Draft NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 2.0

October 2011

Working Draft

Draft NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 2.0

October 17, 2011 REVISION

Working Draft

Table of Contents

Working Draft

Working Draft

Working Draft

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.

Working Draft

Executive Summary

Background

A 21st century clean energy economy demands a 21st century electric grid. Much of the traditional electricity infrastructure has changed little from the design and form of the electric grid as envisioned by Thomas Edison and George Westinghouse at the end of the 19th century.

Congress and the Administration have outlined a vision for the Smart Grid and have laid the policy foundation upon which it is being built. The Energy Independence and Security Act of 2007 (EISA) made it the policy of the United States to modernize the nation's electricity transmission and distribution system to create a smart electric grid.[1] The American Recovery and Reinvestment Act of 2009 (ARRA) accelerated the development of Smart Grid technologies, investing $4.5 billion for electricity delivery and energy reliability activities to modernize the electric grid and implement demonstration and deployment programs (as authorized under Title XIII of EISA).[2] In January 2011, President Obama, in his State of the Union Address, reiterated his vision for a clean energy economy,[3] and he underscored the Administration's commitment in the "Blueprint for a Secure Energy Future."[4] And in June 2011, the White House released a report by the Cabinet-level National Science and Technology Council (NSTC) entitled "A Policy Framework for the 21st Century Grid: Enabling Our Secure Energy Future."[5]

The critical role of standards for the Smart Grid is spelled out in EISA and in the June 2011 NSTC report, which advocates the development and adoption of standards to ensure that today's investments in the Smart Grid remain valuable in the future; to catalyze innovations; to support consumer choice; to create economies of scale to reduce costs; and to open global markets for Smart Grid devices and systems.

Working Draft

[1] Energy Independence and Security Act of 2007 [Public Law No: 110-140].

[2] 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.

[3] The White House, Office of the Press Secretary, "Remarks by the President in State of the Union Address." January 25, 2011. See http://www.whitehouse.gov/the-press-office/2011/01/25/remarks-president-state-union-address.

[4] The White House, "Blueprint for a Secure Energy Future." March 30, 2011. See http://www.whitehouse.gov/sites/default/files/blueprint_secure_energy_future.pdf.

[5] National Science and Technology Council, "A POLICY FRAMEWORK FOR THE 21st CENTURY GRID: Enabling Our Secure Energy Future." See http://www.whitehouse.gov/sites/default/files/microsites/ostp/nstc-smart-grid-june2011.pdf.

Role and Response of the National Institute of Standards and Technology (NIST)

EISA assigns to the National Institute of Standards and Technology (NIST) the "primary responsibility to coordinate development of a framework that includes protocols and model standards for information management to achieve interoperability[6] of Smart Grid devices and systems…."[7]

In response to the urgent need to establish interoperable standards and protocols for the Smart Grid, NIST developed a three-phase plan:

I) To accelerate the identification of an initial set of standards;

II) To establish a robust Smart Grid Interoperability Panel (SGIP) to sustain the development of the many additional standards that will be needed; and

III) To set up a conformity testing and certification infrastructure.

Beginning in 2008 and continuing throughout 2009, NIST convened workshops and meetings that brought together experts and a diverse group of stakeholders to begin the implementation of the three-phase plan. By the end of 2009, significant progress and consensus had been achieved in developing a roadmap and identifying an initial set of standards (Phase I of the NIST plan). The publication in January 2010 of the *NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0* (Release 1.0)[8] represented an important milestone and documented the progress made up to that time.

Release 1.0 of the NIST Framework described a high-level conceptual reference model for the Smart Grid, identified 75 existing standards that are applicable (or likely to be applicable) to the ongoing development of the Smart Grid, specified 15 high-priority gaps and harmonization issues for which new or revised standards and requirements are needed, documented action plans with aggressive timelines by which designated standards-setting organizations (SSOs) will address these gaps, and described the strategy to establish requirements and standards to help ensure Smart Grid cybersecurity.

Content of Framework 2.0

This document, Release 2.0 of the *NIST Framework and Roadmap for Smart Grid Interoperability Standards*, details progress made in Phases II and III of NIST's three-phase plan since the establishment of the Smart Grid Interoperability Panel (SGIP) in November 2009.

Major deliverables have been produced in the areas of Smart Grid architecture, cybersecurity, and testing and certification. The lists of standards have been updated and expanded. The first

Working Draft

[6] "Interoperability" refers to 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.

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

[8] http://www.nist.gov/public_affairs/releases/upload/smartgrid_interoperability_final.pdf.

group of Smart Grid standards to emerge from the SGIP Priority Action Plans (PAPs), filling gaps identified in Release 1.0, were added to the list of identified Smart Grid standards. The listed standards have undergone an extensive vetting process and are expected to stand the "test of time" as useful building blocks for firms producing devices and software for the Smart Grid. Sidebars 1 and 2 below provide additional summary information about the contents of this document.

The reference model, standards, gaps, and action plans described in this document provide a solid foundation for a secure, interoperable Smart Grid. However, the Smart Grid will continually evolve as new requirements and technologies emerge. The processes established by the SGIP, engaging the diverse community of Smart Grid stakeholders, provide a robust ongoing mechanism to develop requirements to guide the standardization efforts now spanning more than 20 standards-setting organizations.

The results of NIST's ongoing work on standards for the Smart Grid reflected in this framework document provide input to industry utilities, vendors, academia, regulators, and other Smart Grid stakeholders. Among the stakeholder groups who may find this Release 2.0 document most useful are the following:

- Utilities and suppliers concerned with how best to understand and implement the Smart Grid (especially Chapters 3, 4, and 6);
- Testing laboratories and certification organizations (especially Chapter 7);
- Academia (especially Section 5.5 and Chapter 8); and
- Regulators (especially Chapters 1, 4, and 6).

<u>Next Steps</u>

Execution of the Priority Action Plans presently under way will continue until their objectives to fill identified gaps in the standards portfolio have been accomplished. As new gaps and requirements are identified, the SGIP will continue to initiate Priority Action Plans to address them. Many of the DOE Smart Grid Investment Grant projects, funded by ARRA as mentioned above, will come to fruition in the near future. In their proposals, awardees were required to describe how the projects would support the NIST Framework. As experience with new Smart Grid technologies is gained from these projects, NIST and the SGIP will use these "lessons learned" to further identify the gaps and shortcomings of the standards upon which these technologies are based. NIST and the SGIP will work with SSOs and other stakeholders to fill the gaps and improve the standards that form the foundation of the Smart Grid.

Work on the SGIP Catalog of Standards will continue to fully populate the Catalog and ensure robust architectural and cybersecurity reviews of the standards. The cybersecurity guidelines will be kept up to date to stay ahead of emerging new threats. Efforts will continue to partner with the private sector as it establishes testing and certification programs consistent with the SGIP testing and certification framework. Work will continue to coordinate with related international Smart Grid standards efforts to maintain U.S. leadership.

Working Draft

NIST will continue to support the needs of regulators as they address standardization matters in the regulatory arena. Under EISA, the Federal Energy Regulatory Commission (FERC) is charged with instituting rulemaking proceedings to adopt the standards and protocols as may be necessary to ensure Smart Grid functionality and interoperability once, in FERC's judgment, the NIST-coordinated process has led to sufficient consensus.[9] FERC obtained public input through two Technical Conferences on Smart Grid Interoperability Standards in November 2010 and January 2011,[10] and through a supplemental notice requesting comments in February 2011.[11] As a result, FERC issued an order in July 2011[12] stating that there was insufficient consensus for it to institute a rulemaking at that time to adopt the initial five families of standards identified by NIST as ready for consideration by regulators.[13]

In that July 2011 order, however, FERC expressed support for the NIST interoperability framework process, including the work done by the SGIP, for development of Smart Grid interoperability standards. The Commission's order stated that the NIST Framework is comprehensive and represents the best vehicle for developing standards for the Smart Grid. FERC's order also encourages stakeholders to actively participate and look to the NIST-coordinated process for guidance on Smart Grid standards. NIST supported the Commission's order, which notes that "In its comments, NIST suggests that the Commission could send appropriate signals to the marketplace by recommending use of the NIST Framework without mandating compliance with particular standards. NIST adds that it would be impractical and unnecessary for the Commission to adopt individual interoperability standards."[14]

Although the NIST framework and roadmap effort is the product of federal legislation, broad engagement of Smart Grid stakeholders at the state and local levels is essential to ensure the consistent voluntary application of the standards being developed. Currently, many states and their utility commissions are pursuing Smart Grid-related projects. Ultimately, state and local projects will converge into fully functioning elements of the Smart Grid "system of systems." Therefore, the interoperability and cybersecurity standards developed under the NIST framework and roadmap must support the role of the states in modernizing the nation's electric grid. The NIST framework can provide a valuable input to regulators as they consider the prudency of investments proposed by utilities.

A key objective of the NIST work is to create a self-sustaining, ongoing standards process that supports continuous innovation as grid modernization continues in the decades to come.[15] NIST envisions that the processes being put in place by the SGIP, as they mature, will provide the

Working Draft

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

[10] http://ferc.gov/EventCalendar/EventDetails.aspx?ID=5571&CalType=%20&CalendarID=116&Date=01/31/2011&View=Listview.

[11] http://ferc.gov/EventCalendar/Files/20110228084004-supplemental-notice.pdf.

[12] http://www.ferc.gov/EventCalendar/Files/20110719143912-RM11-2-000.pdf.

[13] These standards include IEC 61850, 61970, 61968, 60870-6, and 62351. To find more information about these standards, see Table 4-1 in Section 4.3.

[14] See reference http://www.ferc.gov/EventCalendar/Files/20110719143912-RM11-2-000.pdf, p. 6.

[15] As part of this process, the SGIP will help to prioritize and coordinate Smart Grid-related standards. See Chapter 5 for further discussion.

mechanism to evolve the Smart Grid standards framework as new requirements and technologies emerge. The SGIP processes will also evolve and improve as experience is gained.

Working Draft

WHAT’S INCLUDED IN RELEASE 2.0

Chapter 1, “Purpose and Scope,” outlines the role of NIST with respect to the Smart Grid, defines key concepts and priorities discussed in the document, identifies potential uses of the document, and describes the basic content of the document.

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

Chapter 3, **“**Conceptual Architectural Framework,” 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. Because the Smart Grid is an evolving networked system of systems, the high-level model provides guidance for SSOs developing more detailed views of Smart Grid architecture.

Chapter 4, “Standards Identified for Implementation,” presents and describes existing standards and emerging specifications applicable to the Smart Grid. It includes descriptions of selection criteria and methodology, 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, “Smart Grid Interoperability Panel,” presents the mission and structure of the SGIP. The SGIP is a membership-based organization established to identify, prioritize, and address new and emerging requirements for Smart Grid standards. Working as a public-private partnership, the SGIP provides an open process for stakeholders to interact with NIST in the ongoing coordination, acceleration, and harmonization of standards development for the Smart Grid.

Chapter 6, “Cybersecurity Strategy,” provides an overview of the content of the NIST Interagency Report 7628, *Guidelines for Smart Grid Cyber Security* (NISTIR 7628)*,* and outlines the go-forward strategy of the Cybersecurity Working Group (CSWG). Cybersecurity is now being expanded to address the following: combined power systems; information technology (IT) and communication systems in order to maintain the reliability of the Smart Grid; the physical security of all components; the reduced impact of coordinated cyber-physical attacks; and the privacy of consumers.

Chapter 7, “Testing and Certification,” provides details on an assessment of existing Smart Grid standards testing programs, and it offers high-level guidance for the development of a testing and certification framework. This chapter includes a comprehensive roadmap and operational framework for how testing and certification of the Smart Grid devices will be conducted.

Chapter 8, “Next Steps” contains a high-level overview of some of the currently foreseen areas of interest to the Smart Grid community, including electromagnetic disturbance and interference, reliability and “implementability” of standards.

WHAT’S NEW IN RELEASE 2.0

This document, Release 2.0, builds on the work reported in Release 1.0. Throughout the document, facts and figures have been updated. Two new chapters and a number of new sections have been added. In addition to the subjects highlighted below, a number of chapters include forward-looking sections that outline current and future activities.

<u>Chapter 1</u>

New subjects in this chapter include:

- The history of NIST and the Smart Grid has been updated to include activities from 2010 and 2011, and the key events are highlighted in a timeline. (Figure 1-1.)
- A new section, “Use of this Framework,” has been added. (Section 1.2.)
- New key concepts have been added to the “Definitions” section. (Section 1.3.1.)

<u>Chapter 2</u>

Section 2.2 (“Importance to National Energy Policy Goals”) has been updated to include information from the January 2011 State of the Union address and the June 2011 National Science and Technology Council report. The broadening of the Smart Grid vision beyond the borders of the United States is reflected in two new sections that have been added to this chapter: “International Smart Grid Standards” and “International Efforts to Harmonize Architectures.” (Sections 2.3 and 2.4.)

<u>Chapter 3</u>

The conceptual architectural framework described in this chapter in Release 2.0 provides a significant expansion to the conceptual reference model, which had been the primary architecture-related topic discussed in Release 1.0’s Chapter 3. A description of the conceptual architectural framework, now under development, includes the following:

- Architectural Goals for the Smart Grid (Section 3.2);
- Conceptual Reference Model, which comprises the conceptual domain models and the combined reference model (Section 3.3);
- Models for Smart Grid Information Networks (Section 3.4);
- Smart Grid Interface to the Customer Domain (Section 3.6); and
- Conceptual Business Services (Section 3.7.4).

WHAT’S NEW IN RELEASE 2.0 (cont’d)

Chapter 4

With the establishment of the Smart Grid Interoperability Panel, the process for identifying standards has evolved, and the standards listed in this chapter reflect that evolving process. (Section 4.2.)

A new section, “Process of Future Smart Grid Standards Identification,” details the process that will be used in the future. (Section 4.5.)

The heart of Chapter 4, in both Release 1.0 and Release 2.0, is found in two lists of standards:

- Table 4-1 (“Identified Standards”) is discussed in Section 4.3 (“Current List of Standards Identified by NIST”). In Release 2.0, the number of entries in Table 4-1 has increased from 25 to 34, as compared to the list in Release 1.0.
- Table 4-2 (“Additional Standards, Specifications, Profiles, Requirements, Guidelines, and Reports for Further Review”) is discussed in Section 4.4 (“Current List of Additional Standards Subject to Further Review”). In Release 2.0, the number of entries in Table 4-2 has increased from 50 to 62, as compared to the list in Release 1.0.

In addition to the new standards added to the lists in Release 2.0, these lists include a number of updates to those presented in Release 1.0. The information included with the entries in both tables has been expanded, and links to relevant SGIP-related Web pages have been added.

Chapter 5

This is a new chapter, and most of the issues and deliverables discussed within are also new. Major new topics described in this chapter include:

- Overview of the Smart Grid Interoperability Panel (SGIP) (Section 5.1);
- Descriptions of the roles and activities of key SGIP working groups, such as:
    - The Smart Grid Architecture Committee (Section 5.2.1);
    - The Smart Grid Testing and Certification Committee (Section 5.2.1);
    - The Cybersecurity Working Group (Section 5.2.2); and
    - The nine Domain Expert Working Groups (Section 5.4); and
- Descriptions of the SGIP Catalog of Standards (Section 5.2.3), the Interoperability Knowledge Base (Section 5.6), and the NIST Smart Grid Collaboration Site (Section 5.6).

The topic of Priority Action Plans (PAPs), which had been the only subject of Release 1.0’s Chapter 5 (“Priority Action Plans”), has been updated and is now included in Release 2.0 as Section 5.5.

WHAT’S NEW IN RELEASE 2.0 (cont’d)

Chapter 6

This chapter documents the many developments related to Smart Grid cybersecurity since the topic was discussed in Chapter 6 of Release 1.0. Major new topics described in this chapter include:

- Transition of work and organizational structure from the Cyber Security Coordination Task Group (CSCTG) to SGIP’s Cybersecurity Working Group (CSWG);
- Descriptions of the eight CSWG subgroups (Table 6-1);
- Release of National Institute of Standards and Technology Interagency Report (NISTIR) 7628, *Guidelines for Smart Grid Cyber Security* (Section 6.3.1);
- Standards reviewed, to date, as part of SGIP’s Catalog of Standards process (Section 6.3.2); and
- CSWG’s three-year plan (Section 6.3.3).

Chapter 7

This is a new chapter, and the topics and deliverables discussed within are also new. Major topics described in this chapter include:

- Assessment of existing Smart Grid standards testing programs (Section 7.1.1);
- High-level framework development guide (Section 7.1.2);
- Interoperability process reference manual (Section 7.2.1); and
- Interoperability maturity assessment model (Section 7.2.2).

Chapter 8

This chapter, as compared to Chapter 7 (“Next Steps”) in Release 1.0, reflects the evolving and advancing work of NIST in the area of Smart Grid interoperability standards. One issue mentioned briefly in Release 1.0—“Electromagnetic Disturbances and Interference”—is discussed in more detail in this chapter of Release 2.0. (Section 8.1.1.) One new issue—“Implementability and Reliability of Framework Standards”—is introduced and discussed in this chapter of Release 2.0. (Section 8.1.2.)

1. Purpose and Scope

1.1. Overview and Background

Under the Energy Independence and Security Act of 2007 (EISA), the National Institute of Standards and Technology (NIST) was 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 Section 1305][16]

There is an urgent need to establish Smart Grid[17] standards and protocols. Some Smart Grid devices, such as smart meters, are being widely deployed. Installation of synchrophasors, sensors that provide real-time assessments of power system health to provide system operators with better information for averting disastrous outages, has accelerated rapidly. By 2013, it is expected that 1,000 of these devices will monitor conditions on the power grid, a dramatic increase since January 2009.[18] 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.[19]

Federal loan guarantees for commercial renewable energy generation projects,[20] growing venture capital investments in Smart Grid technologies, and other incentives and investments provide

[16] The Department of Energy (DOE) is the lead federal agency with responsibility for the Smart Grid. Under the American Recovery and Reinvestment Act (ARRA), DOE has sponsored 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 as necessary to ensure functionality and interoperability when it determines that the standards identified in the NIST framework development efforts have sufficient consensus. See Section 1305 of the Energy Independence and Security Act of 2007.

[17] 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.

[18] 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.

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

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

Working Draft

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.

