricity and financial market traders. The NIST report provides background information on the analysis process that was used to select and tailor a set of security requirements applicable to the Smart Grid. The process includes both top-down and bottom-up approaches in the selection and tailoring of security requirements for the Smart Grid. The bottom-up approach focuses on identifying vulnerability classes, for example, buffer overflow and protocol errors. The top-down approach focuses on defining components/domains of the Smart Grid system and the logical interfaces between these components/domains. To reduce the complexity, the logical interfaces are organized into logical interface categories. The inter-component/domain security requirements are specified for these logical interface categories based on the interactions between the components and domains. For example, for the AMI system, some of the security requirements are authentication of the meter to the collector, confidentiality for privacy protection, and integrity for firmware updates.

Finally, the NIST report focuses on Smart Grid operations and not on enterprise operations.

6.3 Smart Grid Cyber Security Strategy

The overall cyber security strategy for the Smart Grid examines both domain-specific and common requirements when developing a mitigation strategy to ensure interoperability of

solutions across different parts of the infrastructure. The primary goal of the cyber security strategy should be on prevention. However, it also requires that a response and recovery strategy be developed in the event of a cyber attack on the electric system.

Implementation of a cyber security strategy requires the definition and implementation of an overall cyber security risk assessment process for the Smart Grid. Risk is the potential for an unwanted outcome resulting from an incident, event, or occurrence, as determined by its likelihood and the associated impacts. This type of risk is one component of organizational risk. Organizational risk can include many types of risk (e.g., investment risk, budgetary risk, program management risk, legal liability risk, safety risk, inventory risk, and the risk from information systems). The Smart Grid risk assessment process is based on existing risk assessment approaches developed by both the private and public sectors and includes identifying impact, vulnerability, and threat information to produce an assessment of risk to the Smart Grid and to its domains and sub-domains, such as homes and businesses. Because the Smart Grid includes systems from the IT, telecommunications, and energy sectors, the risk assessment process is applied to all three sectors as they interact in the Smart Grid.

The following documents were used in developing the risk assessment for the Smart Grid:

- National Institute of Standards and Technology (NIST) Special Publication (SP), 800-39, *DRAFT Managing Risk from Information Systems: An Organizational Perspective*, April 2008;
- Federal Information Processing Standard (FIPS) 200, *Minimum Security Requirements for Federal Information and Information Systems,* March 2006;
- FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems,* February 2004;
- North American Electric Reliability Corporation (NERC), *Security Guidelines for the Electricity Sector: Vulnerability and Risk Assessment*, 2002;
- *The National Infrastructure Protection Plan*, 2009;
- The IT, telecommunications, and energy sectors sector-specific plans (SSPs), initially published in 2007 and updated annually; and
- ANSI/ISA-99, *Manufacturing and Control Systems Security, Part 1: Concepts, Models and Terminology*, 2007 and *Part 2: Establishing a Manufacturing and Control Systems Security Program,* 2009.

Following the risk assessment, the next step in the Smart Grid cyber security strategy is to select and tailor (as necessary) the security requirements. The documents used in this step are listed under Task 3 below.

The security requirements and the supporting analysis that are included in the NIST report may be used by implementers of the Smart Grid, e.g., utilities, equipment manufacturers, regulators, as input to their risk assessment processes. The information serves as baseline guidance to the various organizations for assessing risk and selecting appropriate security requirements. In addition, each organization should develop its own cyber security strategy for the Smart Grid.

The tasks within the cyber security strategy for the Smart Grid are undertaken by participants in the CSCTG. In addition, the CSCTG is coordinating activities with the Advanced Security Acceleration Project – Smart Grid (ASAP-SG). The ASAP-SG is a collaborative effort between EnerNex Corporation, multiple major North American utilities, the National Institute of Standards and Technology, and the United States Department of Energy (DOE), including resources from Oak Ridge National Laboratory and the Software Engineering Institute of Carnegie Mellon University. Following are the tasks that are being performed by the CSCTG in the implementation of the cyber security strategy. Also included are the deliverables for each task. Because of the time frame for developing the document, the tasks listed below are occurring in parallel, with significant interactions among the groups addressing the tasks.

Figure 6-1 illustrates the tasks defined for the Smart Grid cyber security strategy. The tasks are defined after the figure.

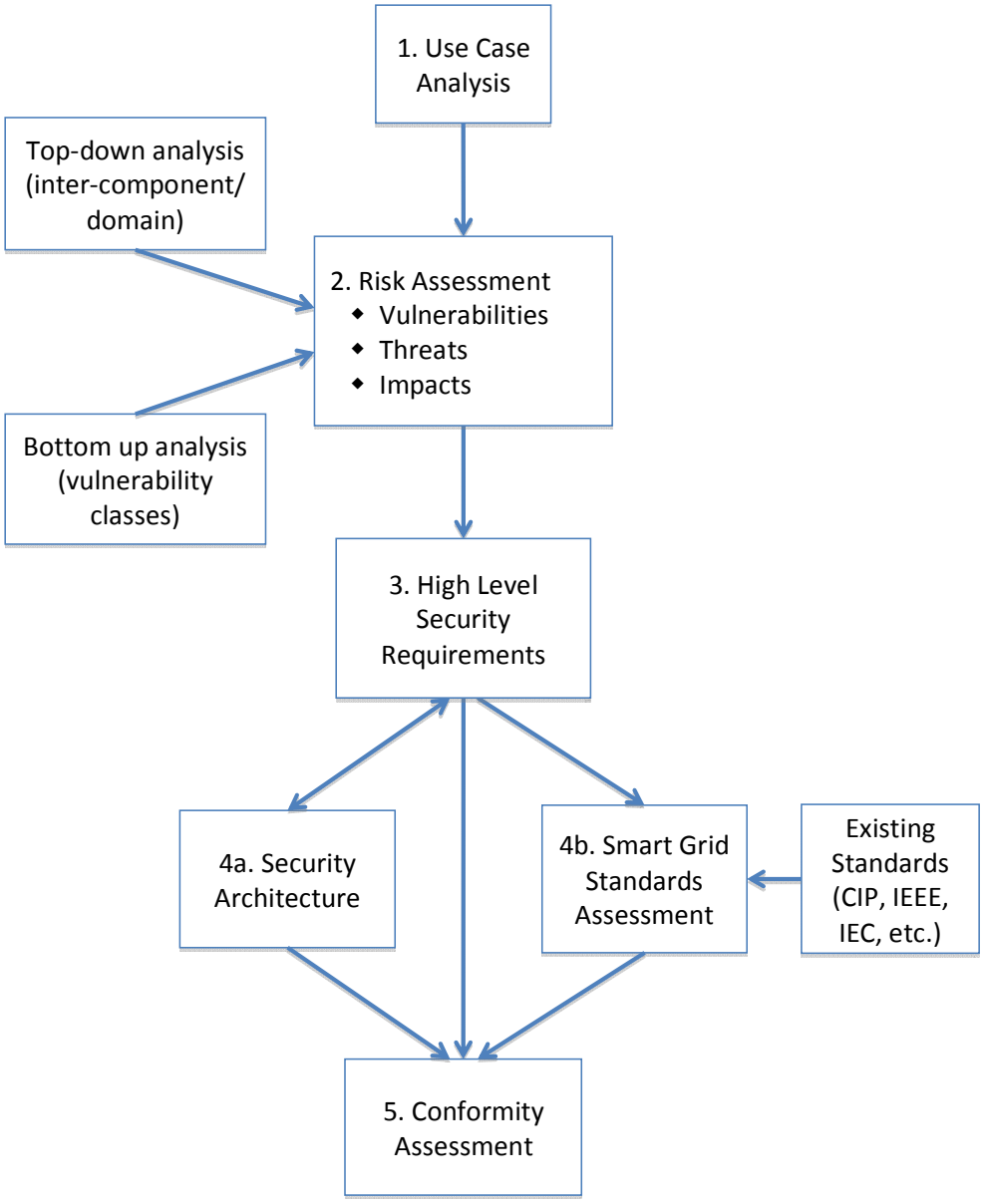


Figure 6-1. Tasks in the Smart Grid Cyber Security Strategy.

Task 1. Selection of use cases with cyber security considerations.[71]

The use cases were selected from several existing sources, e.g., Intelligrid[SM], Electric Power Research Institute (EPRI), and Southern California Edison (SCE). The set of use cases provides a common framework for performing the risk assessment, developing the security architecture, and selecting and tailoring the security requirements.

Task 2. Performance of a risk assessment

The risk assessment, including identifying vulnerabilities, impacts, and threats, has been undertaken from a high-level overall functional perspective. The output will form a basis for the selection of security requirements and the identification of security requirements gaps. The initial draft list of vulnerability classes[72] was developed using information from several existing documents and Web sites, e.g., NIST SP 800-82 and the Open Web Application Security Project (OWASP) vulnerabilities list. These vulnerability classes will ensure that the security controls address the identified vulnerabilities. The vulnerability classes may also be used by Smart Grid implementers, e.g., vendors and utilities, in assessing their systems. Both top-down and bottom-up approaches are used in implementing the risk assessment as specified earlier. The top-down approach focuses on the use cases and the overall Smart Grid functionality. The bottom-up approach focuses on well-understood problems that need to be addressed, such as authenticating and authorizing users to substation IEDs, key management for meters, and intrusion detection for power equipment. Also, interdependencies among Smart Grid domains/systems will be considered when evaluating the impacts of a cyber or physical security incident. An incident in one infrastructure can cascade to failures in other domains/systems.