- **(Phase 1): Engage stakeholders in a participatory public process to identify applicable standards and requirements, gaps in currently available standards, and priorities for additional standardization activities.** With the support of outside technical experts working under contract, NIST compiled and incorporated stakeholder inputs from three public workshops, as well as technical contributions from technical working groups and a Cybersecurity Working Group (CSWG, originally named the Cybersecurity Coordination Task Group, or CSCTG), into the NIST-coordinated standards roadmapping effort.

- **(Phase 2): 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 the framework of interoperability standards. On November 19, 2009, a Smart Grid Interoperability Panel (SGIP) was launched to serve this function and has now grown to over 675 organizations comprising over 1790 members.

- **(Phase 3): 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, initiated and completed two major efforts in 2010: (1) performed an assessment of existing Smart Grid standards testing programs; and (2) provided high-level guidance for the development of a testing and certification framework. A permanent Smart Grid Testing and Certification Committee (SGTCC) was established within the SGIP. The SGTCC has assumed the responsibility for constructing an operational framework, as well as the action plans for development of documentation and associated artifacts supporting testing and certification programs that support Smart Grid interoperability.

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 time span, the global market is projected to grow to more than $171 billion, an increase of almost 150 percent.[21]

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.

WORK

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

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 report summarizing a number of consumer studies found that “concern over climate change, energy security, and global competitiveness have made more consumers receptive to learning about energy.”[22] Among the potential benefits of the Smart Grid, consumers saw three as being “best benefits”:

- Detect outages;
- Reduce brownouts; and
- Integrate renewables.[23]

Another national survey indicated 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 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.”[24]

A recent survey also noted that consumers wanted:[25]

- Lights that turn off automatically when they leave the room;
- Thermostats that automatically adjust for savings when no one is home;
- Information about which devices are using the most electricity; and
- Recommendations for saving energy and money.

The release of the *NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0*[26] was the first output of the NIST plan. It described a high-level conceptual reference model for the Smart Grid which: identified 75 existing standards that are applicable (or likely to be applicable) to the ongoing development of the Smart Grid; specified 15 high-priority gaps and harmonization issues (in addition to cybersecurity) for which new or revised standards and requirements are needed; documented action plans with aggressive timelines by which designated standards-setting organizations (SSOs) will address these gaps; and described the strategy to establish requirements and standards to help ensure Smart Grid cybersecurity.

Working Draft

[22] Smart Grid Consumer Collaborative, “2011 State of the Consumer Report,” January 31, 2011. See: http://smartgridcc.org/sgcc-2011-state-of-the-consumer-report.

[23] Smart Grid Consumer Collaborative, “Consumer Voices: Baseline Focus Groups,” 2010.

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

[25] Smart Grid News, “The Sneak Attack Utilities Are Not Prepared For,” Feb 3, 2011. See: http://www.smartgridnews.com/artman/publish/Business_Strategy/The-sneak-attack-utilities-are-not-prepared-for-3476.html.

[26] http://www.nist.gov/public_affairs/releases/upload/smartgrid_interoperability_final.pdf.

Release 1.0 of the NIST framework document contained information obtained 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. The timeline for the development of the Release 1.0 framework document is displayed in Figure 1-1, which shows the history of NIST and the Smart Grid. 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 first 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 the final version of the report, which was published in January of 2010.

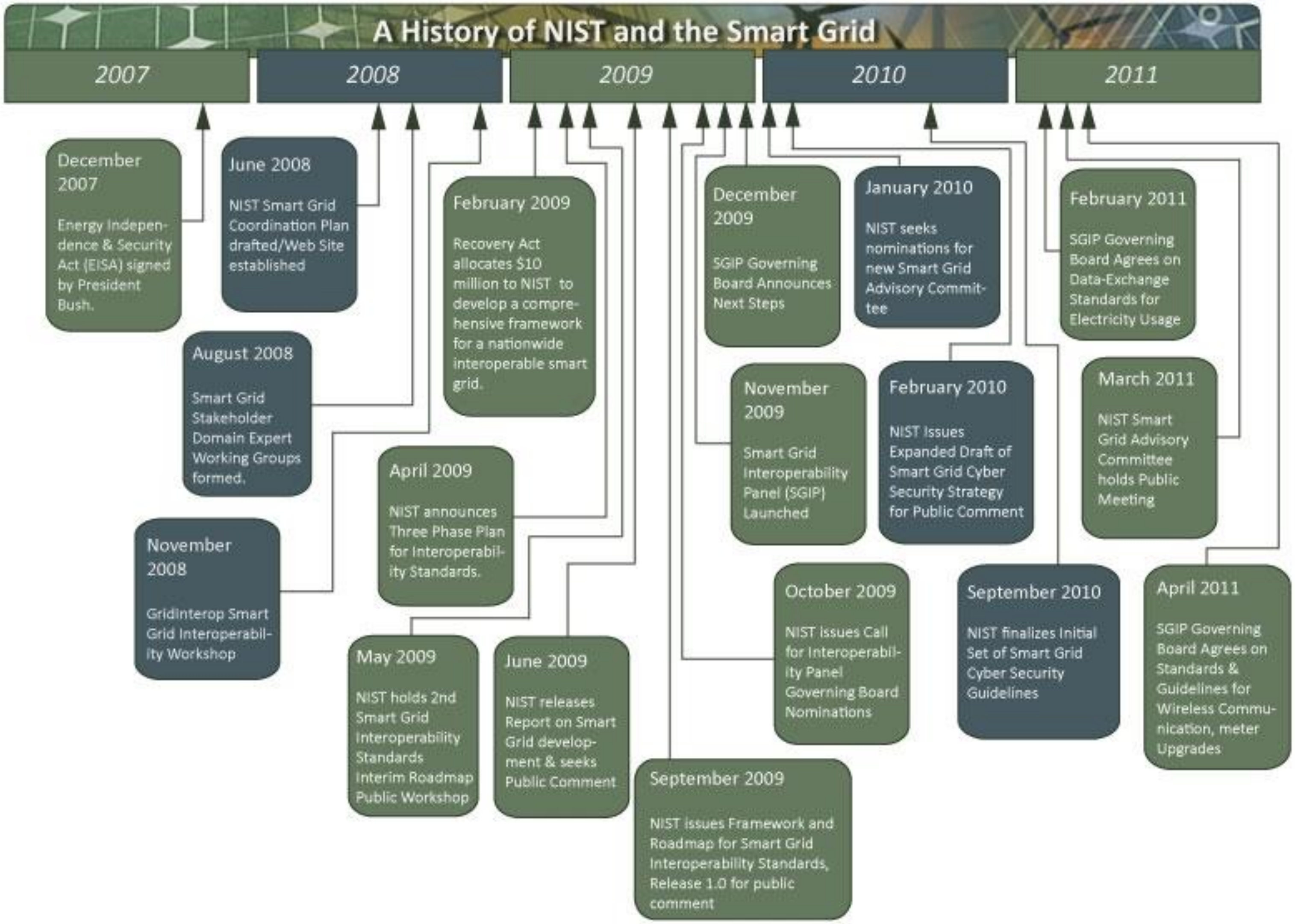
This draft of the second release of the *NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 2.0,* builds upon the work in Release 1.0 and is based on updated information and input from relevant stakeholders. Draft Release 2.0 includes a description of the Smart Grid conceptual reference model and conceptual architectural framework under development by the SGIP's Smart Grid Architecture Committee (SGAC) (Chapter 3); an update to the progress of the Priority Action Plans (PAPs) in closing the previously identified high-priority gaps; a listing of new standards emerging from the PAPs that have been added to the list of identified standards and the list of those for further review (Chapter 4); a description of the recently formed Smart Grid Interoperability Panel (SGIP) (Chapter 5); an expanded cybersecurity section (Chapter 6); and a new testing and certification section (Chapter 7).

This document is the second installment in an ongoing standards coordination and harmonization process. Ultimately, this process will deliver the hundreds of communication protocols, standard 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. This document serves to guide the work of the SGIP and support the safety, reliability, and security of the grid. As of July 2011, there are over 675 member organizations and over 1,790 member representatives in 22 Smart Grid stakeholder categories; 29 of these member representatives are from Canada and 47 more are from other countries, including China. The SGIP provides 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 conjunction with and integral to this process, NIST is coordinating the development of a Smart Grid cybersecurity framework and strategy, by the SGIP Cybersecurity Working Group (CSWG), prior to the establishment of the SGIP and now a part of it, which now comprises more than 550 technical experts. Results of the group's work are included in a companion Smart Grid document, NIST Interagency Report 7628, *Guidelines to Smart Grid Cyber Security* (NISTIR 7628), issued in September, 2010.[27] The Smart Grid cybersecurity framework and strategy will be completed in collaboration with the SGIP and its CSWG.

Working Draft

[27] *NISTIR 7628 Smart Grid Cyber Security Strategy and Requirements*, Sept. 2010. See: http://www.nist.gov/smartgrid/upload/nistir-7628_total.pdf.



December 2007

Energy Independence & Security Act (EISA) signed by President Bush.

June 2008

NIST Smart Grid Coordination Plan drafted/Web Site established

August 2008

Smart Grid Stakeholder Domain Expert Working Groups formed.

November 2008

GridInterop Smart Grid Interoperability Workshop

February 2009

Recovery Act allocates $10 million to NIST to develop a comprehensive framework for a nationwide interoperable smart grid.

April 2009

NIST announces Three Phase Plan for Interoperability Standards.

May 2009

NIST holds 2nd Smart Grid Interoperability Standards Interim Roadmap Public Workshop

June 2009

NIST releases Report on Smart Grid development & seeks Public Comment

September 2009

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

October 2009

NIST issues Call for Interoperability Panel Governing Board Nominations

November 2009

Smart Grid Interoperability Panel (SGIP) Launched

December 2009

SGIP Governing Board Announces Next Steps

January 2010

NIST seeks nominations for new Smart Grid Advisory Committee

February 2010

NIST Issues Expanded Draft of Smart Grid Cyber Security Strategy for Public Comment

September 2010

NIST finalizes Initial Set of Smart Grid Cyber Security Guidelines

February 2011

SGIP Governing Board Agrees on Data-Exchange Standards for Electricity Usage

March 2011

NIST Smart Grid Advisory Committee holds Public Meeting

April 2011

SGIP Governing Board Agrees on Standards & Guidelines for Wireless Communication, meter Upgrades

Figure 1-1. A History of NIST and the Smart Grid

1.2. Use of this Framework

The results of NIST's ongoing technical work reflected in this framework document should assist industry utilities, vendors, academia, regulators, and other Smart Grid stakeholders in future decision making. This document includes a compendium of standards that, in NIST's engineering judgment, are foundational to the Smart Grid. Standards identified in Table 4-1 and Table 4-2, below, have gone through an extensive vetting process, and are expected to stand the "test of time" as useful building blocks for firms producing devices and software for the Smart Grid.

The standards, however, are not static, and these tables include information on and web links to present and anticipated future changes to the standards. As they mature, these standards are undergoing revisions to add new functionalities to them, integrate them with legacy standards, harmonize them with overlapping standards, and remedy shortcomings that are revealed as their implementations undergo interoperability testing. The new testing and certification chapter includes information on efforts now under way to enable vendors and other Smart Grid stakeholders to certify the interoperability of devices being considered for a specific Smart Grid deployment.

Among the stakeholder groups who will find this document most useful are the following:

- For utilities and suppliers concerned with how best to understand and implement the Smart Grid, the document provides a conceptual architectural framework to guide implementations (Chapter 3), a compendium of reference standards (Chapter 4), an introduction to the extensive body of work newly available from NIST concerning Smart Grid privacy and security (Chapter 6), and a taxonomy of the various Smart Grid domains (Chapter 10).

- For testing laboratories and certification organizations, the new testing and certification chapter (Chapter 7) provides updates on efforts now under way to enable vendors and other Smart Grid stakeholders to certify the interoperability of devices being considered for a specific Smart Grid deployment;

- For those in academia, this document provides a benchmark of considerable progress made in advancing the hundreds of standards required for the Smart Grid. In addition, Chapter 8 and summaries of various PAP subgroup efforts in Chapter 5 point to additional research and innovation needed to fill gaps in our collective understanding of the tools, systems, and policies needed to deploy and manage what will be the largest single network yet deployed in the United States; and

- For regulators, the framework serves as a general introduction to both the challenge and promise of the Smart Grid (Executive Summary and Chapter 1), a guide to workable standards useful to delivering the best value for ratepayers by ensuring that technical investments by energy providers utilize standards wisely (Chapter 4), and an introduction to extensive work now under way through the SGIP's CSWG considering Smart Grid privacy and security matters (Chapter 6).

Working Draft

1.3. Key Concepts

The expedited development of an interoperability framework and a roadmap for underpinning standards, such as those outlined in this document, is a fundamental aspect of the overall transformation to a Smart Grid infrastructure. Although electric utilities are ultimately responsible for the safe and reliable operation of the grid, many other participants will be involved in the evolution of the existing electric power infrastructure. 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. To facilitate broad and deep input, the SGIP was established:

- To create a forum with balanced stakeholder governance that would bring together stakeholders with expertise in the many various areas necessary for the Smart Grid, including areas such as power engineering, communications, information technology (IT), and systems engineering;

- To support development of consensus; and

- To provide a source of expert input for the interoperability standards framework and roadmap.

This report contributes to an increased understanding of the key elements critical to realization of the Smart Grid, including standards-related priorities, strengths and weaknesses of individual standards, the level of effective interoperability among different Smart Grid domains, and cybersecurity requirements.

1.3.1. Definitions

Different stakeholders may hold a variety of definitions for the important terms that appear throughout the roadmap. 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.[28]

Energy Service Interface (ESI): The device or application that functions as the gateway between the energy providers and consumers. Located on the consumer side of the exchange,

Working Draft

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

this can have many forms. Its purpose is to facilitate communications between the consumer devices and the energy provider.

Functional Requirement: A requirement that specifies a function that a system or system component must be able to perform.[29]

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.[30] 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.[31]

Interchangeability: The ability of two or more components to be interchanged through mutual substitution without degradation in system performance.

Legacy Systems: A legacy system is an old technology, computer system, component, or application program that continues to be used, typically because it still functions for current users' needs, even though newer technology or more efficient methods of performing a task are now available.

Mature Standard: A mature standard is a standard that has been in use for long enough that most of its initial faults and inherent problems have been removed or reduced by further development.

Non-Functional Requirement: A non-functional requirement is a statement that specifies a constraint about how a system must behave to meet functional requirements.

Reference Model: A reference model is a set of views (diagrams) and descriptions that provides 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.

Reliability: The ability of a system or component to perform its required functions under stated conditions for a specified period of time. It is often measured as a probability of failure or a

[29] IEEE 610.12-1990 – IEEE Standard Glossary of Software Engineering Terminology. See http://standards.ieee.org/findstds/standard/610.12-1990.html.

[30] 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.

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

Working Draft

measure of availability. However, maintainability is also an important part of reliability engineering.

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 component to satisfy a contract, standard, specification, or other formally imposed document.[32]

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 organization and its purpose. These organizations include, but are not limited to, standards development organizations (SDOs), standards-setting organizations (SSOs), and user groups.

Additional terms pertinent to cybersecurity 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 *Guidelines to Smart Grid Cyber Security* (NISTIR 7628[33]).

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 cybersecurity and network communications. These functionalities are especially critical to ongoing and near-term deployments of Smart Grid technologies and services, and they include the priorities recommended by the Federal Energy Regulatory Commission (FERC) in its policy statement:[34]

- **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. With increased access to detailed energy consumption information, consumers can also save energy at all times with efficiency behavior and investments that achieve measurable results, and learn where additional efficiency investments will pay off.

Working Draft

[32] IEEE Std 610.12.

[33] http://csrc.nist.gov/publications/nistir/ir7628/introduction-to-nistir-7628.pdf.

[34] Federal Energy Regulatory Commission, *Smart Grid Policy*, 128 FERC ¶ 61,060 [Docket No. PL09-4-000] July 16, 2009 , http://www.ferc.gov/whats-new/comm-meet/2009/071609/E-3.pdf .

- **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.

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

- **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.

- **Network communications:** Refers to a variety of public and private communication networks, both wired and wireless, that will be used for Smart Grid domains and subdomains. 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. FERC notes, a "… cross-cutting issue is the need for a common semantic framework (i.e., agreement as to meaning) and software models for enabling effective communication and coordination across inter-system interfaces. An interface is a point where two systems need to exchange data with each other; effective communication and coordination occurs when each of the systems understands and can respond to the data provided by the other system, even if the internal workings of the system are quite different."[35] See Section 3.4 for further discussion on information networks.

- **Advanced metering infrastructure (AMI):** Provides real-time monitoring of power usage, and is a current focus of utilities. These advanced metering networks are of many different designs and could also be used to implement residential demand response including dynamic pricing. AMI consists of the communications hardware and software, and the associated system and data management software, that together create 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. Because the networks do not share a common format, NIST is focusing on standardizing the information data models.

- **Distribution grid management:** Focuses on maximizing performance of feeders, transformers, and other components of networked distribution systems and integrating them 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

Working Draft

[35] Proposed Policy Statement, 126 FERC ¶ 126, at p. 32.

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.[36]

- **Cybersecurity:** 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.[37]

1.4. Framework Content Overview

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

Chapter 3, **"**Conceptual Architectural Framework," 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. Because the Smart Grid is an evolving networked system of systems, the high-level model provides guidance for SSOs developing more detailed views of Smart Grid architecture.

Chapter 4, "Standards Identified for Implementation," presents and describes existing standards and emerging specifications applicable to the Smart Grid. It includes descriptions of selection criteria and methodology, 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, "Smart Grid Interoperability Panel," presents the mission and structure of the SGIP. The SGIP is a public-private partnership that is a membership-based organization established to identify, prioritize, and address new and emerging requirements for Smart Grid standards. The SGIP provides an open process for stakeholders to interact with NIST in the ongoing coordination, acceleration, and harmonization of standards development for the Smart Grid.

Chapter 6, "Cybersecurity Strategy," provides an overview of the content of NISTIR 7628 and the go-forward strategy of the Cybersecurity Working Group (CSWG). Cybersecurity is now being expanded to address the following: combined power systems; IT and communication systems in order to maintain the reliability of the Smart Grid; the physical security of all components: the reduced impact of coordinated cyber-physical attacks; and the privacy of consumers.

Chapter 7, "Testing and Certification," provides details on an assessment of existing Smart Grid standards testing programs and high-level guidance for the development of a testing and

Working Draft

[36] National Institute of Standards and Technology U. S. Department of Commerce. (2010 July). *Smart Grid Architecture and Standards: Assessing Coordination and Progress*. http://www.nist.gov/director/ocla/testimony/upload/DOC-NIST-testimony-on-Smart-Grid-FINAL-with-bio.pdf.

[37] Ibid.

certification framework. This chapter includes a comprehensive roadmap and operational framework for how testing and certification of Smart Grid devices will be conducted.

Chapter 8, “Next Steps,” contains a high-level overview of some of the currently foreseen areas of interest to the Smart Grid community, including electromagnetic disturbance and interference, and the “implementability” of standards.

Working Draft

2. Smart Grid Visions

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 future generations. Globally, billions of dollars are 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 of 2007 (EISA), which directed the National Institute of Standards and Technology (NIST) to coordinate development of this framework and roadmap, states that national policy supports the creation of a Smart Grid. Distinguishing characteristics of the Smart Grid cited in EISA include:[38]

- 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 cybersecurity;
- 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.

Working Draft

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

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:

> The applications 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**.**[39]

To monitor and assess the progress of deployments in the United States, DOE tracks activities grouped under six chief characteristics of the envisioned Smart Grid:[40]

- 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 cybersecurity 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 characteristics stipulate:[41]

- That the framework be "flexible, uniform and technology neutral, including but not limited to technologies for managing Smart Grid information";
- That it "be designed to accommodate traditional, centralized generation and transmission resources and consumer distributed resources";

Working Draft

[39] 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.

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

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

- That it be "designed to be flexible to incorporate regional and organizational differences; and technological innovations"; and
- That it 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'; and that "such voluntary standards should incorporate appropriate manufacturer lead time."

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[42]—an increase in capacity that is enough to power six million American homes. In the "State of the Union" address in January 2011, the President set a new goal: "By 2035, 80 percent of America's electricity will come from clean energy sources."[43]

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.[44] 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[45] and 15.5 million smart meters in American homes.[46] In addition, the modernized grid will include almost 700 automated substations and more than 1,000 sensors (phasor measurement units) that will cover the entire electric grid, which will enable operators to detect minor disturbances and prevent them from cascading into local or regional power outages or blackouts.[47] Progress toward realization of the Smart Grid will also contribute to accomplishing

Working Draft

[42] 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.

[43] The White House, Office of the Press Secretary, "Remarks by the President in State of the Union Address." January 25, 2011. See: http://www.whitehouse.gov/the-press-office/2011/01/25/remarks-president-state-union-address.

[44] 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.

[45] Ibid.

[46] http://www.smartgrid.gov/recovery_act/tracking_deployment/ami_and_customer_systems.

[47] 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.

the President's goal, reiterated in his 2011 State of the Union address, to “become the first country to have a million electric vehicles on the road by 2015.”[48] 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.[49]

In June 2011, the White House released a new report by the Cabinet-level National Science and Technology Council (NSTC) entitled “A Policy Framework for the 21st Century Grid: Enabling Our Secure Energy Future.”[50] This report outlines four overarching goals the Administration will pursue in order to ensure that all Americans benefit from investments in the nation’s electric infrastructure:

- Better alignment of economic incentives to boost development and deployment of Smart Grid technologies;
- Greater focus on standards and interoperability to enable greater innovation;
- Empowerment of consumers with enhanced information to save energy, ensure privacy, and shrink bills; and
- Improved cybersecurity and grid resilience.

This report calls on NIST and the Federal Energy Regulatory Commission (FERC) to continue to catalyze the development and adoption of open standards to ensure that the following benefits are realized:

- **Today’s investments in the Smart Grid remain valuable in the future.** Standards can ensure that Smart Grid investments made today will be compatible with advancing technology. Similarly, standards can ensure that Smart Grid devices are installed with proper consideration of the necessary security to enable and protect the grid of tomorrow;
- **Innovation is catalyzed.** Shared standards and protocols help reduce investment uncertainty by ensuring that new technologies can be used throughout the grid, lowering transaction costs and increasing compatibility. Standards also encourage entrepreneurs by enabling a significant market for their work;
- **Consumer choice is supported.** In the absence of Smart Grid interoperability standards, open standards developed in a consensus-based, collaborative, and balanced process, can alleviate concerns that companies may attempt to “lock-in” consumers by using proprietary technologies that make their products (and, therefore, their consumers’ assets) incompatible with other suppliers’ products or services;

Working Draft

[48] The White House, Office of the Press Secretary, “Remarks by the President in State of the Union Address.” January 25, 2011. See: http://www.whitehouse.gov/the-press-office/2011/01/25/remarks-president-state-union-address.

[49] 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.

[50] http://www.whitehouse.gov/sites/default/files/microsites/ostp/nstc-smart-grid-june2011.pdf.

- **Costs are reduced.** Standards can reduce market fragmentation and help create economies of scale, providing consumers greater choice and lower costs;
- **Best practices are highlighted as utilities face new and difficult choices.** Standards can provide guidance to utilities as they face novel cybersecurity, interoperability, and privacy concerns; and
- **Global markets are opened.** Development of international Smart Grid interoperability standards can help to open global markets, create export opportunities for U.S. companies, and achieve greater economies of scale and vendor competition that will result in lower costs for utilities and ultimately consumers.

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[51] 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.

Although the transition to the Smart Grid may unfold over many years, incremental progress along the way can yield significant benefits (see box below). In the United States, electric-power generation accounts for about 40 percent of human-caused emissions of carbon dioxide, the primary greenhouse gas.[52] 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.[53]

The opportunities are many and the returns can be sizable. If the current power grid were 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.[54] In its *National Assessment of Demand Response Potential*, FERC has 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.[55]

Working Draft

[51] 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.

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

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

[54] U.S. Department of Energy, *The Smart Grid: an Introduction*, 2008. See http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/DOE_SG_Book_Single_Pages(1).pdf.

[55] 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.

Anticipated Smart Grid Benefits

A modernized national electrical grid:

- Improves power reliability and quality
- Optimizes facility utilization and averts construction of backup (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
- Enables new products, services, and markets

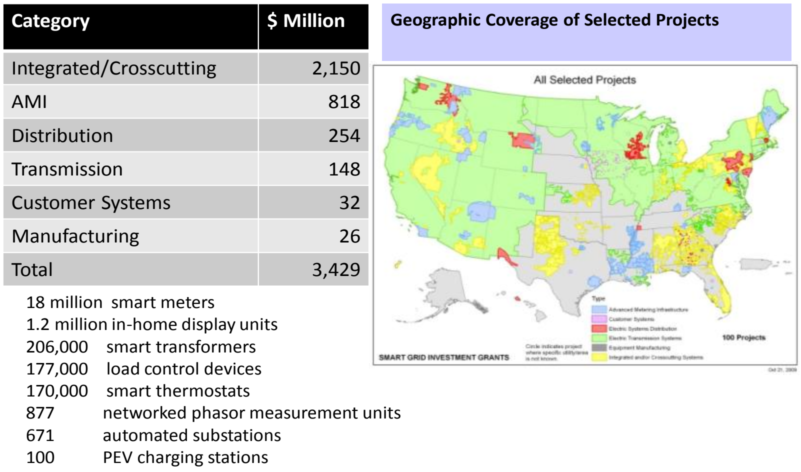
President Obama has called for a national effort to reduce the nation’s greenhouse gas emissions to 14 percent below the 2005 level by 2020, and to about 83 percent below the 2005 level by 2050.[56] Reaching these targets will require a more capable Smart Grid with end-to-end interoperability.

The transition to the Smart Grid already is under way, and it is gaining momentum, spurred by ARRA investments. On October 27, 2009, President Obama announced 100 awards under the Smart Grid Investment Grant Program.[57] 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 NIST’s emerging Smart Grid framework for standards and protocols.”[58]

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

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

[58] ibid.



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
All Selected Projects
Type
Advanced Metering Infrastructure
Customer Systems
Electric Systems Distribution
Electric Transmission Systems
Equipment Manufacturing
Integrated and/or Crosscutting Systems
100 Projects
Circle indicates project where specific utility/area is not known.
SMART GRID INVESTMENT GRANTS
Oct 21, 2009

Figure 2-1. Department of Energy Smart Grid Investment Grants, 2009[59]

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."[60] 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."[61]

2.3. International Smart Grid Standards

The Smart Grid will span the globe, and the United States is not alone in its initiative to modernize the electric grid. A number of other countries have launched significant efforts to encourage the development of the Smart Grid in their own countries and regions.

As countries move forward with their individual initiatives, it is very important that Smart Grid efforts are coordinated and harmonized internationally. An essential element of this coordination will be the development of international standards.

International coordination will provide a double benefit:

- As the United States and other nations construct their Smart Grids, use of international standards ensures the broadest possible market for Smart Grid suppliers based in the

Working Draft

[59] http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/815-830_Welcome-Overview-E-Lightner.pdf .

[60] U.S. Department of Energy, "Secretary Chu Announces Efforts to Strengthen U.S. Electric Transmission Networks," December 18, 2009. See: http://energy.gov/articles/secretary-chu-announces-efforts-strengthen-us-electric-transmission-networks.

[61] Ibid.

United States. By helping these American companies export their Smart Grid products, technologies, and services overseas, we will be encouraging innovation and job growth in a high-tech market of growing importance.

- The use of international standards results in efficiency for manufacturers and encourages supplier competition. As a result, costs will be lower, and those savings will benefit utilities and consumers.

NIST is devoting considerable resources and attention to bilateral and multilateral engagement with other countries to cooperate in the development of international standards for the Smart Grid. Among the countries that have or will begin investing in substantial Smart Grid infrastructure are Canada, Mexico, Brazil, the EU – including many member states, Japan, South Korea, Australia, India, and China.

In addition, NIST and the International Trade Administration (ITA) have partnered with the Department of Energy to establish the International Smart Grid Action Network (ISGAN), a multinational collaboration of 17 countries. ISGAN complements the Global Smart Grid Federation, a global stakeholder organization which serves as an "association of associations" to bring together leaders from Smart Grid stakeholder organizations around the world.

2.4. International Efforts to Harmonize Architectures

Because there are several architectures being developed by different Smart Grid stakeholder groups, NIST and the SGIP must coordinate with these groups to harmonize the architectures that will exist within the Smart Grid architectural framework, evaluating how well they support the architectural goals listed in Section 3.2. In the broadest perspective, the architectural framework being developed by the Smart Grid Architecture Committee (SGAC) of the SGIP provides an overarching perspective above other architectural efforts. These architectures will be evaluated against the conceptual reference model, the semantic framework, the standards and architecture evaluation criteria, and the conceptual business services.

Harmonization efforts are under way with (but are not limited to) the following groups:

- The Institute of Electrical and Electronic Engineers (IEEE) P2030 has been developing a view of the Smart Grid organized into three major areas: physical, communications, and information. This logical architecture conforms to the NIST Conceptual Reference Model and provides a set of defined interfaces for the Smart Grid. An SGAC/P2030 harmonization activity was begun in April 2011.
- The European Telecommunications Standards Institute (ETSI), together with the European Committee for Standardization (Comité Européen Normalisation - CEN) and the European Committee for Electrotechnical Standardization (CENELEC), have started the development of a Smart Grid architecture. The work is in an early stage, but it appears that it will provide a model that has similar deliverables to the SGAC work. The work will be focused on the requirements of European Union stakeholders. ETSI/CEN/CENELEC hosted a meeting in April 2011 to discuss collaboration on architectures, and a white paper describing common

Working Draft

principles and areas of cooperation between the SGIP and Europe's CEN/CENELEC/ETSI Smart Grid-Coordination Group (SG-CG) has now been published.[62]

- The SGAC has also initiated efforts to collaborate on architecture harmonization with:
    - The Chinese Electrical Power Research Institute (CEPRI). (The initial roadmap resembles much of the work done in the EU and the United States, with some very specific changes that support the difference in the Chinese market.)
    - The Korean Smart Grid Association (KSGA). (The KSGA has not published an architecture document yet, but pieces of the architecture have been released, including IT, physical field devices, and interfaces.)
    - The Japanese Federal Government. (Their architecture work has been focused, to a large extent, on the customer domain with strong links to the other six NIST Conceptual Reference Domains.)
    - IEC TC 57 and TC8 have architecture development artifacts under development and have published initial versions for standards integration across the IEC. This work is currently in progress.

Collaboration with additional groups to harmonize architectures will begin as they are identified.

2.5. Key Attributes- Standards and Conformance

The Smart Grid, unprecedented in its scope and breadth, will demand significant levels of cooperation to fully achieve the ultimate vision described in Section 2.1. Efforts directed toward enabling interoperability among the many diverse components of the evolving Smart Grid must address the following issues and considerations.

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 thousands of companies may construct individual components. Standards 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 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.[63] Globally, one prediction forecasts installation of 100

Working Draft

[62] http://www.nist.gov/smartgrid/upload/eu-us-smartgrids-white-paper.pdf.

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

million new smart meters over the next five years.[64]

Sound interoperability standards will 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 development, prioritization, and harmonization process must be systematic, not *ad hoc*.

Moreover, while standards are necessary to achieve interoperability, they are not sufficient. A conformance testing and certification framework for all Smart Grid equipment is also essential. NIST, in consultation with industry, government, and other stakeholders, has started to develop an overall framework for conformance testing and certification and plans to initiate steps toward implementation in 2011. This topic is discussed in greater detail in Chapter 7.

Working Draft

[64] 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 Architectural Framework

3.1. Introduction

The Smart Grid is a complex system of systems, serving the diverse needs of many stakeholders. Devices and systems developed independently by many different suppliers, operated by many different utilities, and used by millions of customers, must work together. Moreover these system must work together not just across technical domains but across smart grid "enterprises" as well as the smart grid industry as a whole. Achieving interoperability in such a massively scaled, distributed system requires architectural guidance, which is provided by the "conceptual architectural framework" described in this chapter.

The architectural framework will be used for several important purposes:

- To provide stakeholders a common understanding of the elements that make up the Smart Grid and their relationships;
- To provide traceability between the functions and the goals of the smart grid as provided by key stakeholder communities
- To provide a series of high level and strategic views of the envisioned systems
- To provide a technical pathway to the integration of systems across domains, companies, and businesses; and
- To guide the various architectures, systems, subsystems, and supporting standards that make up the Smart Grid.

The architectural framework described in this chapter includes the following:

- Architectural Goals for the Smart Grid (Section 3.2);
- Conceptual Reference Model, which comprises the conceptual domain models and the combined reference model (Section 3.3);
- Models for Smart Grid Information Networks (Section 3.4);
- Smart Grid Interface to the Customer Domain (Section 3.6); and
- Conceptual Business Services (Section 3.7.4).

Other important, architecture-related topics discussed in this chapter include the following:

- Use Cases (Section 3.5);
- Standards Review by the Smart Grid Architecture Committee (Section 3.7.1);
- Legacy Integration and Legacy Migration (Section 3.7.2); and
- Common Understanding of Information (Section 3.7.3).

Working Draft

Sections 3.2, 3.3, 3.4, 3.5, and 3.6 were included in *Framework 1.0* and have been updated here. Section 3.7 provides new material that summarizes work in progress by the Smart Grid Interoperability Panel (SGIP) Smart Grid Architecture Committee (SGAC).

3.2. Architectural Goals for the Smart Grid

Fundamental goals of architectures for the Smart Grid include:[65]

- **Options** – Architectures should support a broad range of technology options—both legacy and new. Architectures should be flexible enough to incorporate evolving technologies as well as to work with legacy applications and devices in a standard way, avoiding as much additional capital investment and/or customization as possible.
- **Interoperability** – Architectures must support interfacing with other systems. This includes the integration of interoperable third-party products into the management and cybersecurity infrastructures.
- **Maintainability** – Architectures should support the ability of systems to be safely, securely, and reliably maintained throughout their life cycle.
- **Upgradeability** – Architectures should support the ability of systems to be enhanced without difficulty and to remain operational during periods of partial system upgrades.
- **Innovation** – Architectures should enable and foster innovation. This includes the ability to accommodate innovation in regulations and policies; business processes and procedures; information processing; technical communications; and the integration of new and innovative energy systems.
- **Scalability** – Architectures should include architectural elements that are appropriate for the applications that reside within them. The architectures must support development of massively scaled, well-managed, and secure systems with life spans appropriate for the type of system, which range from 5 to 30 years.
- **Legacy** – Architectures should support legacy system integration and migration. (The key issue of dealing with legacy systems integration and migration is discussed in greater depth in Section 3.7.2.)
- **Security** – Architectures should support the capability to resist unwanted intrusion, both physical and cyber. This support must satisfy all security requirements of the system components. (This is covered in more detail in Chapter 6.).
- **Flexibility** – Architectures should allow an implementer to choose the type and order of implementation and to choose which parts of the architecture to implement without incurring penalties for selecting a different implementation.

Working Draft

[65] The list shown here is an expanded and revised version of the goals described in *Framework 1.0*, Section 2.3.1.

- **Governance** – Architectures should promote a well-managed system of systems that will is enabled through consistent policies over its continuing design and operation for its entire life cycle.
- **Affordability_** Should enable multivendor procurement of interoperable Smart Grid equipment through the development of mature national and international markets. Architecture should fundamentally enable capital savings as well as life cycle savings through standards-based operations and maintenance.

3.3. Conceptual Reference Model

3.3.1. Overview

The conceptual model presented in this chapter supports planning, requirements development, documentation, and organization of the diverse, expanding collection of interconnected networks and equipment that will compose the Smart Grid. For this purpose, the National Institute of Standards and Technology (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, programs, and stakeholders that make decisions and exchange information necessary for performing applications: smart meters, solar generators, and control systems are examples of devices and systems. Applications 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.

These actors, applications, and requirements for communications that enable the functionality of the Smart Grid are described in *use cases,* which are summaries of the requirements that define Smart Grid functions. A use case is a story, told in structured and detailed steps, about how actors work together to define the requirements to achieve Smart Grid goals.

Chapter 10 (Appendix: Specific Domain Diagrams) 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, called the combined reference diagram, that combines attributes of the seven domain-specific diagrams.

Working Draft

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

	Domain	**Actors in the Domain**
1	Customer	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.
2	Markets	The operators and participants in electricity markets.

3	Service Provider	The organizations providing services to electrical customers and utilities.
4	Operations	The managers of the movement of electricity.
5	Bulk Generation	The generators of electricity in bulk quantities. May also store energy for later distribution.
6	Transmission	The carriers of bulk electricity over long distances. May also store and generate electricity.
7	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. However, communications within the same domain may have different characteristics and may have to meet different requirements to achieve interoperability.