In the top-down approach, logical interface diagrams were developed for the six functional priority areas that were the focus of the initial draft of NISTIR 7628: Electric Transportation, Electric Storage, Wide Area Situational Awareness, Demand Response, Advanced Metering Infrastructure, and Distribution Grid Management. In the next draft of the NIST report, a functional architecture for the overall Smart Grid will be included, with logical interfaces identified for the new areas (this will be used in the development of the security architecture). Because there are hundreds of interfaces, each logical interface is allocated to one of eighteen logical interface categories. Some examples are: control systems with high data accuracy and high availability, as well as media and computer constraints; B2B (Business to Business) connections, interfaces between sensor networks and controls systems; and interface to the customer site. A set of attributes, e.g., immature or proprietary protocols, insecure locations, integrity requirements, was defined, and the attributes are allocated to the interface categories, as appropriate. This logical interface category/attributes matrix is used in assessing the impact of a security compromise on confidentiality, integrity and availability. The level of impact is denoted

[71] A use case is a method of documenting applications and processes for purposes of defining requirements.

[72] A *vulnerability* is a weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source. A vulnerability class is a grouping of common vulnerabilities.

as low, moderate, or high[73]. This assessment is performed for each logical interface category. The output from this process is used in the selection of security requirements (Task 3).

Task 3. Specification of high level security requirements.

There are many requirements documents that may be applicable to the Smart Grid. Currently, only the North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) standards are mandatory for the bulk electric system. The following documents have been identified by members of the CSCTG as having security requirements relevant to one or more aspects of the Smart Grid.

The following standards are directly relevant to the Smart Grid:

- NERC CIP 002, 003-009
- IEEE 1686-2007, *IEEE Standard for Substation Intelligent Electronic Devices (IEDs) Cyber Security Capabilities*
- *Security Profile for Advanced Metering Infrastructure*, v 1.0, Advanced Security Acceleration Project – Smart Grid, December 10, 2009
- *UtilityAMI Home Area Network System Requirements Specification*, 2008
- IEC 62351 1-8, Power System Control and Associated Communications - Data and Communication Security

The following documents are applicable to control systems:

- ANSI/ISA-99, *Manufacturing and Control Systems Security, Part 1: Concepts, Models and Terminology* and *Part 2: Establishing a Manufacturing and Control Systems Security Program*
- NIST Special Publication (SP) 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems,* August 2009
- NIST SP 800-82, *DRAFT Guide to Industrial Control Systems (ICS) Security*, Sept. 2008
- DHS Procurement Language for Control Systems [74]

[73] The definitions of low, moderate, and high impact may be found in FIPS 199.

[74] Cyber Security Procurement Language for Control Systems, Version 1.8, Department of Homeland Security, National Cyber Security Division, February 2008.

- *Catalog of Control Systems Security: Recommendations for Standards Developers*, Department of Homeland Security, 2009

- ISA SP100, *Wireless Standards*

The cyber security requirements in the documents listed above are not unique. To assist in assessing and selecting the requirements, a cross-reference matrix was developed. This matrix maps the requirements from the various documents listed above. The matrix will be used to select the security requirements that will be listed for each logical interface category. In addition, there are many security requirements that are common to all the logical interface categories. The majority of these requirements are for governance, risk and compliance. These common requirements will be listed in a separate table, rather than being assigned to each logical interface category. As noted above, these requirements lists are provided as guidance, and are not mandatory. Each organization will need to perform a risk assessment to determine the applicability of the recommended requirements.

In addition, organizations may find it necessary to identify compensating security requirements. A compensating security requirement is implemented by an organization in lieu of a recommended security requirement to provide an equivalent or comparable level of protection for the information/control system and the information processed, stored, or transmitted by that system. More than one compensating requirement may be required to provide the equivalent or comparable protection for a particular security requirement. For example, an organization with significant staff limitations may compensate for the recommended separation of duty security requirement by strengthening the audit, accountability, and personnel security requirements within the information/control system.

Finally, for decades, power system operations have been managing the reliability of the power grid in which power *availability* has been a major requirement, with information integrity as a secondary but increasingly critical requirement. Confidentiality of customer information is also important in the normal revenue billing processes. Although focused on accidental/inadvertent security problems, such as equipment failures, employee errors, and natural disasters, existing power system management technologies can be used and expanded to provide additional security measures.

Task 4a. Development of a security architecture.

As specified in Task 2 above, the first phase in this task is to assess and revise the six functional priority area diagrams. The additional functionality of the Smart Grid will be included in an overall functional architecture that includes the six functional priority areas. This functional architecture will be included in the second draft of NISTIR 7628.

Using the conceptual model included in this framework document, the FERC priority area use case diagrams, and the additional areas of AMI and distribution grid management, the CSCTG developed a more granular functional architecture for the Smart Grid. This architecture consolidates the individual FERC priority area diagrams into a single diagram and expands upon the conceptual model. The functional architecture identifies logical communication interfaces between actors. This functional architecture will be submitted to the SGIP Architecture Committee for its use.

In the next phase of this task, the Smart Grid conceptual reference model (described in Chapter 3) and the functional architecture will be used in developing a single Smart Grid security architecture. The Smart Grid security architecture will overlay the security requirements on this architecture. The objective is to ensure that cyber security is addressed as a critical cross-cutting requirement of the Smart Grid.

Task 4b. Assessment of Smart Grid standards.

In Task 4b, standards that have been identified as relevant to the Smart Grid by the Priority Action Plan (PAP) teams and the SGIP will be assessed to determine if the security requirements are addressed. In this process, security requirement gaps will be identified and recommendations will be made for addressing the gaps. Also, conflicting standards and standards with security requirements not consistent with the security requirements included in NISTIR 7628 will be identified with recommendations.

Task 5. Conformity Assessment.

The final task is to develop a conformity assessment program for security requirements. This program will be coordinated with the activities defined by the testing and certification standing committee of the Smart Grid Interoperability Panel. This task will be initiated in the spring of 2010.

6.4 Time Line and Deliverables

Anticipated to be published in January 2010, a second draft of NISTIR 7628 will include an overall Smart Grid architecture, security requirements for all domains of the Smart Grid, and a Smart Grid cyber security research and development section. The second draft will also address the comments that were submitted in response to the first public draft. The January 2010 draft of NISTIR 7628 will be submitted for public review and comment for 60 days. The final draft of the first version of NISTIR 7628, scheduled to be published in spring of 2010, will address all comments submitted to date, and will include an overall security architecture and design consideration to assist individuals and organizations in using the document. Because the Smart Grid is evolving over time, the content of NISTIR 7628 will need to be reviewed and updated, as required.

7 Next Steps

7.1 Phase II – Smart Grid Interoperability Panel

The Release 1.0 Framework described in this document represents an important first step in establishing the standards needed to realize a secure and interoperable Smart Grid. However it is only the beginning of an ongoing process. Initiating Phase II of the Plan in November 2009, NIST's contractor, Enernex, established the Smart Grid Interoperability Standards Panel (SGIP) to provide a more permanent process with stakeholder representation in order to support the ongoing evolution of the Smart Grid Interoperability Framework; to identify and address additional gaps, reflect changes in technology and requirements in the standards; and to provide ongoing coordination of SSO efforts to support timely availability of new or revised Smart Grid standards. Comprehensive information on the stakeholder make up of the SGIP, its meetings, and its findings is available at the NIST Smart Grid Collaboration Site.[75]

7.2 Smart Grid Conformity Testing

NIST recognizes the importance of ensuring the development of a conformity assessment program for Smart Grid (SG) standards. In order to support interoperability of Smart Grid systems and products, Smart Grid products developed to conform to the interoperability framework should undergo a rigorous standards conformity and interoperability testing process. NIST has initiated a program to develop a Smart Grid Conformity Testing Framework which will be further refined and maintained by the Smart Grid Interoperability Panel. Within NIST's three-phase plan to expedite the acceleration of interoperable Smart Grid standards, Smart Grid Conformity Testing is designated as Phase III. In recognition of the importance of Smart Grid Conformity Testing and the need to couple to standards identified for the Smart Grid, Smart Grid Conformity Testing has been included in the work of the SGIP, including establishing a permanent Testing and Certification standing committee within the SGIP.

In today's standards environment, NIST understands the importance of eliminating duplication of work activities related to Smart Grid standards as well as conformity testing. Recognizing that some efforts exist today to test certain Smart Grid standards, and others are under way, NIST's intention is to leverage existing programs wherever practical. Hence the first step in developing a Smart Grid Conformity Testing Framework is to perform an analysis of existing SG standards conformity testing programs. An in-depth study has been initiated to identify and describe existing conformity assessment programs for Smart Grid products and services based on standards and specifications identified in the NIST Framework and Roadmap Document. This survey will address, in particular, conformity assessment programs assuring interoperability, cyber security, and other relevant characteristics. Descriptions of these programs will include all elements of a conformity assessment system, including accreditation bodies, certification bodies, testing and calibration laboratories, inspection bodies, personnel certification programs, and

[75] http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/WebHome.

quality registrars. The study will also identify present gaps and deficiencies in these existing conformity assessment programs.

In addition, a report outlining the conformity assessment requirements of federal and state governments and other relevant SG stakeholders will be developed.

The results of this study will provide an input to the SGIP's Testing and Certification Committee. The SGIP Testing and Certification Committee will have continuing visibility of Smart Grid conformity testing and certification existing in the industry; recommend improvements and means to fill gaps; and work with current standards bodies and user groups to develop new test programs to fill voids.

Feedback from SDOs and other relevant bodies is another important aspect of the Smart Grid Conformity Testing Framework. Errors, clarifications, and enhancements are typically identified to existing standards throughout the normal conformity testing process. In order to improve interoperability, an overall process is critical to ensure changes and enhancements are incorporated continuously.

NIST expects that the first Conformity Assessment Framework Organizational Coordination Meeting will be held within the SGIP by February 22, 2010. Invited attendees will include the Smart Grid stakeholders but the meeting will be open and advertised to the general public.