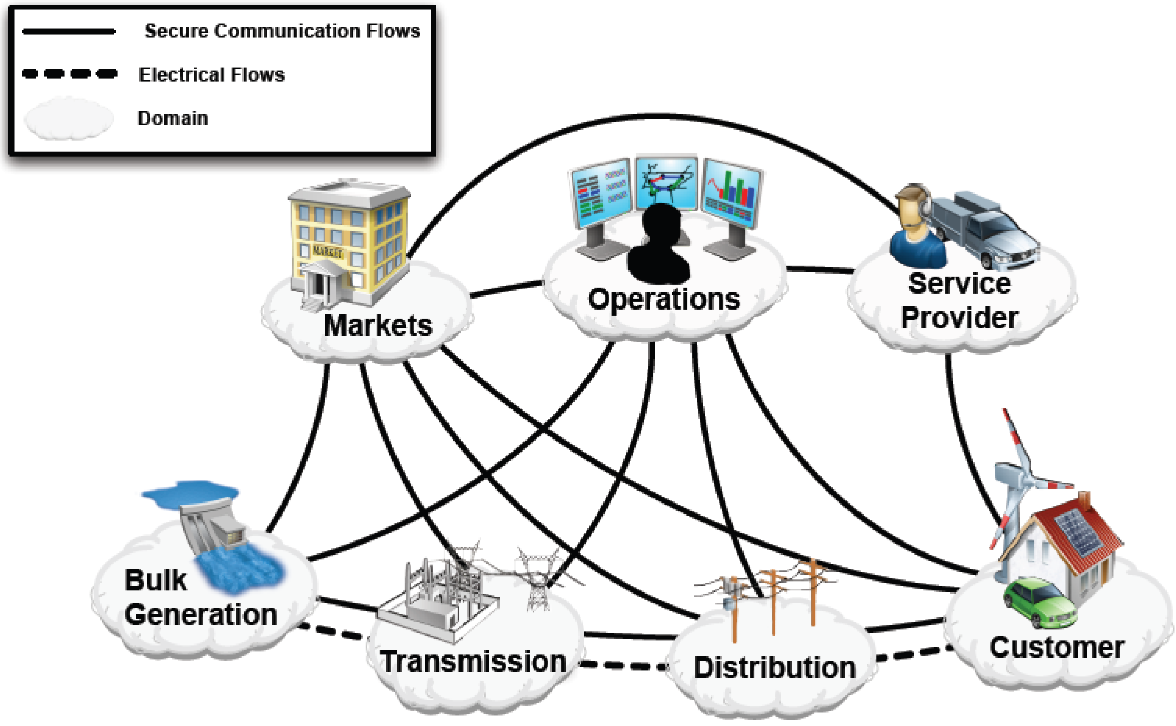
To enable Smart Grid functionality, the actors in a particular domain often interact with actors in other domains, as shown in Figure 3.1. Moreover, particular domains may also contain components of other domains. For example, the 10 Independent System Operators and Regional Transmission Organizations (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 enables the implementation and management of consistent policies and requirements that apply to various actors and applications and to their interactions. Regulations, adopted by the Federal Energy Regulatory Commission (FERC) 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.[66]

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 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. Therefore, the conceptual model must be consistent with the legal and regulatory framework and support its evolution over time. Similarly, the standards and protocols identified in the framework must align with existing and emerging regulatory objectives and responsibilities.

Working Draft

[66] See, for example, the mission statements of the National Association of Regulatory Utility Commissioners (NARUC, http://www.naruc.org/about.cfm) and FERC (http://www.ferc.gov/about/about.asp).



NIST Smart Grid Framework

Figure 3-1. Interaction of Actors in Different Smart Grid Domains through Secure Communication

Working

3.3.2. Description of Conceptual Model

The conceptual model described here provides a high-level, overarching perspective of a few major relationships that are developing across the smart grid domains. 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, as well as the 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 in that it provides a view of the types of interaction development that is at the core of developing architectures for the Smart Grid; it is ***not*** a design diagram that defines a solution and its implementation. Architecture documentation goes much deeper than what is illustrated here, but stops short of specific design and implementation detail. In other words, the conceptual model is descriptive and not prescriptive. It is meant to foster understanding of Smart Grid operational intricacies but not meant to prescribe how a particular stakeholder will implement the Smart Grid.

Draft

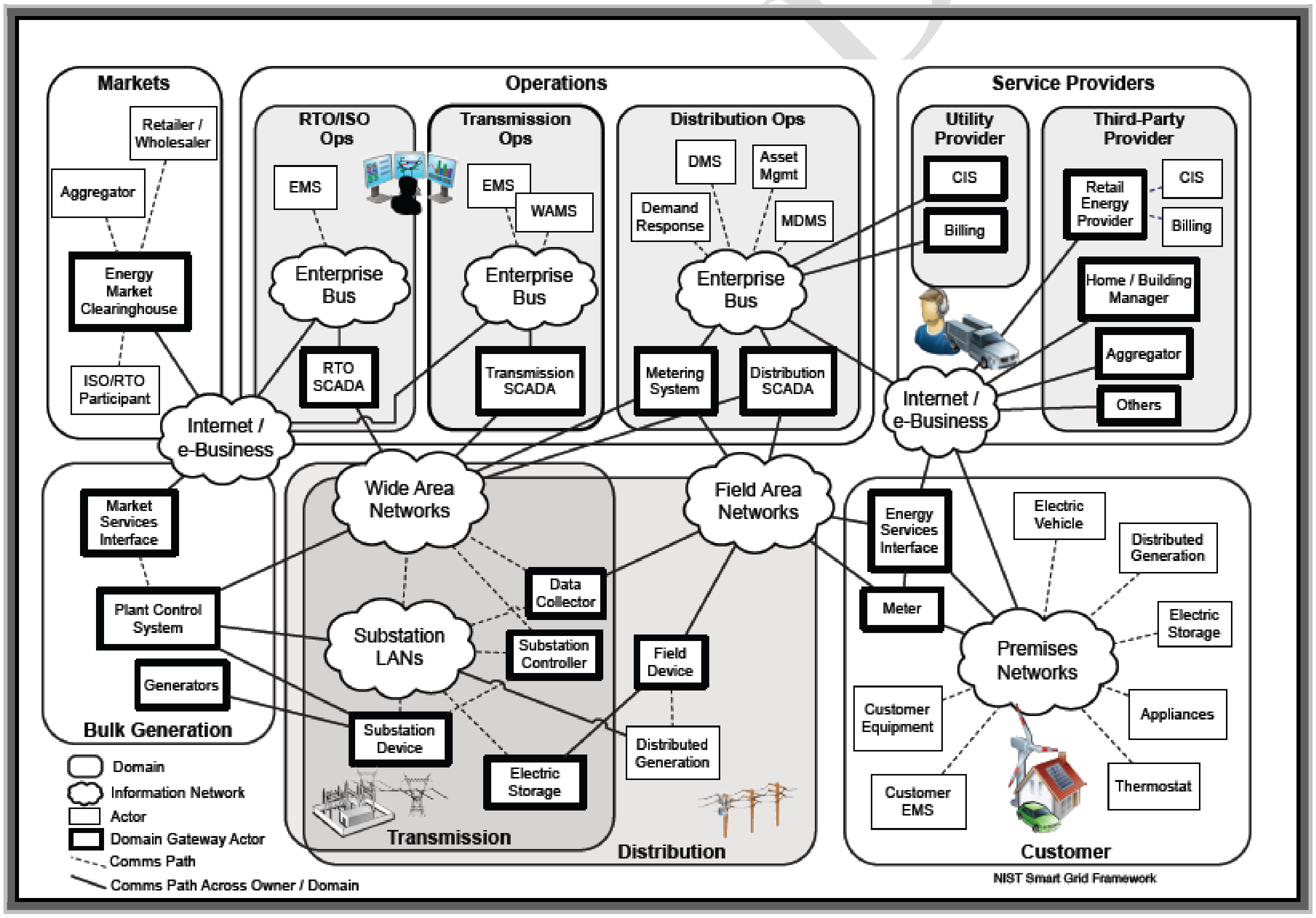


Figure 3-2. Conceptual Reference Diagram for Smart Grid Information Networks

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: A gateway actor is 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 may 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. Systems 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 and 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 a combination of public (e.g., the Internet) and nonpublic networks. 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: customers to third-party providers; bulk generators to grid operators; markets to grid operators; and third-party providers to utilities.

Comms (Communications) Path: The 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.

Working Draft

3.4. Models for Smart Grid Information Networks

The combined reference diagram, Figure 3-2, shows many comunication paths between and within domains. These paths illustrate key information flows between applications that reside both within and between domains.

Currently, various functions are supported by independent and, often, dedicated networks. Examples range from enterprise data and business networks, typically built on the Internet Protocol (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, transmission and 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. This information must be transmitted reliably over networks and must be interpreted consistently by applications. This requires that the meaning, or semantics, of transmitted information be well-defined and understood by all involved actors.

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 sub-network 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 compiled in collaboration with the Open Smart Grid/Smart Grid Network Task Force (OpenSG/SG-NET) and is being used by the Cybersecurity Working Group (CSWG) in the selection and tailoring of security requirements. (See Chapter 6.)

3.4.1. Information Network

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

Figure 3-3 is an illustration of information networks where Smart Grid control and data messages are exchanged. Clouds are used to illustrate networks handling two-way communications between devices and applications. The devices and applications are represented by rectangular boxes and belong to the seven different domains: Customer, Generation, Transmission, Distribution, Operations, Markets, and Service Provider, as identified in Table 3-1.

Working Draft

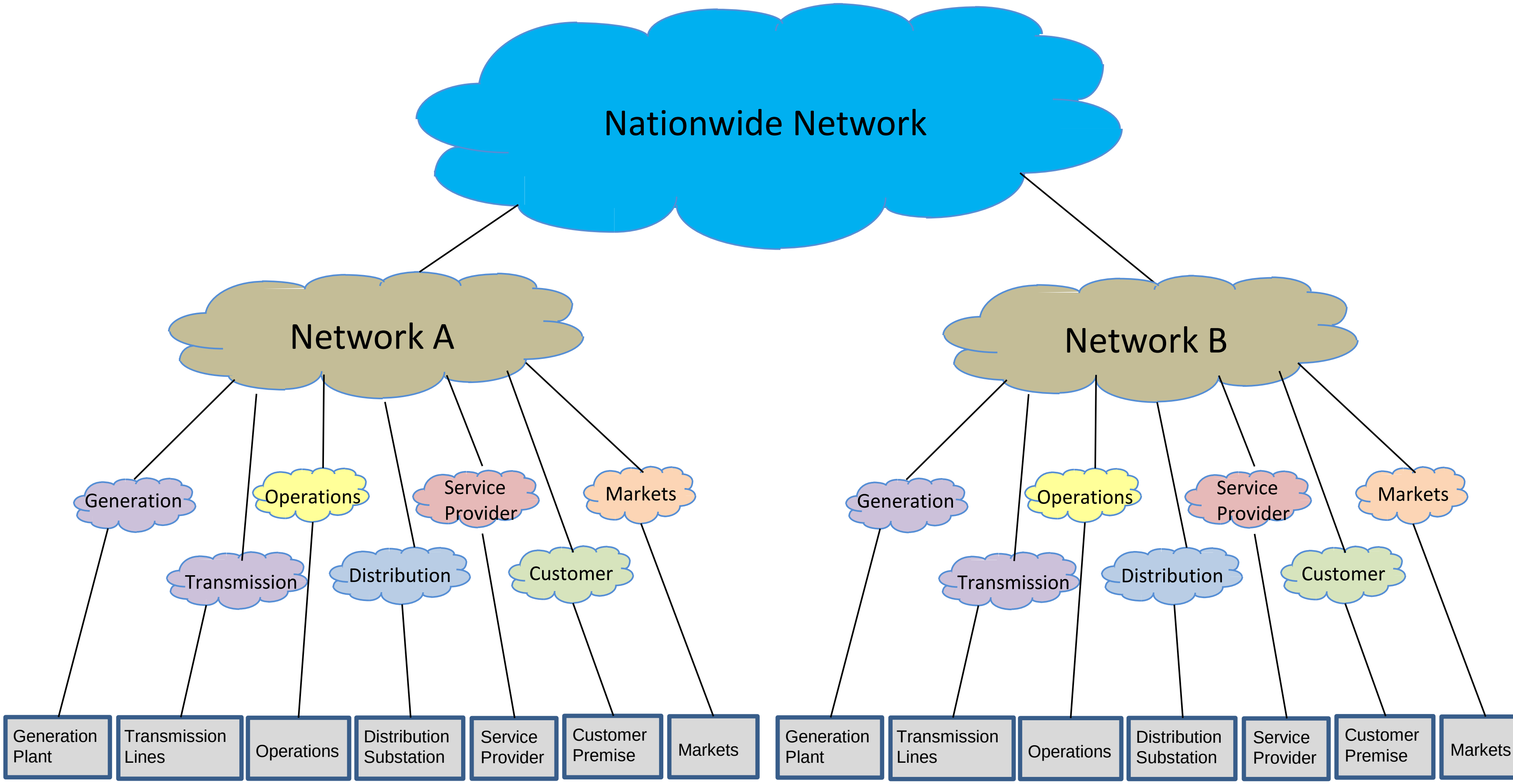


Figure 3-3. Smart Grid Networks for Information Exchange

Example 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 supervisory control and data acquisition (SCADA) systems and computers or display systems at the operation center. While SCADA systems may have different communication characteristics, other computer applications in the Operations, Markets, and Service Provider domains are similar to those in Web and business information processing, and their networking function may not be distinguishable from normal information processing networks.

Each domain-labeled network (for example, “Transmission,” “Generation,” or “Distribution”) is a unique distributed-computing environment and may have its own sub-networks to meet any domain-specific communication requirements.

The physical or logical links within and between these networks, and the links to the network end points, could utilize any appropriate communication technology currently available or to be developed and standardized in the future.

Within each network, a hierarchical structure consisting of multiple network types may be implemented. Some of the network types that may be involved are Home Area Networks, Personal Area Networks, Wireless Access Networks, Local Area Networks, and Wide Area Networks. 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 of all appropriate parameters (e.g., Who can be interconnected? Where? When? How?). Many network requirements need to be met including data management control, as well as network management such as configuration, monitoring, fault detection, fault recovery, addressability, service discovery, routing, quality of service, and security. Network security is a critical requirement to ensure that the confidentiality, integrity, and availability of Smart Grid information, control systems, and related information systems are properly protected. It may be necessary for regional networks, such as Network A and Network B in Figurer 3-3, to have interconnections. There is a need for international networks to connect between either the Nationwide Network or the regional networks, to meet the requirements that support international power flows such as between Canada and the U.S.

Given the diversity of the networks, systems, and energy sectors involved, ensuring adequate security is critical so that a compromise in one system 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 needs to be protected. Security includes the confidentiality, integrity, and availability of all related systems. The CSWG 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.

Working Draft

3.4.2. Security for Smart Grid Information Systems and Control System 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 malicious or accidental cybersecurity events 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 cybersecurity strategy is included in Chapter 6.

3.4.3. Internet Protocol (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 media. They allow applications to be developed independent of both the communication infrastructure and the various communication technologies to be used, whether they be wired or wireless.

Furthermore, IP-based networks enable bandwidth sharing among applications and provide increased reliability with dynamic-routing capabilities. For Smart Grid applications that have specific quality-of-service requirements (e.g., 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. An IP-based network by design is easily scalable, so new Smart Grid devices, such as smart meters, smart home appliances, and data concentrators in neighborhoods, could be readily added.

As the scale of IP-based networks for Smart Grid expands, the numbers of devices connected to the network is expected to increase substantially, and consequently the number of addresses needed in the IP network to uniquely identify these devices will increase as well. The fact that the available pool of Internet Protocol version 4 (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 Internet Protocol

Working Draft

version 6 (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.[67]

For each set of Smart Grid requirements, an analysis will determine whether IP is appropriate and whether cybersecurity and desired performance characteristics can be ensured. 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[68](IETF). These standards are commonly referred to as Request for Comments (RFCs). The definition of the necessary suite of RFCs will be dictated by the networking requirements, which have 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, the establishment and management of Smart Grid connections, and the packetization of Smart Grid application-specific data traffic over IP.

Working with SGIP's Priority Action Plan on IP (PAP01), the IETF has produced a new specification on Smart Grid, *RFC 6272 Internet Protocols for the Smart Grid.*[69] This document provides Smart Grid designers with guidance on how to use the the Internet Protocol Suite (IPS) in the Smart Grid. It provides an overview of the IPS and the key infrastructure protocols that are critical in integrating Smart Grid devices into an IP-based infrastructure; it also provides an example of how one might structure a network for advanced metering application.

3.4.4. Smart Grid and Public Internet: Security Concerns

One of the advantages of the Smart Grid is the ability to efficiently 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 CSWG as described in Chapter 6.

Working Draft

[67] NIST Information Technology Laboratory IPv6 Guide Provides Path to Secure Deployment of Next-Generation Internet Protocol. http://www.nist.gov/itl/csd/ipv6_010511.cfm.

[68] The Internet Engineering Task Force. http://www.ietf.org/.

[69] http://www.ietf.org/rfc/rfc6272.txt and http://tools.ietf.org/html/rfc6272.

3.4.5. Standards Technologies for Smart Grid Communication Infrastructure

There are a number of mature technologies available to support Smart Grid information networks. Network requirements determined to be necessary to support 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 developed by many standards development organizations (SDOs), including the SDOs accredited by the American National Standards Institute (ANSI), the Alliance for Telecommunications Industry Solutions (ATIS), and the Telecommunications Industry Association (TIA), as well as international SDOs, such as the International Telecommunication Union's Telecommunication Standardization Sector (ITU-T), the ITU's Radiocommunication Sector (ITU-R), and the Institute of Electrical and Electronics Engineers Standards Association (IEEE-SA). These standards cover transmission media such as optical fiber, coaxial cable, copper twisted pair, power lines, wireless, cellular, and satellite.

The selection of a specific technology for use in the Smart Grid depends on the requirements of applications and the environment in which the network is to operate. To assist Smart Grid designers in developing appropriate network architecture, the Priority Action Plan on Wireless Communications (PAP02), working with the OpenSG, has compiled a Smart Grid application communication requirements document.[70] In addition, PAP02 has provided methodologies and tools[71] for assessing the applicability of specific technologies. These requirements and tools are applicable to both wireless and wire line technologies.