7.3 Other Issues to be Addressed

This section describes other major standards-related issues and barriers impacting standardization efforts and progress toward a fully interoperable Smart Grid.

7.3.1 Electromagnetic Disturbances

Standards for the Smart Grid should consider electromagnetic disturbances, including severe solar (geomagnetic) storm risks and Intentional Electromagnetic Interference (IEMI) threats such as High-Altitude Electromagnetic Pulse (HEMP).

Our modern high-tech society is built upon a foundation vulnerable to electromagnetic disturbances. The Congressional EMP Commission (CEMPC; http://www.empcommission.org/) has documented some of the electromagnetic-disturbance-based risks and threats to critical U.S national infrastructures, including the electric power grid upon which other infrastructures depend. These threats include IEMI such as HEMP weapons, as well as Geomagnetically-induced currents (GIC) due to severe solar storms. The existence and potential impacts of such threats provide impetus to evaluate, prioritize, and protect/harden the new Smart Grid. Efforts within the Smart Grid Interoperability Panel should be initiated to 1) evaluate the applicability of existing IEC, IEEE (and other relevant bodies), and MIL EMP protection standards, and 2) propose revisions to help address Smart Grid-directed threats.

7.3.2 Electromagnetic Interference

The burgeoning of communications technologies, both wired and wireless, used by Smart Grid equipment can lead to EMC interference, which represents another standards issue requiring study. Additionally, new options may be considered, such as the Utility Telecom Council's proposal for the allocation of dedicated spectra for utility communications. Support of multiple standards is appropriate to meet different real-world requirements and coincides with Congress's requirement that the NIST Interoperability Framework be technology-neutral to encourage innovation. However, some communications technologies perform better in some environments than others, and little guidance is available to utilities to inform their technology choices. NIST identified the potential for wireless interference with equipment operating in unlicensed frequencies as an important issue for study. NIST is working with the FCC and DOE to address this potential issue; further research may result in development of recommendations and guidance on appropriate standards and technologies for wireless smart meter communications. The research goals will be to clearly identify and evaluate potential interference issues, to offer the best technical guidance, if needed, to mitigate interference, and to fill any standards gaps identified.

Regardless of the outcome of these studies, there is no intention to mandate the use of specific spectra (licensed or unlicensed) or the use of specific wireless technologies for Smart Grid equipment. Thus, all current systems, as well as all systems under development, which fully comply with FCC requirements, will be allowed.

In addition to the wireless transmitters discussed above, electromagnetic interference sources include electrostatic discharge, fast transients, and surges, which can lead to interruptions of service. The ability to withstand this interference with sufficient immunity without causing interference to other devices or systems is generally termed electromagnetic compatibility (EMC). There are significant benefits, including minimizing overall costs, to incorporating EMC up front in system development through modeling, simulation, and testing to appropriate standards, including those standards discussed in Section 7.3.1. EMC standards and testing issues relating to the Smart Grid should be addressed within the Smart Grid Interoperability Panel.

7.3.3 Privacy Issues in the Smart Grid

This section summarizes the privacy section included in NISTIR 7628. The benefits anticipated by Smart Grid systems also come with privacy risks that must be addressed. The Smart Grid will be not only an energy management system, but also a multi-directional always "online" communication network. Since the privacy implications of the Smart Grid are still evolving, the Privacy Sub-group of the Cyber Security Coordination Task Group (CSCTG) conducted an initial Privacy Impact Assessment (PIA) for the consumer-to-utility portion of the Smart Grid, as well as taking a broad look at the laws, regulations, and standards relevant to the privacy of information related to consumers' use of electricity. The results of this analysis and the proposed next steps are included in NISTIR 7628.

The PIA analysis was performed following a methodology built around a number of internationally accepted privacy principles including, but not limited to, the American Institute of Certified Public Accountants/Canadian Institute of Chartered Accountants (AICPA/CICA)

Generally Accepted Privacy Principles (GAPPs) and the Organization for Economic Cooperation and Development (OECD) Privacy Principles upon which most international, national, and local data protection laws are based. In addition to these important privacy guidance documents, other privacy aspects, as referenced within the International Organization for Standardization/ International Electrotechnical Commission (ISO/IEC) standards, used by various privacy advocacy groups, in addition to various industry standards and regulations, were taken into consideration.[76] Under GAPP, privacy is defined as "the rights and obligations of individuals and organizations with respect to the collection, use, retention, and disclosure of personal information."[77] The categories of privacy principles used within the PIA methodology included: management and accountability; notice and purpose; choice and consent; collection and scope; use and retention; individual access; disclosure and limiting use; security and safeguards; accuracy and quality; and openness, monitoring, and challenging compliance.

The PIA findings revealed that a lack of consistent and comprehensive privacy policies, standards, and supporting procedures throughout the states, government agencies, utility companies, and supporting entities that will be involved with Smart Grid management, information collection, and use creates a very significant privacy risk that must be addressed.

The ability to access, analyze, and respond to a much wider range of data from all levels of the electric grid is a major benefit of the Smart Grid, but it is also a significant concern from a privacy viewpoint, particularly when the data, resulting analysis and assumptions, are associated with individual consumers or dwellings. Some privacy advocates have raised serious concerns[78] about the type and amount of billing, usage, appliance, and other related information flowing throughout the various components of the Smart Grid.

The privacy implications of frequent meter readings being fed into the Smart Grid networks could provide a detailed time line of activities occurring inside the home. This data may point to a specific individual or give away privacy sensitive data.

The constant collection and use of smart meter data has also raised potential surveillance possibilities posing physical, financial, and reputational risks that must be addressed. Many more types of data are being collected, generated and aggregated within the Smart Grid than when the only data collected was through monthly meter readings by the homeowner or utility employee. Numerous additional entities outside of the energy industry may also be collecting, accessing, and using the data, such as entities that are creating applications and services specifically for smart appliances, smart meters and other yet-to-be-identified purposes. Additionally, privacy issues arise from the question of the legal ownership of the data being collected. With ownership comes both control and rights with regard to usage. If the consumer is not considered the owner of the data obtained from metering and home automation systems, the consumer may not receive the privacy protections provided to data owners under existing laws.

---

[76] Additional details are provided in NISTIR 7628.

[77] http://infotech.aicpa.org/Resources/Privacy/Generally+Accepted+Privacy+Principles/Privacy++An+Introduction+to+Generally+Accepted+Privacy+Principles.htm.

[78] One example of this is available at http://www.philly.com/inquirer/business/20090906_Utilities__smart_meters_save_money__but_erode_privacy.html .

It is important to also consider that the proliferation of a variety of smart appliances and devices within residences means an increase in the number of devices that must be secured to protect the privacy of the data collected and potentially stored within them. The privacy risks presented by these smart appliances and devices are expanded when they are attached to Home Area Networks (HANs) over power lines, effectively extending the perimeter of the HAN to outside the walls of the premises.

While the National Association of Regulatory Utility Commissioners (NARUC) has adopted[79] the "Resolution Urging the Adoption of General Privacy Principles for State Commission Use in Considering the Privacy Implications of the Use of Utility Customer Information," the CSCTG Privacy Group's research indicates that:

- There is not yet consensus among state Public Utility Commissions (PUCs) on how to address the specific privacy implications of the Smart Grid.
- State PUCs may not have in all instances the appropriate authority from their respective legislatures to address Smart Grid privacy issues.

Adaptation of well-established methods for protecting consumer privacy is necessary to keep up with the multitude of use cases of the various technologies and business processes created for the Smart Grid. Legal and regulatory frameworks can be further harmonized and updated as the Smart Grid becomes more pervasive. PIAs of data collection, data flows, and processing are also crucial for a deeper understanding of the evolutionary and revolutionary changes that are coming about with the rollout of Smart Grid implementations.

The Smart Grid architecture should follow developments that enable fair information practices in a meaningful and transparent way. A potential additional measure of protection for consumers' privacy would be in the design of Smart Grid applications and devices that allows consumers to have control of their personal information to the greatest extent possible. The CSCTG Privacy Subgroup will continue researching and addressing Smart Grid privacy issues and will document them as they relate to:

- Information collected by all entities involved with the Smart Grid;
- Identified privacy concerns and risks;
- Best privacy practices; and
- Existing laws, regulations and standards.

7.3.4 Safety

The safe operation of the Smart Grid is of primary importance to all stakeholders; thus it is critical to incorporate appropriate safety procedures, criteria, and considerations into the relevant Smart Grid standards. For example, without proper attention to safety in standards, utility crews or first responders could find themselves in situations where they are potentially exposed to live wires connected to such sources as energy storage units or photovoltaic solar panels. These and other related issues should be addressed in a comprehensive manner across the Smart Grid. The SGIP should take on this role by reviewing overall safety operations and integrating safety

[79] http://www.naruc.org/Resolutions/privacy_principles.pdf .

considerations as it works to facilitate development of interoperability standards and establishment of a conformity testing and certification framework. The scope includes not only transmission and distribution systems, but also other devices and systems (such as the operation of Smart Grid consumer products in the home). Consideration should be given to correlating with NFPA's National Electric Code and IEEE's National Electric Safety Code. Only through a coordinated effort that includes a demonstrated compliance to safety criteria will it be possible to ensure that the Smart Grid operates in a manner that does not threaten life or property.

7.4 Conclusion

As the SGIP progresses in its work to identify and address additional standards gaps and provide ongoing coordination to accelerate the development of Smart Grid standards, NIST will publish updated Interoperability Framework documents as needed. There are continued opportunities for participation by new Smart Grid community members in the overall NIST process, including within the SGIP and its committees and working groups. Future meetings, workshops, and public comment opportunities will appear on the NIST Smart Grid Collaboration Site. [80]

[80] http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/WebHome.