3.5. Use Cases

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." A black-box use case describes the actor/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. Black-box use cases "descriptive." In contrast, white-box use cases describe the internal details of the system, in addition to the interaction and associated requirements. White-box use cases are "prescriptive," because they do not allow the implementer to change the internal system design.

Working Draft

[70] http://osgug.ucaiug.org/UtiliComm/Shared%20Documents/Interim_Release_4/SG%20Network%20System%20Requirements%20Specification%20v4.0.xls.

[71] NISTIR 7761, NIST Priority Action Plan 2, *Guidelines for Assessing Wireless Standards for Smart Grid Applications*, February 2011. http://collaborate.nist.gov/twiki-sggrid/pub/SmartGrid/PAP02Objective3/NIST_PAP2_Guidelines_for_Assessing_Wireless_Standards_for_Smart_Grid_Applications_1.0.pdf.

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, which describe the details of a particular solution, are prescriptive, they are not covered by the framework. 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 have already been developed, and the number will grow substantially. The scope of the body of existing use cases also covers cross-cutting requirements, including cybersecurity, network management, data management, and application integration, as described in the *GridWise Architecture Council Interoperability Context-Setting Framework.*[72]

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), attended by more than 600 people. This activity focused on six Smart Grid functionalities: wide-area situational awareness, demand response, energy storage, electric transportation, advanced metering infrastructure, and distribution grid management. The workshop utilized the Intelligrid^{SM}[73] approach for developing requirements from relevant use cases to identify the interoperability standards needed for the Smart Grid. More recently, a series of use case workshops were begun to continue the development of use cases to further the identification of requirements for the Smart Grid, and to further the standardization of use cases.

Detailed use cases can be found on the NIST Smart Grid Collaboration Site.[74] The use cases include the CSWG's use cases in priority and supplemental areas.

3.6. Smart Grid Interface to the Customer Domain

The interface between the Smart Grid and the Customer domain is of special importance as the most visible part of this domain.

Working Draft

[72] The GridWise Architecture Council. (2008, March). GridWise™ Interoperability Context-Setting Framework

http://www.gridwiseac.org/pdfs/interopframework_v1_1.pdf .

[73] *IEC PAS 62559, Edition 1.0, 2008-01, IntelliGrid^{SM} Methodology for Developing Requirements for Energy Systems.* See http://webstore.iec.ch/preview/info_iecpas62559%7Bed1.0%7Den.pdf.

[74] NIST Smart Grid Collaboration Site. IKB Use Cases http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/IKBUseCases.

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.

Through these interfaces, 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 interoperability challenge. In addition, ensuring cybersecurity is a critical consideration.

3.6.1. Distinction between the Meter and Energy Services Interface (ESI)

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 customers' 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 in place there for a very long time as the electrical interface to the electric utility. The meter may be 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.

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. Some third-party service providers 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

Working Draft

extensible to allow for innovation in market structures and services. Basic functions of the ESI include demand response signaling (e.g., 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. This is due to cost and the fact that Internet access is not universal. 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.

3.6.2. The ESI and the Home Area Network

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, such as 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 be able to participate in a demand response application. . 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. The Energy Independence and Security Act of 2007 (EISA) provides guidance on this issue. Section 1305 of EISA requires 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 advises that “such voluntary standards should incorporate appropriate manufacturer lead time.”

There are a large number of physical data communication interfaces—wired, wireless, and power line carrier (PLC)—presently available for establishing connectivity with residential devices, and there will be more in the future. Mass-produced appliances and consumer electronics differ

Working Draft

widely in terms of their expected service life and whether or not they are prone to regional relocation as consumers move. Makers of these devices may choose to embed one or more communication technologies in their products. The ESI could support a defined subset of widely used standard data communication protocols chosen from among those discussed in and listed in Chapter 4. Alternatively, the manufacturer may choose to employ a modular approach that would allow consumers to plug-in communication devices of their choosing. Work regarding standardization of a modular interface is currently under way in the Home-to-Grid (H2G) DEWG.

Many consumers and businesses are located in multi-unit buildings. Any data communication interfaces supported by the ESI and residential devices 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 the Internet Protocol suite as the network- and transport-layer protocols 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. Work regarding the ESI standards is currently under way in the Industry-to-Grid (I2G) and Building-to-Grid (B2G) Domain Expert Working Groups (DEWGs).

Working Draft

3.7. Ongoing Work of the Smart Grid Architecture Committee (SGAC)

The preceding sections of this chapter, Sections 3.2 – 3.6, provide updated versions of architecture-related material included in *Framework 1.0*. Since the publication of that earlier document, the SGAC has identified additional issues requiring attention. For the newly identified issues, SGAC subgroups, called Working Parties, have been established, some deliverables have been published, and much work is in process. The subsections below—and the collaborative Web pages listed here as references—provide a snapshot of the current status of SGAC activities as of July 2011.

3.7.1. Standards Review by the SGAC

As part of the overall NIST effort to identify standards and protocols that ensure Smart Grid interoperability, it is important to evaluate and review the architectural elements of each proposed standard. The SGIP's formal process for evaluating standards and adding them to the Catalog of Standards (see Section 4.2 for more details) includes a review by the SGAC.

To date, the SGAC has produced detailed reports that contain analyses and recommendations for improvements in the following standards:

- Association of Edison Illuminating Companies (AEIC) Metering Guidelines;
- ANSI C12.19: American National Standard For Utility Industry End Device Data Tables; ANSI C12.21: American National Standard Protocol Specification for Telephone Modem Communication;

- IETF RFC 6272: Internet Protocols for the Smart Grid;
- North American Energy Standards Board (NAESB) Energy Usage Information;
- National Electrical Manufacturers Association (NEMA) Upgradeability Standard (NEMA SG AMI 1-2009);
- Society of Automotive Engineers (SAE) J1772-TM: SAE Electric Vehicle and Plug in Hybrid Electric Vehicle Conductive Charge Coupler;
- SAE J2847/1: Communication between Plug-in Vehicles and the Utility Grid;
- SAE J2836/1: Use Cases for Communication between Plug-in Vehicles and the Utility Grid; and
- NISTIR Interagency Report (NISTIR) 7761: Guidelines for Assessing Wireless Standards for Smart Grid Applications.

In the coming months, the SGAC will continue to assess standards for review. To improve the evaluation process, the SGAC is developing a standards review checklist.[75] The SGAC has also formed teams to review the standards.

3.7.2. Legacy Devices and Systems

The integration of existing or "legacy" devices or systems is critical to the development of systems for the Smart Grid. Because Smart Grid goals include both innovation and upgradeability, the Smart Grid architectural framework must address the existence of legacy aspects as the Smart Grid systems evolve.

Legacy devices and systems are those that were designed and deployed in the past They have aspects (including devices, systems, protocols, syntax, and semantics) that exist due to past design decisions, and these aspects may be inconsistent with the current architectural requirements of the Smart Grid. Legacy aspects can nevertheless be integrated, by implementing an intervening layer (an "adapter") that provides conformance.

The decision of whether to implement adapters to integrate legacy devices or systems must be determined on a case-by-case basis. Sometimes adapters are a good solution, and they can satisfy functional and performance requirements and may increase system flexibility and support technology evolution. Alternatively, adapters may limit functionality or performance. The implementation of adapters may result in a lower initial cost but may also result in a higher maintenance cost and/or eventual replacement cost when they are retired. When considering legacy integration, a business case needs to include an evaluation of life cycle costs and benefits.

Working Draft

[75] http://collaborate.nist.gov/twiki-sggrid/pub/SmartGrid/SGIPDocumentsAndReferencesSGAC/SGAC_PAP_Closeout_Check_list_0v1.doc.

The requirements established for legacy integration should clearly specify the degree of conformance needed (e.g., minimum or full conformance). Every decision must be considered for its impact on the overall system. For example, a security issue in one system might have an undesired effect on another system even though the systems are only indirectly related.

Three key goals of legacy integration and migration are:

- New systems should be designed so that present or legacy aspects do not unnecessarily limit future system evolution.
- A reasonable time frame for adaptation and migration of legacy systems must be planned to ensure legacy investments are not prematurely stranded.
- Legacy systems should be integrated in a way that ensures that security and other essential performance and functional requirements are met.

The SGAC Heterogeneity Working Party is developing evaluation criteria and guidance for the integration of legacy systems, and the ongoing work is available on the SGAC Heterogeneity Working Party collaborative Web page.[76]

3.7.3.Common Understanding of Information

The Smart Grid requires a high degree of communication and interaction among many diverse systems owned by stakeholders who in some cases have not previously worked together. These systems typically have overlapping information requirements, but they may describe that information in different terms. A descriptive semantic model shows the data types and relationships between data types within a system. Usually, redesigning the applications to use the same semantic model (a model of the data types and relationships used in a system) internally is not a practical answer. The information expressed using one party's terminology (or model) must be *transformed* into the other party's terms to achieve integration.

The most straightforward way to implement any one transformation is to custom-build bilateral transformation code between two systems, often including tables of correspondence between the object instance identification used by each party. However, this approach is impractical when large numbers of systems are involved, which is the case with the Smart Grid. If there are "*n*" systems, then the number of transformations needed is on the order of n^2. This means that the software maintenance and expansion costs to meet new business needs may become prohibitive as the number of systems becomes large.

Canonical Data Models (CDMs)

To address the problem of scaling to large numbers of systems that use different semantic models, the Smart Grid requires a canonical data model (a single semantic model that a set of semantic models can be mapped into) to reduce the number of mappings from order n^2 to $n+1$. There are two basic parts to the concept of a canonical data model.

When CDMs are used, exchanges between applications are organized as shown in Figure 3-4.

[76] http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/SGIPHeterogeneitySGAC.

Working Draft

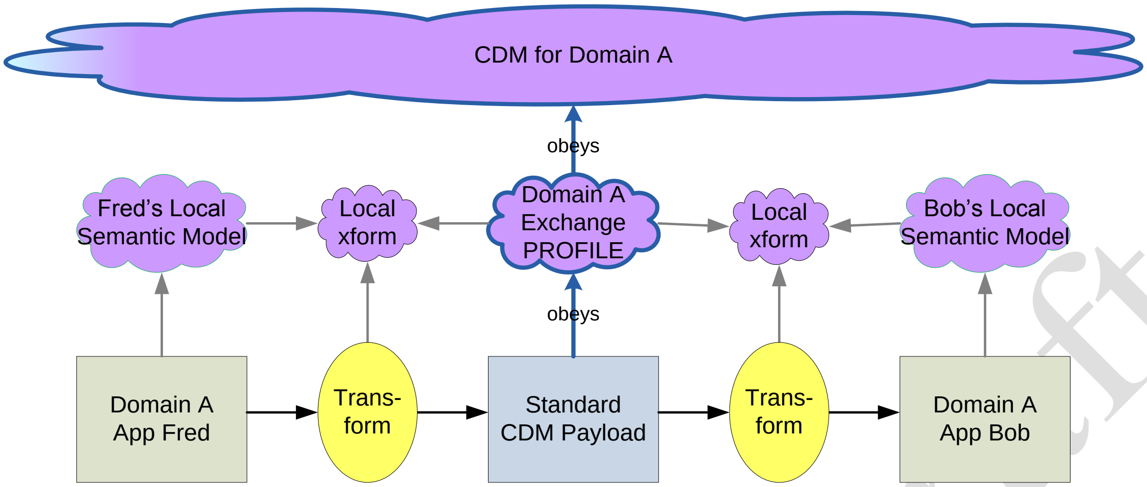


Figure 3-4. Exchange between Two Applications Governed by a Canonical Data Model (CDM)

In this picture, the producer application (App) has the obligation to transform its output to the canonical form, and then the receiver has the obligation to transform from the canonical form into the receiver form. Where multiparty exchanges exist, all parties transform only to the canonical form and never need to know the internal details of any other application. And, the canonical form of the individual exchange is derived from an overarching CDM that would also cover other related exchanges. Using this approach, a maximum of *n+1* transformations is needed.

The SGAC Smart Grid Semantic Framework

The Smart Grid is heavily dependent on the consistency of semantic models developed and maintained by SDOs to support the various systems of the Smart Grid. There is substantial benefit to promoting coordination and consistency of relevant semantic models within and across domains. The SGAC Semantic Working Party was established to begin to provide this desired coordination, and initial work has set the stage for future engagement of relevant stakeholders and SDOs in this effort. Planned deliverables, including the following, will be posted to the working party's collaborative Web page[77] as they are produced:

- Definitions of semantic concepts and methodologies for Smart Grid;
- Semantic harmonization scenarios for use by Smart Grid standards development groups. These scenarios will spell out how the framework can be used to integrate (in the general sense) two or more standards;
- Requirements to guide SDOs in the development and coordination of CDMs;
- A "map" showing the overall relationships among domain industry standard CDMs, and showing which standard exchanges belong to which domains;

Working Draft

[77] http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/SGIPSemanticModelSGAC.

- Documentation describing where exchanges go across domain boundaries and how harmonization between the domains is established;
- Identification of semantic methodologies, procedures, and design principles, along with identified toolsets; and
- A library of common semantic building blocks.

3.7.4. Conceptual Business Services

The SGAC has created a set of conceptual business services for the Smart Grid. The Open Group, an organization that promotes the development of open, vendor-neutral standards and certification,[78] defines a "business service" as a unit of business capability supported by a combination of people, process, and technology.[79] The SGAC used The Open Group's Architecture Framework (TOGAF) as a methodology for its work.

The output of the activity includes:

- An analysis of U.S. legislation and regulations pertaining to improving the grid;
- An analysis of goals, called goal decomposition, relating the high-level goals into lower business-level goals;
- A review of the use cases and requirements created by the Smart Grid community; and
- A set of conceptual services, or building blocks, that support these requirements.

The following building blocks will be used by the SGIP:

- To map SDO standards efforts to the overall Smart Grid "ecosystem." This mapping will help determine the location of gaps in the standards under development and also help determine where there are gaps in existing standards.
- To use the business services within the DEWGs to create prototype models by combining several business services. The Business and Policy Group is using them, for example, to develop a "prices to devices" white paper that will allow prices to be directly sent from wholesale markets to end devices.
- To compare the coverage of one Smart Grid architecture to the SGIP architecture framework and to the coverage of other Smart Grid architectures.

Working Draft

[78] See http://www3.opengroup.org/.

[79] http://pubs.opengroup.org/architecture/togaf9-doc/arch/chap22.html.

The Conceptual Architecture Development Working Party has been established to lead the SGAC's work in this area, and the outputs are published on its collaborative Web page.[80]

Working Draft

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

4. Standards Identified for Implementation

4.1. Guiding Principles Used for Identifying Interoperability Standards

The Energy Independence and Security Act of 2007 (EISA) assigns the National Institute of Standards and Technology (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.

Two lists are presented in this chapter:

- The first, Table 4-1 in Section 4.3, is a list of Smart Grid standards and specifications identified as important for the Smart Grid. Requirements documents and guidelines are also included in this table. Table 4-1 is based on the outcomes of several workshops, individual stakeholder inputs, Smart Grid Interoperability Panel (SGIP) Domain Expert Working Group (DEWG) discussions and work products, public comments solicited on both the standards and the first release of this framework document, and results of further reviews by the SGIP.

- The second list, Table 4-2 in Section 4.4, 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 workshops, stakeholder inputs, and public review. The work products and consensus beginning to emerge from these additional mechanisms are discussed in greater detail in Chapter 5.

The lists of standards in this release of the NIST Framework document include a number of updates to those presented in Release 1.0. The changes are as follows:

- Several standards have been moved from Table 4-2 (in Release 1.0) to Table 4-1 (in Release 2.0). These are standards that have emerged as part of the SGIP Priority Action Plans (PAPs) process and been recommended by the SGIP Governing Board for inclusion in the SGIP Catalog of Standards. Examples include the North American Energy Standards Board (NAESB) Wholesale Electric Quadrant (WEQ19), Retail Electric Quadrant (REQ) 18, Energy Usage Information that resulted from PAP10, and the Society of Automotive Engineers (SAE) standards that resulted from PAP11.

- Several standards that did not exist at the time Release 1.0 was completed in January 2010 have been added to the tables. In some cases, the added standards are closely related to standards already included on the lists. Among those added to Table 4-1, for example, is Institute of Electrical and Electronics Engineers (IEEE) Standard 1815, which is the adoption of the Distributed Network Protocol (DNP)3 standard by the IEEE and is now listed along

Working Draft

with DNP3 in Table 4-1. Among those standards added to Table 4-2 are standards now under development in the PAPs, such as Organization for the Advancement of Structured Information Standards (OASIS) Energy Interoperation (EI).

Because the Smart Grid is evolving from the existing power grid, NIST has also included standards that support widely deployed legacy systems. Priority Action Plans have been established with the goal of resolving interoperability issues between the standards for legacy equipment and other standards identified for the Smart Grid. For example, PAP12[81] seeks to enable implementations of the Distributed Network Protocol, DNP3 as specified in IEEE 1815, to work with implementations of the International Electrotechnical Commission (IEC) 61850 standard. In addition to the major principles, desirable and 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 initial and the current version (Release 2.0) of the *NIST Framework and Roadmap for Smart Grid Interoperability Standards*, and NIST will refine these criteria for use with subsequent versions. This set of criteria is extensive, and the complete list does not apply to each standard, specification, or guideline listed in Table 4-1 and Table 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- or specification-setting organizations (SSOs)" and "SDOs" are used loosely and interchangeably within the standards-related literature. However, for the purpose of this document, NIST is using the term "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 development organizations that develop standards in processes marked by openness, balance, and transparency, and characterized by due process to address negative comments. NIST uses the two terms, SSOs and SDOs, to address the wide variations in types of organizations that are developing standards, specifications, user guidelines, and other input, which are then being identified and considered for use in the Smart Grid framework.

Also, in this document, NIST uses the definition of voluntary consensus standards from Office of Management and Budget (OMB) Circular A-119, *Federal Participation in the Development and Use of Voluntary Consensus Standards and in Conformity Assessment Activities*,[82] where such standards are defined as developed and adopted by voluntary consensus standards bodies. For these voluntary consensus standards, OMB Circular A-119 outlines provisions that require that the relevant intellectual property owners have agreed to make that intellectual property available on a non-discriminatory, royalty-free, or reasonable-royalty basis to all interested parties. As defined in the OMB document, voluntary consensus standards bodies are "domestic or

Working Draft

[81] http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/PAP12DNP361850.