8 List of Acronyms

ACSE	Association Control Service Element
AEIC	Association of Edison Illuminating Companies
AES	Advanced Encryption Standard
AMI	Advanced Metering Infrastructure
AMR	Automated Meter Reading
ANSI	American National Standards Institute
API	Application Programming Interface
ASHRAE	American Society of Heating, Refrigerating and Air Conditioning Engineers
ATIS	Alliance for Telecommunications Industry Solutions
BAS	Building Automation System
CA	Contingency Analysis
CEIDS	Consortium for Electric Infrastructure to Support a Digital Society
CIM	Common Information Model
CIGRE	International Council on Large Electric Systems
CIP	Critical Infrastructure Protection
CIS	Customer Information System
CM	Configuration Management
CPP	Critical Peak Pricing
CSCTG	Smart Grid Cyber Security Coordination Task Group
CSRC	Computer Security Resource Center
DA	Distribution Automation
DDNS	Dynamic Domain Name System
DER	Distributed Energy Resources
DES	Data Encryption Standard
DEWG	Domain Expert Working Group
DGM	Distribution Grid Management
DHCP	Dynamic Host Configuration Protocol

DHS	Department of Homeland Security
DLC	Direct Load Control
DMS	Distribution Management System
DNS	Domain Name System
DOD	Department of Defense
DOE	Department of Energy
DP	Dynamic Pricing
DR	Demand Response
DWML	Digital Weather Markup Language
ECWG	Electronic Commerce Working Group
EDL	Exchange Data Language
EISA	Energy Independence and Security Act
EMCS	Utility/Energy Management and Control Systems
EMS	Energy Management System
EPRI	Electric Power Research Institute
ES	Energy Storage
ESI	Energy Services Interface
ESP	Energy Service Provider
EUMD	End Use Measurement Device
EV	Electric Vehicle
EVSE	Electric Vehicle Supply Equipment
FBI	Federal Bureau of Investigation
FCC	Federal Communications Commission
FERC	Federal Energy Regulatory Commission
FIPS	Federal Information Processing Standards
FTP	File Transfer Protocol
GHG	Greenhouse Gases
GID	Generic Interface Definition

GIS	Geographic Information System
GOOSE	Generic Object-Oriented Substation Event
GSA	General Services Administration
GWAC	GridWise Architecture Council
HTTP	Hyper Text Transfer Protocol
HVAC	Heating Ventilating and Air Conditioning
IATFF	Information Assurance Technical Framework Forum
ICS	Industrial Control Systems
IEC	International Electrotechnical Commission
IECSA	Integrated Energy and Communications System Architecture
IED	Intelligent Electronic Device
IEEE	Institute of Electrical and Electronic Engineers
IETF	Internet Engineering Task Force
IHD	In-Home Display
IOSS	Interagency OPSEC Support Staff
IP	Internet Protocol
IRM	Interface Reference Model
ISA	International Society of Automation
ISO	International Organization for Standardization, Independent Systems Operator
IT	Information Technology
ITU	International Telecommunication Union
KPI	Key Point of Interoperability
LAN	Local Area Network
LMS	Load Management System
LTC	Load Tap Changer
MDMS	Meter Data Management System
MGI	Modern Grid Initiative
MIB	Management Information Base

MIME	Multipurpose Internet Mail Extensions
MFR	Multilevel Feeder Reconfiguration
MMS	Manufacturing Messaging Specification
MPLS	Multi Protocol Label Switching
NAESB	North American Energy Standards Board
NARUC	National Association of Regulatory Utility Commissioners
NASPI	North American Synchrophasor Initiative
NEMA	National Electrical Manufacturers Association
NERC	North American Electric Reliability Corporation
NIAP	National Information Assurance Partnership
NIPP	National Infrastructure Protection Plan
NIST	National Institute of Standards and Technology
NOAA	National Oceanic and Atmospheric Administration
NSA	National Security Agency
NSM	Network and System Management
OASIS	Organization for the Advancement of Structured Information Standards
OGC	Open Geospatial Consortium
OID	Object Identifier
OMG	Object Management Group
OMS	Outage Management System
OpenSG	Open Smart Grid
OSI	Open Systems Interconnection
OWASP	Open Web Application Security Project
PEV	Plug-in Electric Vehicles
PDC	Phasor Data Concentrator
PMU	Phasor Measurement Unit
QOS	Quality of Service
RAS	Remedial Automation Schemes

RBAC	Role Based Access Control
RFC	Request for Comments, Remote Feedback Controller
RSA	Rivest, Shamir, Adelman
RTO	Regional Transmission Operator
RTP	Real-Time Pricing
RTU	Remote Terminal Unit
SCADA	Supervisory Control and Data Acquisition
SCL	Substation Configuration Language
SCP	Secure Copy Protocol
SDO	Standards Development Organization
SHA	Secure Hash Algorithm
SNMP	Simple Network Management Protocol
SNTP	Simple Network Time Protocol
SOA	Service-Oriented Architecture
SP	Special Publication
SSO	Standards-Setting Organizations
SSH	Secure Shell
SSP	Sector-Specific Plan
TIA	Telecommunications Industry Association
TCP	Transport Control Protocol
TFTP	Trivial File Transfer Protocol
TOGAF	The Open Group Architecture Framework
TOU	Time-of-Use
UCA	Utility Communications Architecture
UCAIug	UCA International Users Group
UID	Universal Identifier
UML	Unified Modeling Language
VA	Volt-amperes

VAR	Volt Amps Reactive
VVWC	Voltage, VAR, and Watt Control
WAMS	Wide-Area Measurement System
WAN	Wide Area Network
WASA	Wide Area Situational Awareness
WG	Working Group
XML	Extensible Markup Language

9 Appendix: Specific Domain Diagrams

9.1 Introduction[81]

The conceptual model consists of several *domains,* each of which contains many *applications* and *actors* that are connected by *associations,* through *interfaces.*

- **Actors** may be devices, computer systems, or software programs and/or the organizations that own them. Actors have the capability to make decisions and exchange information with other actors through interfaces.
- **Applications** are the tasks performed by the actors within the domains. Some applications are performed by a single actor, others by several actors working together.
- **Domains** group actors to discover the commonalities that will define the interfaces. In general, actors in the same domain have similar objectives. Communications within the same domain may have similar characteristics and requirements. Domains may contain other domains.
- **Associations** are logical connections between actors that establish bilateral relationships. Actors interact with associated actors through interfaces. **Associations** are in Figure 3-1; the electrical associations between domains are shown as dashed lines and the communications associations are shown as solid lines.
- **Interfaces** represent the point of access between domains. Communications interfaces are at each end of the communication associations and represent the access point for information to enter and exit a domain (interfaces are logical).**Interfaces** show either electrical connections or communications connections. Each of these interfaces may be bi-directional. Communications interfaces represent an information exchange between two domains and the actors within; they do not represent physical connections. They represent logical connections in the Smart Grid information network interconnecting various domains (as shown in Figure 3-3).

There are seven domains represented within the Smart Grid system as shown in Table 9-1. These represent logical domains based on the present and near-term view of the grid. In the future some of the domains may combine (such as transmission and distribution), and others may shrink in importance (perhaps bulk generation becomes less important as micro-generators become more prevalent).

Table 9-1. Domains in the Smart Grid Conceptual Model.

Domain	Description
Customers	The end users of electricity. May also generate, store, and manage the use of energy. Traditionally, three customer types are discussed, each with its own domain: home, commercial/building, and industrial.

[81] This section is based on the *Report to NIST on the Smart Grid Interoperability Standards Roadmap August 10, 2009, Section 3.2, written by EPRI.*

Markets	The operators and participants in electricity markets.
Service Providers	The organizations providing services to electrical customers and utilities.
Operations	The managers of the movement of electricity.
Bulk Generation	The generators of electricity in bulk quantities. May also store energy for later distribution.
Transmission	The carriers of bulk electricity over long distances. May also store and generate electricity.
Distribution	The distributors of electricity to and from customers. May also store and generate electricity.

It is important to note that domains are NOT organizations. For instance, an ISO or RTO may have actors in both the Markets and Operations domains. Similarly, a distribution utility is not entirely contained within the Distribution domain – it is likely to also contain actors in the Operations domain, such as a Distribution Management System, and in the Customer domain, such as meters.

The Smart Grid Domain Diagrams (including Figure 3-1) are presented at two levels of increasing detail, as shown in Figure 9-1. Users of the model are encouraged to create additional levels or identify particular actors at a particular level in order to discuss the interaction between parts of the Smart Grid.

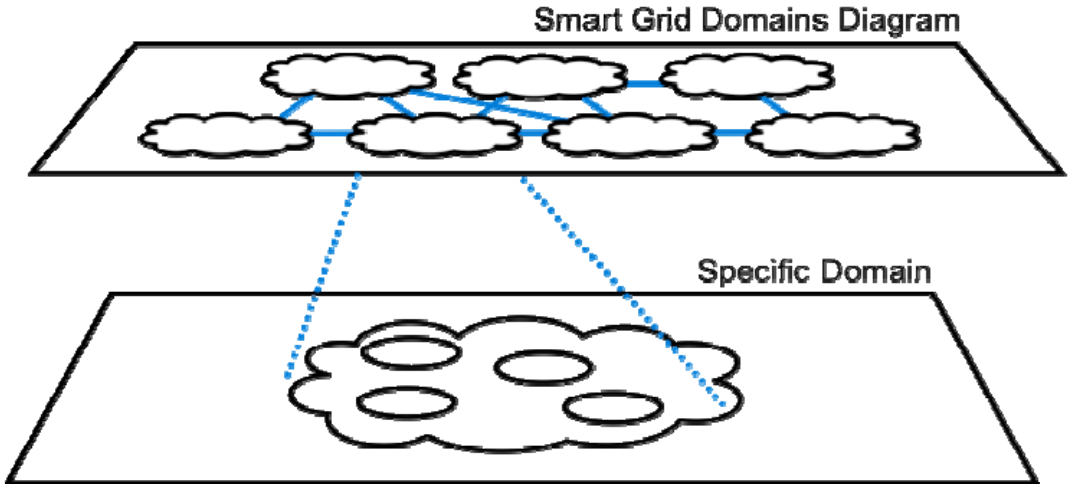


Figure 9-1. Examining the Domains in Detail.

The purpose of the domain diagrams is to provide a framework for discussing both the existing power system and the evolving Smart Grid. While Chapter 3 shows domain interactions and overall scope, the following sections describe the details of the specific domains. Note that the domain diagrams, as presented, are not intended to be comprehensive in identifying all actors and all paths possible in the Smart Grid. This achievement will only be possible after additional elaboration and consolidation of use cases is achieved by stakeholder activities that are ongoing.

It is important to note that the domain diagram (or the conceptual model) of the Smart Grid is not limited to a single domain or a single application or use case. The use of "Smart Grid" in some circles has been applied to only distribution automation or in others to only advanced metering or demand response, for example. The conceptual model assumes that "Smart Grid" includes a wide variety of use cases and applications, especially (but not limited to) functional priorities and cross-cutting requirements identified by FERC. The scope also includes other cross-cutting requirements including data management, and application integration, as described in the GridWise Architecture Council Interoperability Context-Setting Framework.

9.2 Customer Domain

The customer is ultimately the stakeholder that the entire grid was created to support. This is the domain where electricity is consumed (see Figure 9-2). Actors in the Customer domain enable customers to manage their energy usage and generation. Some actors also provide control and information flow between the customer and the other domains. The boundaries of the Customer domain are typically considered to be the utility meter and the Energy Services Interface (ESI). The ESI provides a secure interface for Utility-to- Consumer interactions. The ESI in turn can act as a bridge to facility-based systems such as a Building Automation System (BAS) or a customer's Energy Management System (EMS).

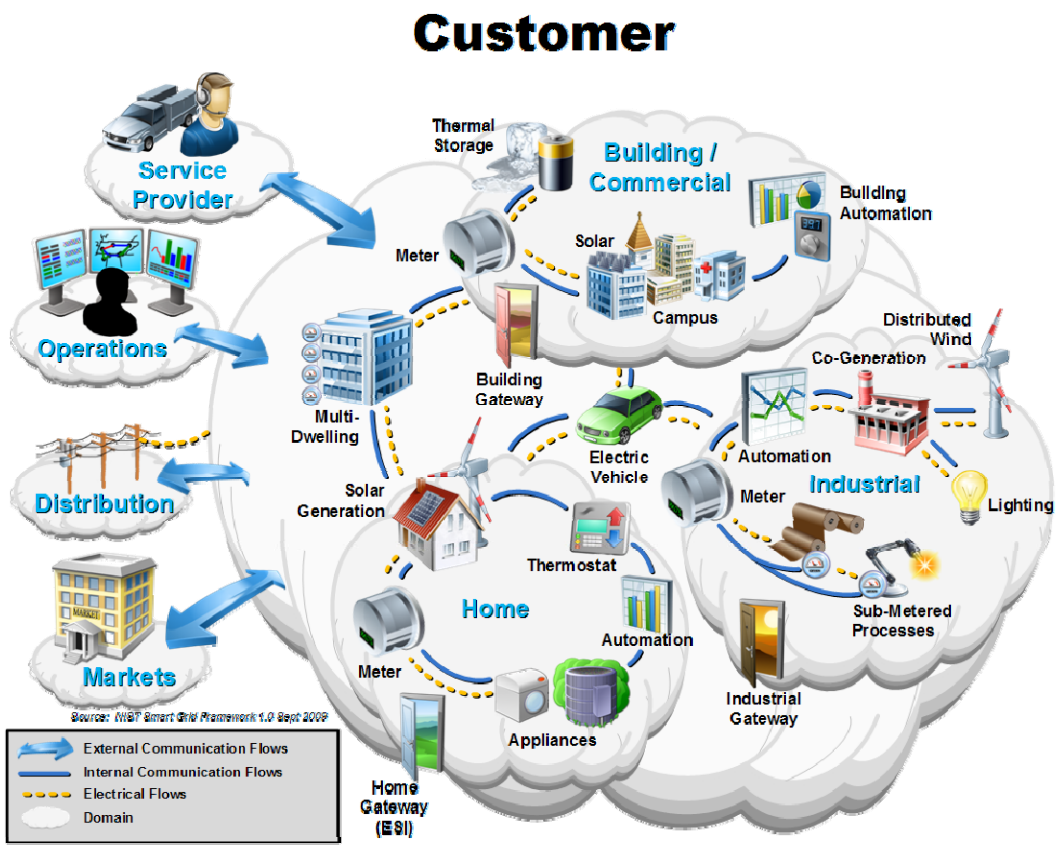


Figure 9-2. Customer Domain Diagram.

The Customer domain is usually segmented into sub-domains for home, commercial/building, and industrial. The energy needs of these sub-domains are typically set at less than 20kW20 kW of demand for Home, 20-200 kW for Commercial/Building, and over 200kW200 kW for Industrial. Each sub-domain has multiple actors and applications, which may also be present in the other sub-domains. Each sub-domain has a meter actor and an ESI that may reside in the meter or on the EMS or in an independent gateway.

The ESI is the primary service interface to the Customer domains. The ESI may communicate with other domains via the AMI infrastructure or via another means, such as the Internet. The ESI communicates to devices and systems within the customer premises across a Home Area Network or other Local Area Network.

There may be more than one EMS— and therefore more than one communications path—per customer. The EMS is the entry point for such applications as remote load control, monitoring and control of distributed generation, in-home display of customer usage, reading of non-energy meters, and integration with building management systems and the enterprise. The EMS may provide auditing/logging for cyber security purposes. The Customer domain is electrically connected to the Distribution domain. It communicates with the Distribution, Operations, Market, and Service Provider domains.

Table 9-2. Typical Application Category in the Customer Domain.

Example Application Category	Description
Building or Home Automation	A system that is capable of controlling various functions within a building such as lighting and temperature control.
Industrial Automation	A system that controls industrial processes such as manufacturing or warehousing. These systems have very different requirements compared to home and building systems.
Micro-generation	Includes all types of distributed generation including; Solar, Wind, and Hydro generators. Generation harnesses energy for electricity at a customer location. May be monitored, dispatched, or controlled via communications.

9.3 Markets Domain

The markets are where grid assets are bought and sold. Actors in the Markets domain exchange price and balance supply and demand within the power system (see Figure 9-3). The boundaries of the Market domain include the edge of the Operations domain where control happens, the domains supplying assets (e.g., generation, transmission, etc) and the Customer domain.

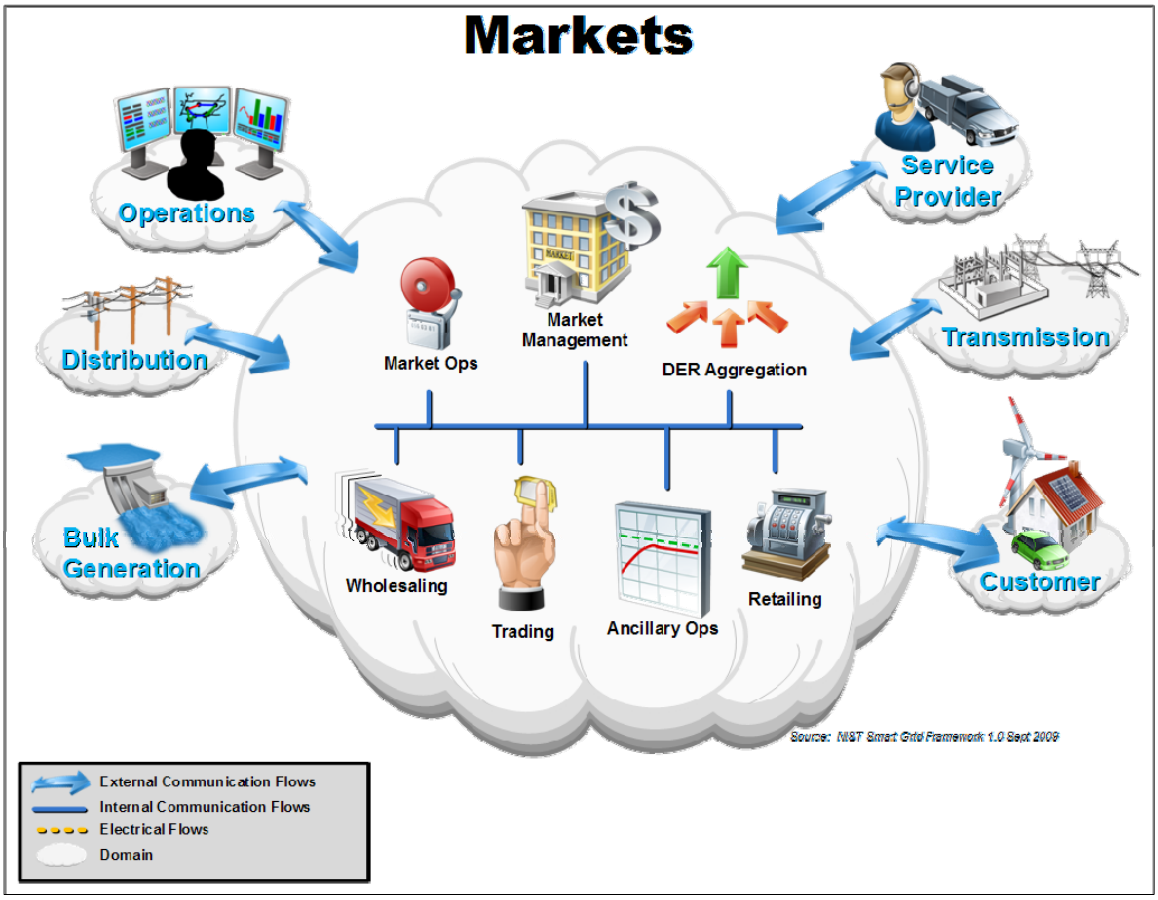


Figure 9-3. Overview of the Markets Domain.