[82] OMB Circular A-119, *Federal Participation in the Development and Use of Voluntary Consensus Standards and in Conformity Assessment Activities*, February 10, 1998, http://standards.gov/a119.cfm.

international organizations which plan, develop, establish, or coordinate voluntary consensus standards using agreed-upon procedures,"[83] 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. Consensus includes a process for attempting to resolve objections by interested parties. The process includes the following attributes:

- All comments are considered fairly;
- 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, it is NIST's position that Smart Grid interoperability standards should be developed in processes that are open, transparent, balanced, and have due process, consistent with the decision of the World Trade Organization's Technical Barriers to Trade Committee Principles for the Development of International Standards.[84] That is, 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 or under the control of a single organization or group of organizations, and readily and reasonably available to all for Smart Grid applications."[85] In addition, Smart Grid interoperability standards should be developed and implemented internationally, wherever practical.

Because of the massive investment and accelerated time line 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 SDO-developed voluntary consensus standards. Rather, Table 4-1 and Table 4-2 also include specifications, requirements, and guidelines developed by other 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. The SSO documents were developed by user groups, industry alliances, consortia, and other organizations. Ultimately, however, it is envisioned that these specifications and other documents will be used for development of standards by SDOs.

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, however, that they will be made available under

Working Draft

[83] Ibid.

[84] Annex 4, *Second Triennial Review of the Operation and Implementation of the Agreement on Technical Barriers to Trade, WTO G/TBT/9, November 13, 2000*.

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

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. In 2010, NIST and the American National Standards Institute (ANSI) coordinated to make documentary standards available to SGIP working groups and other stakeholders for a limited time to support working group and PAP assignments.

Working Draft

Guiding Principles for Identifying Standards for Implementation

For *Release 2.0*, a standard, specification, or guideline is evaluated on whether it:

- Is well-established and widely acknowledged as important to the Smart Grid.
- Is an open, stable, and mature industry-level standard developed in a consensus process 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 standards- or specification-setting organization (SSO) such as a users group to ensure that it is regularly revised and improved to meet changing requirements and that there is a 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;
  - Cybersecurity; and
  - 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. See http://www.ferc.gov/whats-new/comm-meet/2009/071609/E-3.pdf .

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

- Focuses on the semantic understanding layer of the GWAC stack,[*] which has been identified as most critical to Smart Grid interoperability.
- Is openly available under fair, reasonable, and non-discriminatory terms.
- Has associated conformance tests or a strategy for achieving them.
- Accommodates legacy implementations.
- Allows for additional functionality and innovation through:
  - *Symmetry* – facilitates bidirectional 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 prearrangement.[**]
  - *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.

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

[**] 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 Table 4-1 of Section 4.3 and Table 4-2 of Section 4.4 in the initial (Release 1.0) and current (Release 2.0) versions of this document is described below. During the first phase of the NIST three-phase plan for Smart Grid interoperability, NIST's approach to accelerate the development of standards was to 1) identify existing standards that could be immediately applied to meet Smart Grid needs, or were 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.

After the publication of the *NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0,* and the establishment of the SGIP, NIST has transitioned the standard identification process so that it now works through various SGIP venues and activities. These venues include the many SGIP committees, SGIP working groups, PAPs, and numerous face-to-face meetings in conjunction with many industry conferences relevant to the Smart Grid, such as Connectivity Week (http://www.connectivityweek.com/), Grid Interop (http://www.gridinterop.com/), North American Synchro-Phasor Initiative (NASPI) working group meetings (http://www.naspi.org/), and IEEE Conferences and Committee meetings (http://www.ieee.org/index.html). A summary of the SGIP, the SGIP's Governing Board, various committees, working groups, and PAPs can be found in Chapter 5, and detailed information about them and their activities can be found on the NIST Smart Grid Collaboration Site.[86]

PAPs are established by the SGIP when there is a need for interoperability coordination on resolving urgent standards issues. The PAPs themselves are executed within the scope of the SSOs that assume responsibility for the tasks that implement the plans. The role of the SGIP is to facilitate this process, ensure that all PAP materials are publicly available to the extent possible as they are developed on the NIST Smart Grid Collaboration Site, and provide guidance as needed when significant differences among the participants in the PAP occur, or there is uncertainty about the PAP goals.[87] Once the issues are resolved, the standard resulting from the PAP and actions of the participating SSOs continues through the SGIP review and approval process and ultimately is listed in the SGIP Catalog of Standards (CoS)[88]. The CoS is discussed in greater detail in Section 5.3, where the purpose and scope, as well as the process and procedures for its management are described.

Note that the SGIP CoS is anticipated to be a key but not an exclusive source of input to the NIST process for coordinating the development of a framework of protocols and model standards for the Smart Grid under its EISA responsibilities.

The CoS is a compendium of standards and practices considered to be relevant for the development and deployment of a robust and interoperable Smart Grid. The CoS may contain multiple entries that may accomplish the same goals and are functionally equivalent; similarly, a single CoS entry may contain optional elements that need not be included in all implementations. In general, compliance with a standard does not guarantee interoperability due to the reasons given above. Though standards facilitate interoperability, they rarely, if ever, cover all levels of agreement and configuration required in practice. As a part of its work program, the SGIP is defining a testing and certification program that may be applied to the equipment, devices, and systems built to the standards listed in the CoS and that, if applied, will substantiate that implementations designed to the respective standards not only have compliance with the standards, but are also interoperable with one another. The CoS entry indicates where test profiles are defined and testing organizations identified for a particular standard.

Working Draft

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

[87] http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/PriorityActionPlans.

[88] http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/SGIPCatalogOfStandards#The_process_in_a_snapshot

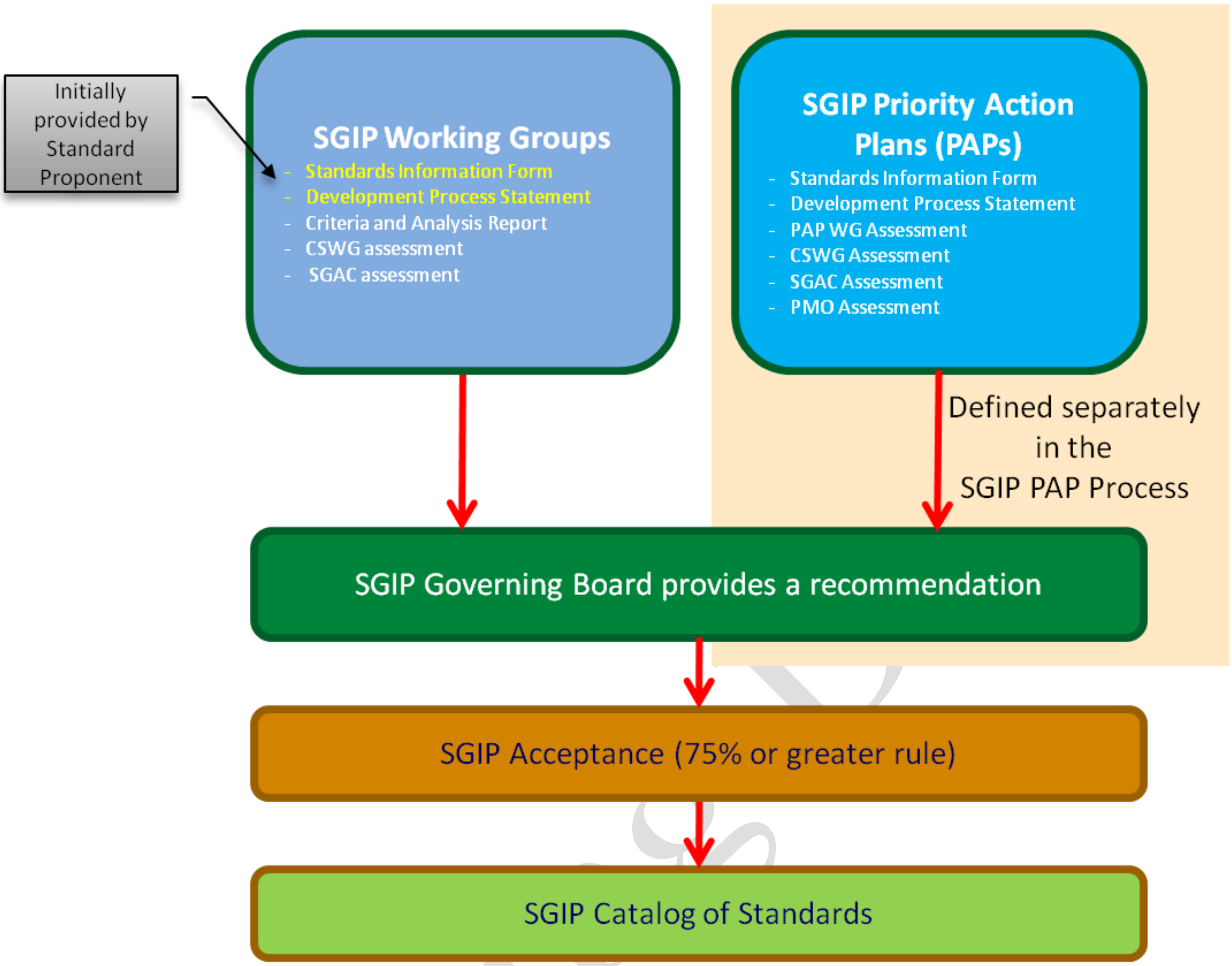

Initially provided by Standard Proponent
SGIP Working Groups
- Standards Information Form
- Development Process Statement
- Criteria and Analysis Report
- CSWG assessment
- SGAC assessment
SGIP Priority Action Plans (PAPs)
- Standards Information Form
- Development Process Statement
- PAP WG Assessment
- CSWG Assessment
- SGAC Assessment
- PMO Assessment
Defined separately in the SGIP PAP Process
SGIP Governing Board provides a recommendation
SGIP Acceptance (75% or greater rule)
SGIP Catalog of Standards

Figure 4-1. Basic Process by which Standards can be added to the Catalog of Standards (CoS)

The SGIP finalized the process for adding standards to the CoS in May, 2011. The process[89] includes review by the Standards Subgroup of the Cybersecurity Working Group (CSWG) to determine if the standards have adequately addressed cybersecurity requirements, which are defined in the NIST Interagency Report (NISTIR) 7628, *Guidelines for Smart Grid Cyber Security*.[90] The SGIP Smart Grid Architecture Committee (SGAC) also performs a review against its requirements, and the Governing Board votes to recommend the standard to the SGIP plenary, which then votes on whether to approve the standard for the CoS.

Since Table 4-1 and Table 4-2 were published in Release 1.0 before the CoS process was established, and a full cybersecurity review had not been performed on most of them, the

[89] http://collaborate.nist.gov/twiki-sggrid/pub/SmartGrid/SGIPGBDocumentsUnderReview/Standards_Catalog_Process_and_Structure_V0_9_20110401.pdf.

[90] http://csrc.nist.gov/publications/PubsNISTIRs.html#NIST-IR-7628.

cybersecurity review will be applied to all of the other standards identified in the tables below, as well as those identified in future NIST and SGIP activities. The following standards were reviewed in 2010: the NAESB Energy Usage Information, Oasis Web Services-(OASIS WS-) Calendar, Wireless Standards for the Smart Grid, Association of Edison Illuminating Companies (AEIC) Advanced Metering Infrastructure (AMI) Interoperability Standard Guidelines for ANSI C12.19 / IEEE 1377 / Measurement Canada (MC)12.19 End Device Communications and Supporting Enterprise Devices, Networks and Related Accessories; the following standards addressing plug in electric vehicles, SAE J1772-3, SAE J2836-1, SAE J2847-1, and National Electrical Manufacturers Association (NEMA) SG-AMI 1-2009: Requirements for Smart Meter Upgradeability and the Internet Protocol Suite. So far in 2011, cybersecurity reviews were completed for standards addressing time synchronization and Phasor Measurement Units (IEEE 1588, IEEE C37.238 IEC 61850-90-5), and AMI-related standards (C12.1, C12.18, C12.19, C12.21, C12.22).

Cybersecurity and architecture reviews will be applied to all of the other standards identified in the tables below, as well as those identified in future NIST and SGIP activities. Results of these reviews will be made publicly available on the Cybersecurity Working Group (CSWG) and Smart Grid Architecture Committee (SGAC) Web sites.[91] Standards organizations and prospective users of the reviewed specifications can use this information to address identified gaps or other issues. The CSWG has assigned liaisons to other working groups, PAPs, Domain Expert Working Groups (DEWGs), and SDOs to participate in and support the cybersecurity review of their activities when needed. Similarly, the SGAC has also assigned liaisons to these groups.

4.3. Current List of Standards Identified by NIST

As described previously, Table 4-1 lists the standards identified by NIST at the conclusion of the process described in Release 1.0,[92] which was a transparent and highly participatory public process. These standards support interoperability of Smart Grid devices and systems. The list also includes additional standards reviewed and recommended through the PAP development process and the SGIP Governing Board. Those standards have been moved from Table 4-2 in Release 1.0 to Table 4-1 in this release. Table 4-1 also includes standards coordinated by the PAPs and SGIP working groups and approved by the SGIP Plenary for the SGIP CoS. Table 4-1 groups the documents into families, such as the Internet Engineering Task Force (IETF) standards, and further identifies the families as standards and specifications, requirements, and guidelines. Cybersecurity standards appear together as a group in each of Table 4-1 and Table 4-2. These tables include the names of responsible standards bodies with links to the standard, the CSWG assessment, and to the draft SGIP Catalog of Standards information forms, if available, and a short description of the application and discussion of PAP and other standards activities that are applicable.

Working Draft

[91] http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/NISTStandardsSummaries.

[92] http://www.nist.gov/public_affairs/releases/upload/smartgrid_interoperability_final.pdf , p. 48.

All of the standards listed in Table 4-1 are subject to review by the SGIP CSWG Standards subgroup and the SGIP Smart Grid Architecture Committee (SGAC). The standards that have been reviewed as of July, 2011, by the CSWG and the SGAC are listed in Sections 6.3.2 and 3.7.1.

Table 4-1 now identifies 34 Smart Grid-relevant standards, and Table 4-2 identifies an additional 62 standards for further review. As noted in Table 4-1 and Table 4-2, many of the standards are undergoing development and require modifications, some of which are being addressed through the SGIP PAPs. The SGIP CSWG and the SGAC, whose ongoing efforts are described in more detail in Chapters 6 and 3, respectively, are also addressing some of these needed modifications. As discussed further in Chapter 7, experience gained with devices designed to meet the requirements of the standards from interoperability testing and certification activities managed by Interoperability Testing and Certification Authorities (ITCAs) will also influence the changes to these standards.

Working Draft

Table 4-1. Identified Standards

	Standard	**Application**	**Comments**
Standards and Specifications			
1	ANSI/American Society of Heating, Refrigeration, and Air Conditioning Engineers (ASHRAE) 135-2010/ISO 16484-5 BACnet http://www.techstreet.com/cgi-bin/basket?action=add&item_id=4427156 A Data Communication Protocol for Building Automation and Control Networks	BACnet defines an information model and messages for building system communications at a customer's site. BACnet incorporates a range of networking technologies, using IP protocols, to provide scalability from very small systems to multi-building operations that span wide geographic areas.	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 80 countries. BACnet serves as a customer domain communication protocol and is relevant to the Price, DR/DER, Energy Usage, and Facility Smart Grid Information Model PAPs (PAP03: Develop Common Specification for Price and Product Definition - http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/PAP03PriceProduct, PAP09: Standard DR and DER Signals - http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/PAP09DRDER, PAP10: Standard Energy Usage Information - http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/PAP10EnergyUsagetoEMS, and PAP17 Facility Smart Grid Information Standard - http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/PAP17FacilitySmartGridInformationStandard). Widely used in commercial, industrial and institutional buildings.
2	ANSI C12 Suite :		Open, mostly mature standards developed and maintained by an SDO. It is recognized that ANSI C12.19 version 2, and

Working Draft

	ANSI C12.1 http://webstore.ansi.org/RecordDetail.aspx?sku=ANSI+C12.1-2008 ANSI C12.18-2006: http://webstore.ansi.org/FindStandards.aspx?SearchString=c12.18&SearchOption=0&PageNum=0&SearchTermsArray=null|c12.18|null CSWG Report: http://collaborate.nist.gov/twiki-sggrid/pub/SmartGrid/CSCTGStandards/CSWG_Standards_ANSI_C12.18_Review_final.docx ANSI C12.19-2008 http://webstore.ansi.org/RecordDetail.aspx?sku=ANSI+C12.19-2008	Performance- and safety-type tests for revenue meters. Protocol and optical interface for measurement devices. Revenue metering End Device Tables.	correspondingly IEEE 1377 version 2, are extremely flexible metering data and information models that provide a wide range of functions and capabilities for delivery of actionable information, such as energy usage in kilowatt hours from a meter, such as energy usage information, load profiles and control information, such as load control, programming and firmware management. These capabilities call complex programming to secure the control and the information. ANSI C12.19 version 2 implements a comprehensive information class model by which the table and procedures classes and their class attributes are modeled using an extensible XML-based Table Definition Language (TDL). The instances of the data model (TDL classes) can be described in terms of the XML-based Exchange Data Language (EDL) that can be used to constrain oft-utilized information into a well-known form. The model and element instance information can be used by head end systems that implement ANSI C12.19 interoperable to communicate and manage any end device produced by any vendor company. PAP05 has been set up to establish consistent sets of commonly used data tables, procedures and services for meter information communication that will greatly reduce the time for utilities and others requiring to implement Smart Grid functions, such as demand response and real-time usage information (PAP05: Standard Meter Data Profiles). The task was undertaken by the Association of Edison Illuminating Companies

Working Draft

	CSWG Report http://collaborate.nist.gov/twiki-sggrid/pub/SmartGrid/CSCTGStandards/CSWG_Standards_ANSI_C12.19_Review_final.docx		(AEIC). AEIC completed a new interoperability standard on November 19, 2010, “SmartGrid/AEIC AMI Interoperability Standard Guidelines for ANSI C12.19 / IEEE 1377 / MC12.19 End Device Communications and Supporting Enterprise Devices, Networks and Related Accessories, Version 2.0.” The interoperability standard is also included in this table.
	ANSI C12.20 http://webstore.ansi.org/FindStandards.aspx?SearchString=c12.20&SearchOption=0&PageNum=0&SearchTermsArray=null|c12.20|null	Electricity Meters - 0.2 and 0.5 Accuracy Classes	It is recognized that C12.22 and correspondingly IEEE 1703 AMI communication frameworks are essential standards relevant to the Smart Grid and the communication of C12.19-based energy usage information and controls. The purpose of the ANSI C12.22 standard is to define the network framework and means to transport the Utility End Device Data Tables via any Local-area / Wide-area network for use by enterprise systems in a multi-source environment. The ANSI C12.22 was designed and it is intended to accommodate the concept of an advanced metering infrastructure (AMI) such as that identified by the Office of Electricity Delivery and Energy Reliability of the US Department of Energy; the Smart Metering Initiative of the Ontario Ministry of Energy (Canada); and the stated requirements of Measurement Canada for the approval of a metering device for use in Canada. ANSI C1.22 provides a uniform, managed, adaptive and secured network data and message delivery system for Utility End Devices and ancillary devices (e.g. home appliances and communication technology) that can operate in a
	ANSI C12.21/IEEE P1702/MC1221 http://webstore.ansi.org/FindStandards.aspx?SearchString=c12.21&SearchOption=0&PageNum=0&SearchTermsArray=null|c12.21|null	Transport of measurement device data over telephone networks.	