Communication between the Markets domain and the domains supplying energy are critical because efficient matching of production with consumption is dependent on markets. Energy supply domains include the Bulk Generation domain and Distributed Energy Resources (DER). DER reside in the Transmission, Distribution, and Customer domains. NERC CIPs consider suppliers of more than 300 megawatts to be Bulk Generation; most DER is smaller and is typically served through aggregators. DERs participate in markets to some extent today, and will participate to a greater extent as the Smart Grid becomes more interactive.

Communications for Markets domain interactions must be reliable. They must be traceable and auditable. They must support e-commerce standards for integrity and non-repudiation. As the percentage of energy supplied by small DER increases, the allowed latency in communications with these resources must be reduced.

The high-priority challenges in the Markets domain are: extension of price and DER signals to each of the Customer sub-domains; simplification of market rules; expanding the capabilities of aggregators; interoperability across all providers and consumers of market information; managing the growth (and regulation) of retailing and wholesaling of energy, and evolving communication mechanisms for prices and energy characteristics between and throughout the Markets and Customer domains.

Table 9-3. Typical Applications in the Markets Domain.

Example Application Category	Description
Market Management	Market managers include ISOs for wholesale markets or NYMEX/CME for forward markets in many ISO/RTO regions. There are transmission and services and demand response markets as well. Some DER Curtailment resources are treated today as dispatchable generation.
Retailing	Retailers sell power to end customers and may in the future aggregate or broker DER between customers or into the market. Most are connected to a trading organization to allow participation in the wholesale market.
DER Aggregation	Aggregators combine smaller participants (as providers or customers or curtailment) to enable distributed resources to play in the larger markets.
Trading	Traders are participants in markets, which include aggregators for provision and consumption and curtailment, and other qualified entities. There are a number of companies whose primary business is the buying and selling of energy.
Market Operations	Make a particular market function smoothly. Functions include financial and goods sold clearing, price quotation streams, audit, balancing, and more.
Ancillary Operations	Provide a market to provide frequency support, voltage support, spinning reserve and other ancillary services as defined by FERC, NERC and the various ISOs. These markets function on a regional or ISO basis normally.

9.4 Service Provider Domain

Actors in the Service Provider domain perform services to support the business processes of power system producers, distributors and customers (see Figure 9-4). These business processes range from traditional utility services, such as billing and customer account management, to enhanced customer services, such as management of energy use and home energy generation.

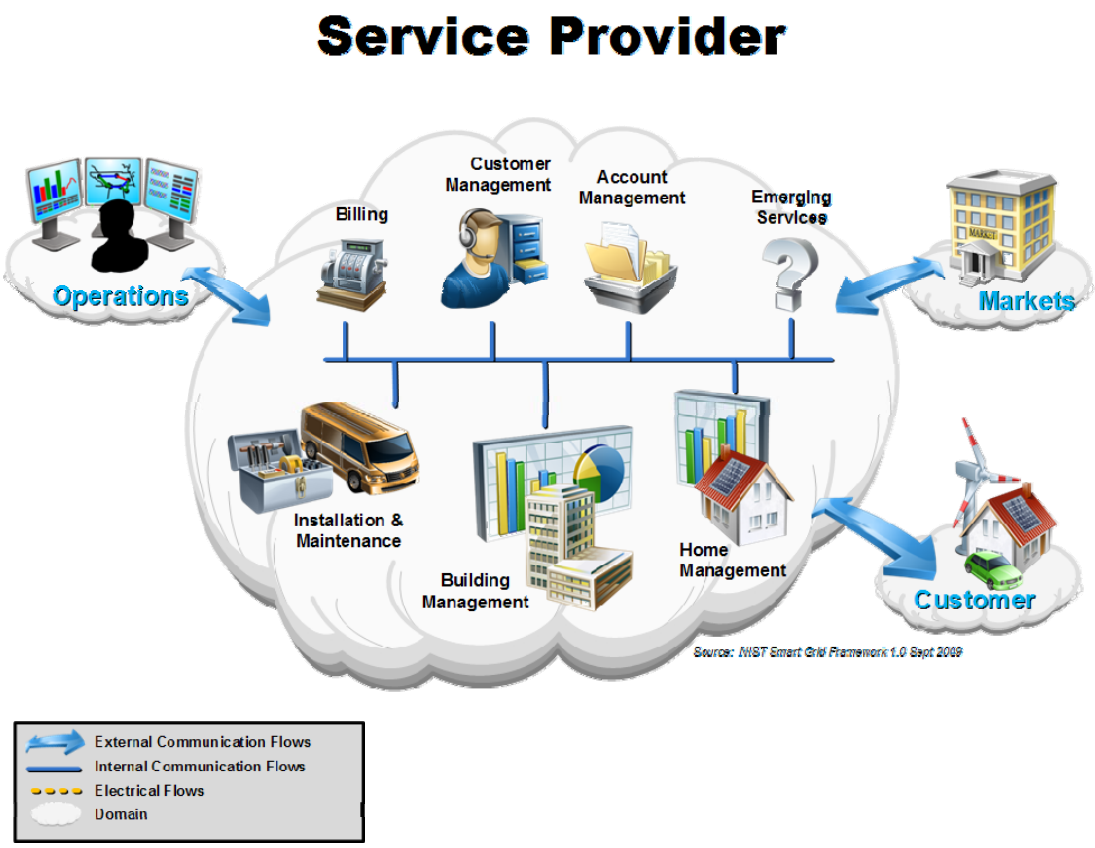


Figure 9-4. Overview of the Service Provider Domain.

The service provider must not compromise the cyber security, reliability, stability, integrity, or safety of the electrical power network when delivering existing or emerging services.

The Service Provider domain shares interfaces with the Markets, Operations, and Customer domains. Communications with the Operations domain are critical for system control and situational awareness; communications with the Markets and Customer domains are critical for enabling economic growth through the development of "smart" services. For example, the Service Provider domain may provide the interface enabling the customer to interact with the market(s).

Service providers will create new and innovative services and products to meet the new requirements and opportunities presented by the evolving Smart Grid. Services may be performed by the electric service provider, by existing third parties, or by new participants drawn by the new business models. Emerging services represent an area of significant new economic growth.

The priority challenge in the Service Provider domain is to develop the key interfaces and standards that will enable a dynamic market-driven ecosystem while protecting the critical power infrastructure. These interfaces must be able to operate over a variety of networking technologies while maintaining consistent messaging semantics. Some benefits to the Service Provider domain from the deployment of the Smart Grid include:

1) The development of a growing market for third parties to provide value-added services and products to customers, utilities and other stakeholders at competitive costs.
2) The decrease in cost of business services for other Smart Grid domains.
3) A decrease in power consumption and an increase in power generation as customers become active participants in the power supply chain.

Table 9-4. Typical Applications in the Service Provider Domain.

Example Application Category	Description
Customer Management	Managing customer relationships by providing point-of-contact and resolution for customer issues and problems.
Installation & Management	Installing and maintaining premises equipment that interacts with the Smart Grid.
Building Management	Monitoring and controlling building energy and responding to Smart Grid signals while minimizing impact on building occupants.
Home Management	Monitoring and controlling home energy and responding to Smart Grid signals while minimizing impact on home occupants.
Billing	Managing customer billing information, including sending billing statements and processing payments.
Account Management	Managing the supplier and customer business accounts.
Emerging Services	All of the services and innovations that have yet to be created. These will be instrumental in defining the Smart Grid of the future.

9.5 Operations Domain

Actors in the Operations domain are responsible for the smooth operation of the power system. Today, the majority of these functions are the responsibility of a regulated utility (see Figure 9-5). The Smart Grid will enable more of them to be outsourced to service providers; others may evolve over time. No matter how the Service Provider and Markets domains evolve, there will still be basic functions needed for planning and operating the service delivery points of a “wires” company.

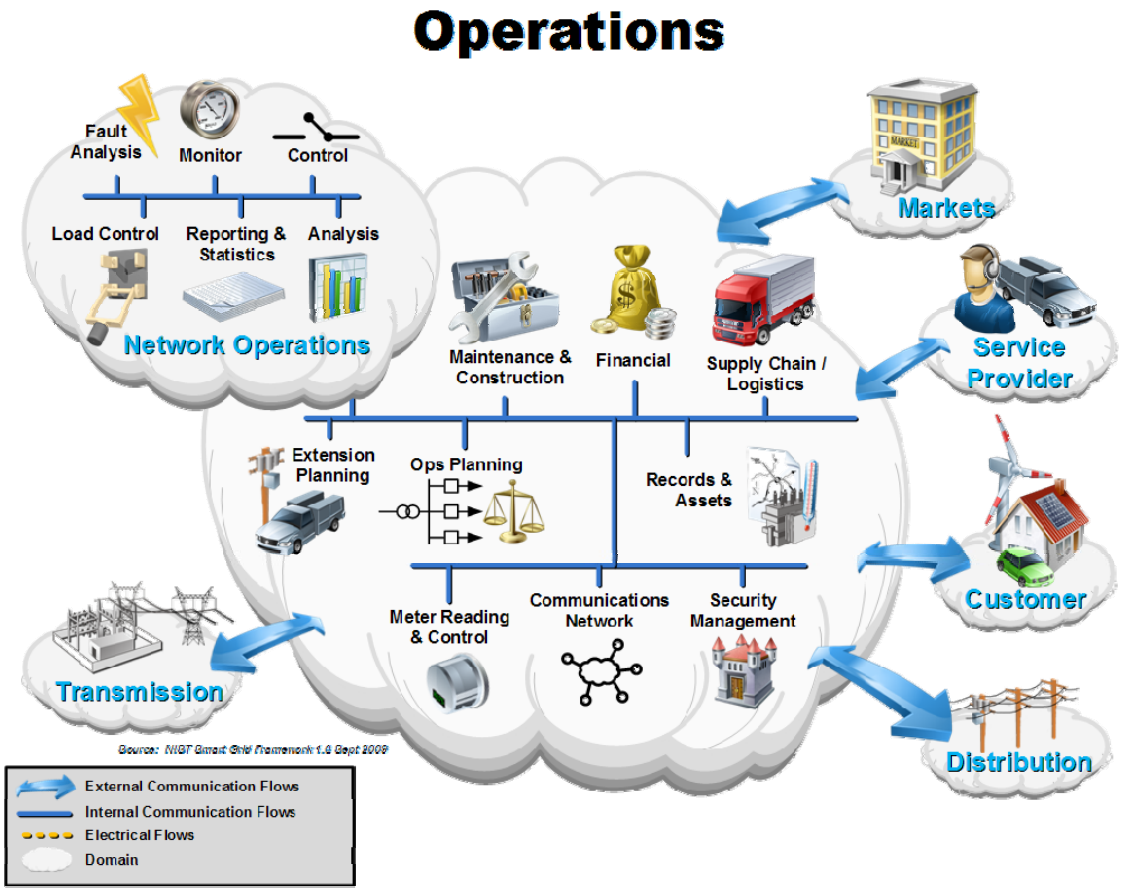


Figure 9-5. Overview of the Operations Domain.

In transmission operations, Energy Management Systems (EMSs) are used to analyze and operate the transmission power system reliably and efficiently, while in distribution operations, similar Distribution Management Systems (DMSs) are used for analyzing and operating the distribution system.

Representative applications within the Operations domain are described in Table 9-5. These applications are derived from the IEC 61968-1 Interface Reference Model (IRM) for this domain.

Table 9-5. Typical Applications in the Operations Domain.

Example Application Category	Description
Monitoring	Network Operation Monitoring actors supervise network topology, connectivity and loading conditions, including breaker and switch states, and control equipment status. They locate customer telephone complaints and field crews.
Control	Network control is coordinated by actors in this domain, although they may only supervise wide area, substation, and local automatic or manual control.
Fault Management	Fault Management actors enhance the speed at which faults can be located, identified, and sectionalized and service can be restored. They provide information for customers, coordinate with workforce dispatch and compile information for statistics.
Analysis	Operation Feedback Analysis actors compare records taken from real-time operation related with information on network incidents, connectivity and loading to optimize periodic maintenance.
Reporting and Statistics	Operational Statistics and Reporting actors archive on-line data and perform feedback analysis about system efficiency and reliability.
Calculations	Real-time Network Calculations actors (not shown) provide system operators with the ability to assess the reliability and security of the power system.
Training	Dispatcher Training actors provide facilities for dispatchers that simulate the actual system they will be using (not shown in Figure 9-5).
Records and Assets	The Records and Asset Management actors track and report on the substation and network equipment inventory, provide geospatial data and geographic displays, maintain records on non-electrical assets, and perform asset investment planning.

Operation Planning	Operational Planning and Optimization actors perform simulation of network operations, schedule switching actions, dispatch repair crews, inform affected customers, and schedule the importing of power. They keep the cost of imported power low through peak generation, switching, load shedding or demand response.
Maintenance and Construction	Maintenance and Construction actors coordinate inspection, cleaning and adjustment of equipment, organize construction and design, dispatch and schedule maintenance and construction work, and capture records gathered by field to view necessary information to perform their tasks.
Extension Planning	Network Extension planning actors develop long term plans for power system reliability, monitor the cost, performance and schedule of construction, and define projects to extend the network such as new lines, feeders or switchgear.
Customer Support	Customer Support actors help customers to purchase, provision, install and troubleshoot power system services, and relay and record customer trouble reports.

9.6 Bulk Generation Domain

Applications in the Bulk Generation domain are the first processes in the delivery of electricity to customers (see Figure 9-6). Electricity generation is the process of creating electricity from other forms of energy, which may vary from chemical combustion to nuclear fission, flowing water, wind, solar radiation and geothermal heat. The boundary of the Bulk Generation domain is typically the Transmission domain. The Bulk Generation domain is electrically connected to the Transmission domain and shares interfaces with the Operations, Markets and Transmission domains.

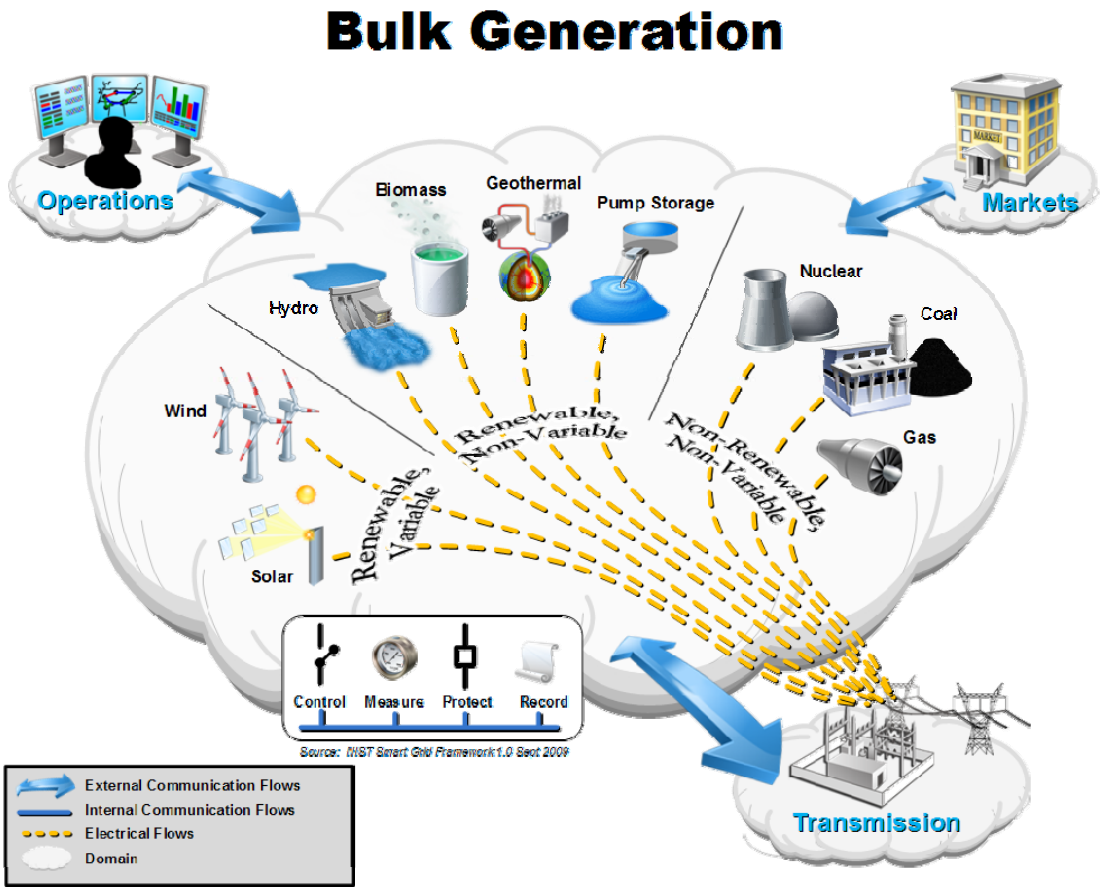


Figure 9-6. Overview of the Bulk Generation Domain.

Communications with the Transmission domain are the most critical because without transmission, customers cannot be served. The Bulk Generation domain must communicate key performance and quality of service issues such as scarcity (especially for wind and sun) and generator failure. These communications may cause the routing of electricity onto the transmission system from other sources. A lack of sufficient supply may be addressed directly (via Operations) or indirectly (via Markets).

New requirements for the Bulk Generation domain include green house gas emissions controls, increases in renewable energy sources, and provision of storage to manage the variability of renewable generation. Actors in the Bulk Generation domain may include various devices such as protection relays, remote terminal units, equipment monitors, fault recorders, user interfaces, and programmable logic controllers.

Table 9-6. Typical Applications in the Bulk Generation Domain.

Example Application Category	Description
Control	Performed by actors that permit the Operations domain to manage the flow of power and reliability of the system. An example is the use of phase angle regulators within a substation to control power flow between two adjacent power systems
Measure	Performed by actors that provide visibility into the flow of power and the condition of the systems in the field. In the future, measurement might be found built into meters, transformers, feeders, switches and other devices in the grid. An example is the digital and analog measurements collected through the SCADA system from a remote terminal unit (RTU) and provide to a grid control center in the Operations domain.
Protect	Performed by Actors that react rapidly to faults and other events in the system that might cause power outages, brownouts, or the destruction of equipment. Performed to maintain high levels of reliability and power quality. May work locally or on a wide scale.
Record	Performed by actors that permit other domains to review what has happened on the grid for financial, engineering, operational, and forecasting purposes.
Asset Management	Management performed by actors that work together to determine when equipment should have maintenance, calculate the life expectancy of the device, and record its history of operations and maintenance so it can be reviewed in the future for operational and engineering decisions.