Working Draft

	CSWG Report http://collaborate.nist.gov/twiki-sggrid/pub/SmartGrid/CSCTGStandards/CSWG_Standards_ANSI_C12.21_Review_final.docx		"plug and play" and "end-to-end" multi-source enterprise AMI environment, in a manner that allows independence from the underlying network implementation. The independence from the underlying native network protects the C12.19 End Device from premature obsolescence that may occur as networks may come and go. Also, ANSI C12.22 extends the definitions provided by ANSI C12.19 standard to include provisions for enterprise-level asset management, data management, and uniform data exchange interfaces, through the use of network and relay tables and services. In addition it is to provide all the necessary support services needed to deploy, commission, notify, manage, and access End Devices in a manner that preserves privacy, security and the integrity of the network [ref. Section 1.2 Purpose IEEE 1377)]. This standard is also to be considered in the context of protecting smart meters from electromagnetic interference.
3	ANSI/CEA 709 and Consumer Electronics Association (CEA) 852.1 LON Protocol Suite: http://www.lonmark.org/technical_resources/standards	This is a general purpose local area networking protocol in use for various applications including electric meters, street lighting, home automation, and building automation.	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, Demand Response (DR)/Distributed Energy Resource (DER), and Energy Usage PAPs

Working Draft

	ANSI/CEA 709.1-B-2002 Control Network Protocol Specification http://www.ce.org/Standards/browseByCommittee_2543.asp	This is a specific physical layer protocol designed for use with ANSI/CEA 709.1-B-2002.	(PAP03: Develop Common Specification for Price and Product Definition - http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/PAP03PriceProduct, PAP09: Standard DR and DER Signals - http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/PAP09DRDER, and PAP10: Standard Energy Usage Information - http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/PAP10EnergyUsagetoEMS).
	ANSI/CEA 709.2-A R-2006 Control Network Power Line (PL) Channel Specification http://www.ce.org/Standards/browseByCommittee_2545.asp	This is a specific physical layer protocol designed for use with ANSI/CEA 709.1-B-2002.	
	ANSI/CEA 709.3 R-2004 Free-Topology Twisted-Pair Channel Specification http://www.ce.org/Standards/browseByCommittee_2544.asp	This is a specific physical layer protocol designed for use with ANSI/CEA 709.1-B-2002.	
	ANSI/CEA-709.4:1999 Fiber-Optic Channel Specification \www.ce.org\Standards\	This protocol provides a way to tunnel local operating network messages through an Internet Protocol (IP) network using the	

Working Draft

	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	User Datagram Protocol (UDP), thus providing a way to create larger internetworks.	
4	IEEE 1815 (DNP3) IEEE Xplore - IEEE Std 1815-2010 http://ieeexplore.ieee.org/xpl/mostRecentIssue.jsp?reload=true&punumber=5518535	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 initially developed and supported by a group of vendors, utilities, and other users, and now maintained by an SDO. IEEE has adopted it as an IEEE standard, IEEE Std 1815-2010, excluding the cybersecurity part which is being updated by IEEE Substation Committee Working Group (WG) C12. A Priority Action Plan (PAP12) was established to support transport of Smart Grid data and management functions between networks implementing IEEE 1815 and IEC 61850. PAP12 has coordinated actions on the development of mapping between IEC 61850 and IEEE 1815 (DNP3) objects that will allow presently communicated supervisory control and data acquisition (SCADA) information to be used

Working Draft

			in new ways, while also providing the ability to create new applications using the existing DNP3 infrastructure. A draft IEEE 1815.1 mapping standard has been developed, and a new working group C14 under IEEE substation committee has been established to adopt it as a formal IEEE standard. It is also anticipated to be adopted later by IEC as a dual-logo IEEE/IEC standard. (PAP12: Mapping IEEE 1815 (DNP3) to IEC 61850 Objects - http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/PAP12DNP361850).
5	IEC 60870-6 / Telecontrol Application Service Element 2 (TASE.2) http://webstore.iec.ch/webstore/webstore.nsf/artnum/034806) CSWG Report http://collaborate.nist.gov/twiki-sggrid/pub/SmartGrid/CSCTGStandards/StandardsReviewPhase-1Report.pdf Narrative http://collaborate.nist.gov/twiki-sggrid/pub/SmartGrid/N	This standard defines the messages sent between control centers of different utilities.	Open, mature standard developed and maintained by an SDO. It is widely implemented with compliance testing. This is part of the IEC 60870 Suite of standards. It is used in almost every utility for inter-control center communications between SCADA and/or Energy Management System (EMS) systems. It is supported by most vendors of SCADA and EMS systems.

Working Draft

	ISTStandardsSummaries/IEC_60870_Narrative_10-6-2010.doc		
6	IEC 61850 Suite http://webstore.iec.ch/webstore/webstore.nsf/artnum/033549!opendocument CSWG Report http://collaborate.nist.gov/twiki-sggrid/pub/SmartGrid/CSCTGStandards/StandardsReviewPhase-1Report.pdf Narrative http://collaborate.nist.gov/twiki-sggrid/pub/SmartGrid/NISTStandardsSummaries/IEC_61850_Narrative_10-6-2010.doc	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 with conformance testing that is developed and maintained by an SDO. It has been widely adopted world-wide and is starting to be adopted in North America. Developed initially for field device communications within substations, this set of standards is now being extended to communications between substations, between substations and control centers, and including hydroelectric plants, DER, and synchrophasors. It is also adapted for use in wind turbines (IEC 61400-25) and switchgears (IEC 62271-3). Several PAPs (PAP07, PAP08, PAP12, and PAP13) are dedicated to further development work in various areas. PAP07 has developed requirements to update IEC 61850-7-420 Distributed Energy Resource (DER) Information Models to include storage devices and Smart Grid functionality necessary to support high penetration of DER. PAP07 is also mapping the information models to application protocols including Smart Energy Profile (SEP)2 and DNP3. The new information models requirements are included in the IEC Technical Report, IEC 61850-90-7 which is expected to be completed in June 2011 and will also be included in the modified normative standard that will

Working Draft

			follow. (PAP07: Energy Storage Interconnection Guidelines - http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/PAP07Storage) PAP12 has been working on the mapping of IEEE 1815 (DNP3) to IEC 61850 objects, and it has resulted in a draft IEEE standard P1815.1 being completed in early 2011 for adoption by IEEE around mid-2011. (PAP12: Mapping IEEE 1815 (DNP3) to IEC 61850 Objects - http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/PAP12DNP361850) PAP13 is established to assist and accelerate the integration of standards (IEEE C37.118 and IEC 61850) that impact phasor measurement systems and applications that use synchrophasor data, as well as implementation profiles for IEEE Std 1588 for precision time synchronization. (PAP13: Harmonization of IEEE C37.118 with IEC 61850 and Precision Time Synchronization - http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/PAP1361850C27118HarmSynch) IEEE will split current IEEE C37.118-2005 into two parts in its new revision to facilitate the harmonization with IEC standards: C37.118.1

Working Draft

			Standard for synchrophasor measurements for power systems aimed to become an IEEE/IEC dual-logo standard, and C37.118.2, Standard for synchrophasor data transfer for power systems to be harmonized with / transitioned to IEC 61850-90-5, which is currently under development. PAP8 is working on harmonizing this family of standards, the IEC 61970 family of standards (Common Information Model or CIM), and Multispeak for distribution grid management (PAP08: CIM/61850 for Distribution Grid Management - 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 CSWG Report http://collaborate.nist.gov/twiki-sggrid/pub/SmartGrid/CSCTGStandards/StandardsReviewPhase-1Report.pdf Narrative IEC 61968 http://collaborate.nist.go	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 PAP08 activities relating to integration with IEC 61850 and Multispeak (PAP08: CIM/61850 for Distribution Grid Management - http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/PAP08DistrObjMultispeak). .

Working Draft

	v/twiki-sggrid/pub/SmartGrid/NISTStandardsSummaries/IEC_61968_Narrative_10-6-2010.doc Narrative IEC 61970 http://collaborate.nist.gov/twiki-sggrid/pub/SmartGrid/NISTStandardsSummaries/IEC_61970_Narrative_10-6-2010.doc		
8	IEEE C37.118-2005 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 (To be published as IEEE C37.118.1 and IEEE C37.118.2 in its new revision)	This standard defines phasor measurement unit (PMU) performance specifications and communications for synchrophasor data.	Open standard, 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 and H19. Some items not covered in C37.118-2005 include communication service modes, remote device configuration, dynamic measurement performance, and security. IEEE will split current IEEE C37.118-2005 into two parts in its new revision to facilitate the harmonization with IEC standards: C37.118.1 “Standard for synchrophasor measurements for power systems” by IEEE PSRC WG H11 to become an IEEE/IEC dual-logo standard, and C37.118.2, “Standard for synchrophasor data

Working Draft

			transfer for power systems" by IEEE PSRC WG H19 to be harmonized with / transitioned to IEC 61850-90-5, which is currently under development. IEEE PSRC WG C5 is developing a "Guide for Synchronization, Calibration, Testing, and Installation of Phasor Measurement Units (PMU) applied in Power System Protection and Control" based on the C37.118 standards and previous publications by North American Synchro-Phasor Initiative (NASPI) in these areas. They are part of PAP13 relating to harmonization of IEC 61850 and IEEE C37.118 standards (PAP13: Harmonization of IEEE C37.118 with IEC 61850 and Precision Time Synchronization - http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/PAP1361850C27118HarmSynch).
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 utilities and distributed generation (DG) and storage.	Open standards developed and maintained by an SDO 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 PAP07, covering energy storage interconnections (PAP07: Energy Storage Interconnection Guidelines -

Working Draft

			http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/PAP07Storage). When applied to utility-interactive equipment, Underwriters Laboratories (UL) 1741, "Standard for Safety Inverters, Converters, Controllers and Interconnection System Equipment for Use With Distributed Energy Resources," should be used in conjunction with 1547 and 1547.1 standards which supplement them. The products covered by these requirements are intended to be installed in accordance with the National Electrical Code, National Fire Protection Association (NFPA) 70.
10	IEEE 1588 http://ieee1588.nist.gov/ IEEE C37.238 http://standards.ieee.org/develop/project/C37.238.html	Standard for time management and clock synchronization across the Smart Grid for equipment needing consistent time management.	Open standard. Version 2 is not widely implemented for power applications. Developed and maintained by an SDO. IEEE PSRC Subcommittee Working Group H7 is developing a new standard C37.238 (IEEE Standard Profile for use of IEEE Std. 1588 Precision Time Protocol in Power System Applications). The new standard is part of PAP13, which covers incorporating precision time synchronization with harmonization of IEEE and IEC standards for communications of phasor data (http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/PAP1361850C27118HarmSynch).

Working Draft

11	Internet Protocol Suite, Request for Comments (RFC) 6272, Internet Protocols for the Smart Grid. CoS Web page: http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/SGIPCosSIFIETFRFC6272	Internet Protocols for IP-based Smart Grid Networks IPv4/IPv6 are the foundation protocol for delivery of packets in the Internet network. Internet Protocol version 6 (IPv6) is a new version of the Internet Protocol that provides enhancements to Internet Protocol version 4 (IPv4) and allows a larger address space.	A set of open, mature standards produced by IETF for Internet technologies. As part of the tasks for PAP01 (PAP01: Role of IP in the Smart Grid - http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/PAP01InternetProfile), a core set of IP protocols has been identified for Smart Grid. After review by PAP01, CSWG, and SGAC, it has been recommended by the SGIP Governing Board (SGIPGB) and approved by the SGIP Plenary for inclusion in the SGIP Catalog of Standards. The list has been published by the IETF as RFC6272, which identifies the key protocols of the Internet Protocol Suite for Use in the Smart Grid. The target audience is those people seeking guidance on how to construct an appropriate Internet Protocol Suite profile for the Smart Grid.
12	Inter-System Protocol(ISP)-based Broadband-Power Line Carrier (PLC) coexistence mechanism: (Portion of) IEEE 1901-2010 (ISP) and International Telecommunications Union Telecommunication Standardization Sector (ITU-T) G.9972 (06/2010)	Both IEEE 1901-2010, "IEEE Standard for Broadband over Power Line Networks: Medium Access Control and Physical Layer Specifications," and ITU-T G.9972 (06/2010), "Coexistence mechanism for wireline home networking transceivers," specify Inter-System Protocol (ISP) based Broadband (> 1.8 MHz) PLC (BB-PLC) coexistence mechanisms to enable the coexistence of different BB-PLC protocols for home networking.	Open standards developed and maintained by SDOs. Both IEEE 1901 and ITU-T G.9972 are developed and maintained by SDOs. Through coordination by PAP15 (PAP15: Harmonize Power Line Carrier Standards for Appliance Communications in the Home - http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/PAP15PLCForLowBitRates), the divergence between the two standards has been successfully eliminated before ratification. IEEE 1901-compliant devices implementing either one of the two IEEE 1901 Physical(PHY)/Media Access Control(MAC) Layers can coexist with each other. Likewise, ITU-

Working Draft

	IEEE 1901-2010 https://sbwsweb.ieee.org/ecustomercme_enu/start.swe?SWECmd=GotoView&src=0&Join=n&SWEView=Catalog+View+%28eSales%29_Main_JournalMags_IEEE&mem_type=Customer&HideNew=N&SWEHo=sbwsweb.ieee.org&SWETS=1298228970 ITU-T G.9972 http://www.itu.int/rec/T-REC-G.9972-201006-P/en		T G.9960/9961 devices that implement ITU-T G.9972 can coexist with IEEE 1901-compliant devices implementing either one of the two IEEE P1901 PHY/MACs, and vice versa.
13	Multispeak http://www.multispeak.org/about/Specification/Pages/default.aspx	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's task for harmonization of IEC 61850/CIM and Multispeak (PAP08: CIM/61850 for Distribution Grid Management - http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/PAP08DistrObjMultispeak).
14	NEMA Smart Grid Standards Publication SG-AMI 1-2009 –	This standard will be used by smart meter suppliers, utility customers, and key constituents,	This standard serves as a key set of requirements for smart meter upgradeability. These requirements should be used by smart meter

Working Draft

	Requirements for Smart Meter Upgradeability http://www.nema.org/stds/sg-ami1.cfm CoS Web page: http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/SGIPCosSifSGAMI1	such as regulators, to guide both development and decision making as related to smart meter upgradeability.	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. This standard was coordinated by PAP00 Meter Upgradeability Standard - http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/PAP00MeterUpgradability and has been recommended by the SGIPGB and approved by the SGIP Plenary for the CoS.
15	NAESB WEQ19, REQ18, Energy Usage Information http://www.naesb.org/member_login_check.asp?doc=weq_rat102910_weq_2010_ap_6d_rec.doc, http://www.naesb.org/member_login_check.asp?doc=req_rat102910_req_2010_ap_9d_rec.doc CoS Web page: http://collaborate.nist.go	The standards specify two-way flows of energy usage information based on a standardized information model.	Open standards, developed and maintained by an SDO. These are new standards to be adopted and deployed. It will be a basis for additional standards and recommendations including those from PAP17; also used as input for Energy Interoperation. The standards have been reviewed by PAP10 (PAP10: Standard Energy Usage Information - http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/PAP10EnergyUsagetoEMS) and SGAC. It has been recommended by the SGIP Governing Board and approved by the SGIP Plenary for inclusion in the Catalog of Standards.

Working Draft

	v/twiki-sggrid/bin/view/SmartGrid/SGIPCosSIFNAESBREQ18WEQ19		
16	NISTIR 7761, NIST Guidelines for Assessing Wireless Standards for Smart Grid Applications *http://collaborate.nist.gov/twiki-sggrid/pub/SmartGrid/PAP02Objective3/NIST_PAP2_Guidelines_for_Assessing_Wireless_Standards_for_Smart_Grid_Applications_1.0.pdf* CoS Web page: http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/SGIPCosSIFNISTIR7761	This report is a draft of key tools and methods to assist smart grid system designers in making informed decisions about existing and emerging wireless technologies. An initial set of quantified requirements have been brought together for advanced metering infrastructure (AMI) and initial Distribution Automation (DA) communications. These two areas present technological challenges due to their scope and scale. These systems will span widely diverse geographic areas and operating environments and population densities ranging from urban to rural.	The wireless technologies presented here encompass different technologies that range in capabilities, cost, and ability to meet different requirements for advanced power systems applications. System designers are further assisted by the presentation of a set of wireless functionality and characteristics captured in a matrix for existing and emerging standards-based wireless technologies. Details of the capabilities are presented in this report as a way for designers to initially sort through the available wireless technology options. To further assist decision making, the document presents a set of tools in the form of models that can be used for parametric analyses of the various wireless technologies.