9.7 Transmission Domain

Transmission is the bulk transfer of electrical power from generation sources to distribution through multiple substations (see Figure 9-7). A transmission network is typically operated by a Regional Transmission Operator or Independent System Operator (RTO/ISO) whose primary responsibility is to maintain stability on the electric grid by balancing generation (supply) with load (demand) across the transmission network. Examples of actors in the transmission domain include remote terminal units, substation meters, protection relays, power quality monitors, phasor measurement units, sag monitors, fault recorders, and substation user interfaces.

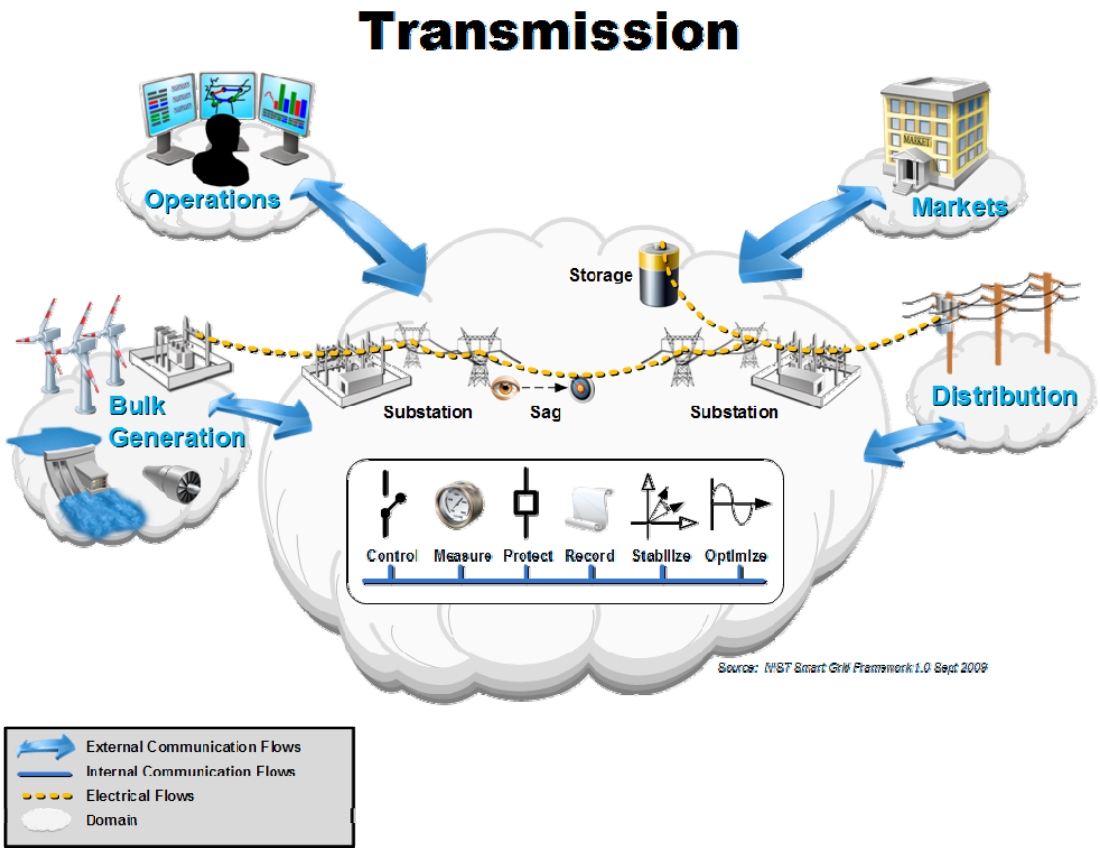


Figure 9-7. Overview of the Transmission Domain.

Actors in the Transmission domain typically perform the applications shown in the diagram (Figure 9-7) and described in the table. The transmission domain may contain Distributed Energy Resources such as electrical storage or peaking generation units.

Energy and supporting ancillary services (capacity that can be dispatched when needed) are procured through the Markets domain, scheduled and operated from the Operations domain, and finally delivered through the Transmission domain to the distribution system and finally to the Customer domain.

Most activity in the Transmission domain is in a substation. An electrical substation uses transformers to change voltage from high to low or the reverse across the electric supply chain. Substations also contain switching, protection and control equipment. Figure 9-7 depicts both step-up and step down sub-stations connecting generation (including peaking units) and storage with distribution. Substations may also connect two or more transmission lines.

Transmission towers, power lines and field telemetry such as the line sag detector shown make up the balance of the transmission network infrastructure. The transmission network is typically monitored and controlled through a supervisory control and data acquisition (SCADA) system composed of a communication network, monitoring devices and control devices.

Table 9-7. Typical Applications in the Transmission Domain.

Example Application Category	Description
Substation	The systems within a substation.
Storage	A system that controls the charging and discharging of an energy storage unit
Measurement & Control	Includes all types of measurement and control systems to measure, record, and control with the intent of protecting and optimizing grid operation.

9.8 Distribution Domain

The Distribution domain is the electrical interconnection between the Transmission domain, the Customer domain and the metering points for consumption, distributed storage, and distributed generation (see Figure 9-8). The electrical distribution system may be arranged in a variety of structures, including radial, looped or meshed. The reliability of the distribution system varies depending on its structure, the types of actors that are deployed, and the degree to which they communicate with each other and with the actors in other domains.

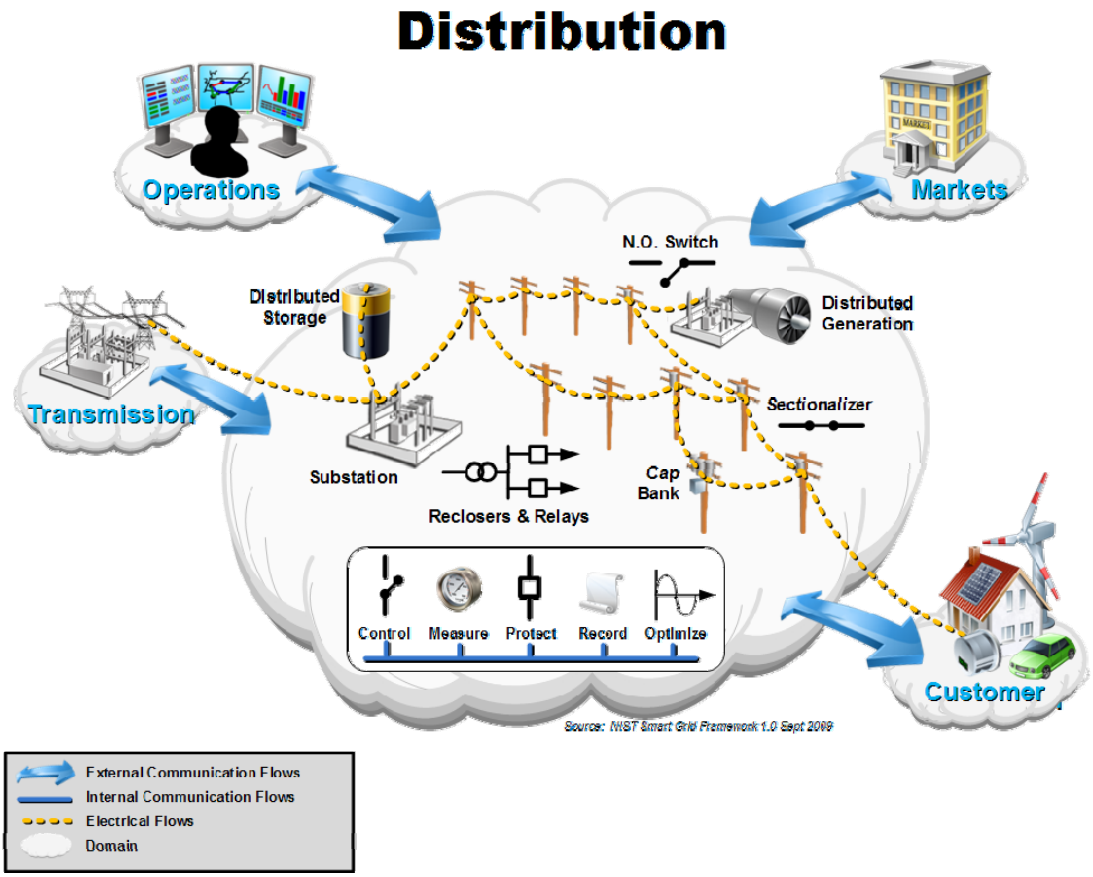


Figure 9-8. Overview of the Distribution Domain.

Historically, distribution systems have been radial configurations, with little telemetry, and almost all communications within the domain was performed by humans. The primary installed sensor base in this domain is the customer with a telephone, whose call initiates the dispatch of a field crew to restore power. Many communications interfaces within this domain have been hierarchical and unidirectional, although they now generally can be considered to work in both directions, even as the electrical connections are just beginning to support bidirectional flow. Distribution actors may have local inter-device (peer-to-peer) communication or a more centralized communication methodology.

In the Smart Grid, the Distribution domain will communicate more closely with the Operations domain in real-time to manage the power flows associated with a more dynamic Markets domain and other environmental and security-based factors. The Markets domain will communicate with the Distribution domain in ways that will affect localized consumption and generation. In turn, these behavioral changes due to market forces may have electrical and structural impacts on the Distribution domain and the larger grid. Under some models, third-party Customer Service Providers may communicate with the Customer domain using the infrastructure of the Distribution domain, which would change the communications infrastructure selected for use within the Domain.

Table 9-8. Typical Applications within the Distribution Domain.

Example Application Category	Description
Substation	The control and monitoring systems within a substation.
Storage	A system that controls a charging and discharging of an energy storage unit
Distributed Generation	A power source located on the distribution side of the grid.
Measurement & Control	Includes all types of measurement and control systems to measure, record, and control with the intent of protecting and optimizing grid operation.