Working Draft

17	Open Automated Demand Response (OpenADR http://openadr.lbl.gov/pdf/cec-500-2009-063.pdf)	The specification defines messages exchanged between the Demand Response (DR) Service Providers (e.g., utilities, independent system operators (ISOs) and customers for price-responsive and reliability-based DR	Developed by Lawrence Berkeley National Laboratory and California Energy Commission and is currently supported by the OpenADR Alliance. Demand response signals are currently being standardized in OASIS Energy Interoperation. (PAP09: Standard DR and DER Signals - http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/PAP09DRDER). OpenADR 2.0 profile is a profile (subset) of the Energy Interoperation standard.
18	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 service-oriented architecture (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 eXtensible Markup Language (XML) schema defined data.	Widely supported open standard, with compliance testing program.
19	Open Geospatial Consortium Geography Markup Language (GML) http://www.opengeospat	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 International Organization for Standardization (ISO) 19118 for the transport and storage of geographic information modeled according to the conceptual modeling framework

Working Draft

	ial.org/standards/gml		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).
20	Smart Energy Profile 2.0 http://www.zigbee.org/Standards/ZigBeeSmartEnergy/Overview.aspx CSWGG Report on Draft Technical Requirements Document 0.7 http://collaborate.nist.gov/twiki-sggrid/pub/SmartGrid/CSCTGStandards/CSWG_Standards_SEP_2.0_Tech_Requirements_TRD_Review_v10.pdf	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. PAP 18 focuses on developing specific requirements to allow the coexistence of SEP 1.x and 2.0 and to support the migration of 1.x implementations to 2.0. The PAP has produced a white paper summarizing the key issues with migration and making specific recommendations and a requirements document to be submitted to the ZigBee Alliance for consideration in developing the technology-specific recommendations, solutions, and any required changes to the SEP 2.0 specifications themselves. PAP18:SEP 1.x to SEP 2 Transition and Coexistence - http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/PAP18SEP1To2TransitionAndCoexistence).
Requirements and Guidelines			
21	OpenHAN http://osgug.ucaiug.org/sgsystems/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,	A specification developed by a users group, Utility Communications Architecture International Users Group (UCAIug), that contains a “checklist” of requirements that enables utilities to compare the many available

Working Draft

		and control.	HANs.
22	AEIC Guidelines http://www.aeic.org/meter_service/AEICSmartGridStandardv2-11-19-10.pdf CSWG Report http://collaborate.nist.gov/twiki-sggrid/pub/SmartGrid/CSCTGStandards/CSWG_Standards_PAP_5_AEIC_Metering_Guidelines_111210.pdf	A guideline comprising 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.
23	SAE J1772: SAE Electric Vehicle and Plug in Hybrid Electric Vehicle Conductive Charge Coupler SAE J1772: SAE Electric Vehicle and Plug in Hybrid Electric Vehicle Conductive Charge Coupler	A recommended practice covering the general physical, electrical, functional, and performance requirements to facilitate conductive charging of Electric Vehicle(EV)/Plug-in Hybrid Electric Vehicle (PHEV) vehicles in North America.	This recommended practice responds to a need for a coupling device identified very early on in the EV industry and meets new interoperability and communications requirements. After review by PAP11 (PAP11: Common Object Models for Electric Transportation - http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/PAP11PEV), CSWG, and SGAC, it has been recommended by the SGIPGB and approved by the SGIP Plenary for

Working Draft

	CoS Web page: http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/SGIPCosSIFSAEJ1772		inclusion in the SGIP Catalog of Standards.
24	SAE J2836/1: Use Cases for Communication Between Plug-in Vehicles and the Utility Grid http://standards.sae.org/j2836/1_201004 CoS Web page: http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/SGIPCosSIFSAEJ28361	This document establishes use cases for communication between plug-in electric vehicles and the electric power grid, for energy transfer and other applications.	This document responds to a need by system designers for documentation of use cases as inputs to creation of end-to-end system solutions between EVs and utilities. After review by PAP11 (PAP11: Common Object Models for Electric Transportation - http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/PAP11PEV), CSWG and SGAC, it has been recommended to and approved by the SGIPGB for inclusion in the SGIP Catalog of Standards.
25	SGTCC Interoperability Process Reference Manual (IPRM) http://collaborate.nist.gov/twiki-sggrid/pub/SmartGrid/SGTCCIPRM/SGTCC_IPRM_Version_1.0_Upd	The Interoperability Process Reference Manual (IPRM) developed by SGIP's Smart Grid Testing and Certification Committee (SGTCC) outlines the conformance, interoperability, and cybersecurity testing and	A guide developed and maintained by the SGIP's SGTCC. The IPRM has been designed to capture testing and certification processes and best practices needed to verify product interoperability amongst two or more products using the same standards-based communications technology. These processes and best practices are intended for use by an Interoperability

Working Draft

	ated.pdf	certification requirements for SGIP-recommended Smart Grid standards.	Testing and Certification Authority (ITCA) in the design and management of a testing and certification program.
26			

Cybersecurity			
27	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%20Profile%20-%20v1_0.pdf	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.
28	Department of Homeland Security (DHS), National Cyber Security Division. 2009, September.	The catalog presents a compilation of practices that various industry bodies have recommended to increase the security of control systems from	This is a source document for the NIST Interagency Report NISTIR 7628, *Guidelines for Smart Grid Cyber Security* (http://csrc.nist.gov/publications/nistir/ir7628/introduction-to-nistir-7628.pdf

Working Draft

	Catalog of Control Systems Security: Recommendations for Standards Developers. http://www.us-cert.gov/control_systems/pdf/FINAL-Catalog_of_Recommendations_Rev4_101309.pdf	both physical and cyber attacks.	http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol1.pdf http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol2.pdf http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol3.pdf).
29	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 cybersecurity 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 NIST Interagency Report NISTIR 7628, *Guidelines for Smart Grid Cyber Security* (http://csrc.nist.gov/publications/nistir/ir7628/introduction-to-nistir-7628.pdf http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol1.pdf http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol2.pdf http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol3.pdf).
30	IEC 62351 Parts 1-8 http://webstore.iec.ch/webstore/webstore.nsf/artnum/037996!opendocument CSWG Report http://collaborate.nist.g	This family of standards defines information security for power system control operations.	Open standard, developed and maintained by an SDO. Defines security requirements for power system management and information exchange, including communications network and system security issues, Transmission Control Protocol (TCP)/IP and Manufacturing Messaging Specification (MMS) profiles, and security for Inter-Control Center Protocol (ICCP) and substation automation and protection. It is for use

Working Draft

	ov/twiki-sggrid/pub/SmartGrid/CSCTGStandards/StandardsReviewPhase-1Report.pdf Narrative http://collaborate.nist.gov/twiki-sggrid/pub/SmartGrid/NISTStandardsSummaries/IEC_62351_Narrative_10-6-2010.doc		in conjunction with related IEC standards, but has not been widely adopted yet.
31	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.
32	NERC Critical Infrastructure Protection (CIP) 002-009 http://www.nerc.com/p	These standards cover organizational, processes, physical, and cybersecurity standards for the bulk power system.	Mandatory standards for the bulk electric system. Currently being revised by the North American Electric Reliability Corporation (NERC).

Working Draft

	age.php?cid=2|20		
33	NIST Special Publication (SP) 800-53 http://csrc.nist.gov/publications/nistpubs/800-53A/SP800-53A-final-sz.pdf, NIST SP 800-82	These standards cover cybersecurity standards and guidelines for federal information systems, including those for the bulk power system.	Open standards developed by NIST. SP800-53 defines security measures required for all U.S. government computers. SP800-8 defines security specifically for industrial control systems, including the power grid.
34	IEC 61851 http://webstore.iec.ch/webstore/webstore.nsf/Artnum_PK/27424	Applies to equipment for charging electric road vehicles at standard alternating current (ac) supply voltages (as per IEC 60038) up to 690 V and at direct current (dc) voltages up to 1 000 V, and for providing electrical power for any additional services on the vehicle if required when connected to the supply network.	
35	NISTIR 7628 Introduction to NISTIR 7628 Guidelines for Smart Grid Cyber Security http://csrc.nist.gov/publications/nistir/ir7628/introduction-to-nistir-7628.pdf	A guideline that is the following: • An overview of the cybersecurity strategy used by the CSWG to develop the high-level cybersecurity Smart Grid requirements; • A tool for organizations that are researching, designing, developing, implementing, and integrating Smart Grid technologies—established and	A guideline published by NIST in 2010. It was developed through a participatory public process that, starting in March 2009, included several workshops as well as weekly teleconferences, all of which were open to all interested parties. There were two public reviews of drafts of the report, both announced through notices in the *Federal Register*. The guidelines are not prescriptive, nor mandatory. Rather they are advisory, intended to facilitate each organization’s efforts to develop a cybersecurity strategy effectively focused on prevention, detection, response, and recovery.

Working Draft

	Vol 1 http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol1.pdf Vol 2 http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol2.pdf Vol 3 http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol3.pdf This is the reference document for the CSWG reviews	emerging; • An evaluative framework for assessing risks to Smart Grid components and systems during design, implementation, operation, and maintenance; and • A guide to assist organizations as they craft a Smart Grid cybersecurity strategy that includes requirements to mitigate risks and privacy issues pertaining to Smart Grid customers and uses of their data.	

Working Draft

Many of the necessary modifications to these standards and related specifications will be driven by the SGIP's PAPs. In addition, the CSWG and the SGAC, whose ongoing efforts are described in more detail in Chapters 6 and 3, respectively, are also addressing some of these needed modifications. As discussed further in Chapter 7, feedback from interoperability testing and certification activities managed by Interoperability Testing and Certification Authorities (ITCAs) will also influence the changes in these standards.

4.4. Current List of Additional Standards Subject to Further Review

The description of the process to establish the list of additional Smart Grid standards identified for further review, contained in Table 4-2, is described in the previous Release 1.0 of this document.[93] These additional candidate standards were not included with those in Table 4-1 because they were under development, or did not meet the guiding principles outlined in Section 4.1. Several standards that are now being developed or revised—by SSOs with PAP coordination—have been added to this table.

Standards identified by SGIP working groups after the publication of Release 1.0 have also been added to Table 4-2 of the current release. (As described above, standards included in Table 4-2 in Release 1.0 of this document that have been recommended by the SGIPGB and approved by the SGIP Plenary for inclusion in SGIP CoS, have been moved from Table 4-2 in Release 1.0 to Table 4-1 in Release 2.0.)

The treatment of wireless technology standards in these tables deserves special clarification. Most wireless technology standards listed in Table 4-2 (rows 11-15) of Release 1.0 were not developed specifically for Smart Grid communications. Therefore, issues related to their applicability to Smart Grid have been assigned to the Priority Action Plan on Wireless Communications (PAP02). This group has undertaken the task of compiling Smart Grid application communication requirements, developing a catalog for wireless communication technologies and their characterizations, and developing methods and tools for evaluating wireless communications. In February 2011, PAP02 published "Guidelines for Assessing Wireless Standards for Smart Grid Applications, Version 1.0."[94] A preliminary review of Smart Grid application communication requirements that are currently available reveals that several wireless standards may be used by many communication applications across different Smart Grid domains. However, additional work in PAP02 is needed to more accurately characterize the performance of these wireless technologies, to assess how well they support the Smart Grid applications communication requirements, and to identify issues and gaps if applicable. Therefore, these wireless technology standards listed in Table 4-1 in Release 1.0 also appear in that table in Release 2.0.

Working Draft

[93] http://www.nist.gov/public_affairs/releases/upload/smartgrid_interoperability_final.pdf, p. 61.

[94] Guidelines for Assessing Wireless Standards for Smart Grid Applications. See: http://collaborate.nist.gov/twiki-sggrid/pub/SmartGrid/PAP02Objective3/NIST_PAP2_Guidelines_for_Assessing_Wireless_Standards_for_Smart_Grid_Applications_1.0.pdf.

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 ANSI C12.23 ANSI C12.24	End Device Tables communications over any network. Compliance Testing for Standard Protocols (C12.18, C12.19, C12.21 and C12.22). A catalog of calculation algorithms for VAR/VA that is in draft form. It may ultimately become a report instead of a standard.	Open, mostly mature standards developed and maintained by an SDO. 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 #23 in this list). This further review may require a PAP to be established by the SGIP. Draft standard for compliance testing of ANSI C12

Working Draft

			communication standards. 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	IEC 61400-25	Communication and control of wind power plants.	An open standard developed and maintained by an SDO. This set of standards is being considered for addition to the

Working Draft

			“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.
5	ITU Recommendation G.9960/G.9661 (G.hn) http://www.itu.int/ITU-T/aap/AAPRecDetails.aspx?AAPSeqNo=1853	In-home broadband home networking over power lines, phone lines, and coaxial cables. G.9660 covers system architecture and PHY, G.9661 covers MAC.	An open standard developed and maintained by an SDO. The harmonization and coexistence of this standard with other PLCs is being addressed by PAP15 for PLC. Harmonization of coexistence between IEEE and ITU-T completed successfully. Now the ISP-based broadband PLC coexistence mechanism has been ratified by ITU-T as Recommendation G.9972 and by IEEE in the 1901 standard. PAP15 recommends that ITU-T G.9960/G.9961 compliant devices must implement and activate (always on) ITU-T G.9972. (PAP15: Harmonize Power Line Carrier Standards for Appliance Communications in the Home - http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/PAP15

Working Draft

			PLCForLowBitRates).
6	IEEE P1901 http://standards.ieee.org/findstds/standard/1901-2010 .html	Broadband communications over power lines, medium access control (MAC) and physical layer (PHY) protocols.	An open standard developed and maintained by an SDO. The harmonization and coexistence of this standard with other PLCs is being addressed by PAP15 for PLC. Harmonization of coexistence between IEEE and ITU-T completed successfully. Now the ISP-based broadband PLC coexistence mechanism has been ratified by ITU-T as Recommendation G.9972 and by IEEE in the 1901 standard. PAP15 recommends that IEEE 1901 compliant devices must implement and activate (always on) ISP as specified in IEEE 1901. (PAP15: Harmonize Power Line Carrier Standards for Appliance Communications in the Home - http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/PAP15PLCForLowBitRates).
7	IEEE P1901.2 and ITU-T G.9955/G.9956 (G.hnem)	Low frequency narrowband communications over power lines.	PAP15 provides requirements for narrowband power line communications standards under development.

Working Draft

			Note: These standards will be removed from this list and from further consideration unless they include specification enabling coexistence of narrowband power line carrier (PLC) standards.
8	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.
9	ISO/IEC 12139-1	High-speed power line communications medium access control physical layer (PHY) protocols.	The harmonization and coexistence of this standard with other PLC standards is being addressed by PAP15 for PLC. (PAP15: Harmonize Power Line Carrier Standards for Appliance Communications in the Home - http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/PAP15PLCForLowBitRates).
10	IEEE 802 Family	This includes standards developed by the IEEE 802 Local Area and Metropolitan Area Network Standards Committee.	A set of open, mature standards for wired and wireless LLC/MAC/PHY protocols, developed and maintained by an SDO. Other related specifications include those developed by Industry fora such as WiFi Alliance, WiMAX Forum, and Zigbee Alliance to promote the use of these standards

Working Draft

			and to provide implementation testing and certification. Version 1.0 of the Guidelines for Assessing Wireless Standards for Smart Grid Applications has been recommended by the SGIPGB and approved by the SGIP Plenary for the CoS. (PAP02: Wireless Communications for the Smart Grid - http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/PAP02Wireless). The guideline is a draft of key tools and methods to assist Smart Grid system designers in making informed decisions about existing and emerging wireless technologies. An initial set of quantified requirements has been brought together for advanced metering infrastructure (AMI) and initial Distribution Automation (DA) communications.
11	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. Version 1.0 of the Guidelines for Assessing Wireless Standards for Smart Grid Applications is now under consideration for approval by PAP02 (PAP02: Wireless Communications for the Smart Grid - http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/PAP02Wireless). The guideline provides

Working Draft

			key tools and methods to assist Smart Grid system designers in making informed decisions about existing and emerging wireless technologies. An initial set of quantified requirements has been brought together for advanced metering infrastructure (AMI) and initial Distribution Automation (DA) communications.
12	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. Version 1.0 of the Guidelines for Assessing Wireless Standards for Smart Grid Applications has been approved by the SGIP Governing Board and SGIP Plenary for inclusion in the Catalog of Standards. (PAP02: Wireless Communications for the Smart Grid - http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/PAP02Wireless). The guideline provides of key tools and methods to assist Smart Grid system designers in making informed decisions about existing and emerging wireless technologies. An initial set of quantified requirements has been brought together for advanced metering infrastructure (AMI) and initial Distribution Automation

Working Draft

			(DA) communications.
13	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.
14	ISA SP100	Wireless communication standards intended to provide reliable and secure operation for non-critical monitoring, alerting, and control applications specifically focused to meet the needs of industrial users.	Standards developed by ISA-SP100 Standards Committee, Wireless Systems for Automation.
15	Network Management Standards - including Interne-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.
16	ASHRAE 201P Facility Smart Grid Information Model	An information model standard designed to enable appliances and control systems in homes, buildings, and industrial facilities to manage electrical loads and generation sources in response to communication with a smart electrical grid and to communicate information about those electrical loads to utility and other electrical service	The standard is currently under development and is linked to PAP17. The standard is communication protocol independent. It is anticipated that it will be used by several SDOs and other organizations to make protocol specific implementations.

Working Draft

		providers.	
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 2030 Standards: IEEE P2030 IEEE P2030.1 IEEE P2030.2	IEEE Smart Grid series of standards: (1) 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;" (2) IEEE P2030.1 "Draft Guide for Electric-Sourced Transportation Infrastructure;" and (3) IEEE P2030.2 "Draft Guide for the Interoperability of Energy Storage Systems Integrated with the Electric Power Infrastructure."	The IEEE 2030 Smart Grid series standards are developed to provide guidelines for smart grid interoperability. IEEE P2030 provides a knowledge base addressing terminology; characteristics; functional performance and evaluation criteria; and the application of engineering principles for Smart Grid systems with end-use applications and loads. The guide discusses alternate approaches to good practices for the Smart Grid. (http://grouper.ieee.org/groups/scc21/2030/2030_index.html). IEEE P2030.1 provides guidelines that can be used by utilities, manufacturers, transportation providers, infrastructure developers, and end users of electric-sourced vehicles and related support infrastructure in

Working Draft

Working Draft

			addressing applications for road-based personal and mass transportation. (http://grouper.ieee.org/groups/scc21/2030.1/2030.1_index.html); IEEE P2030.2 provides guidelines for discrete and hybrid energy storage systems that are integrated with the electric power infrastructure, including end-use applications and loads. (http://grouper.ieee.org/groups/scc21/2030.2/2030.2_index.html).
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.	An open standard, developed and maintained by an SDO. 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/TR 61000-1-2 (2002-06) Ed. 1.0	The effects of high-altitude EMP (HEMP) on civil equipment and systems.	A family of open standards developed and maintained by an SDO, The IEC 61000 series of standards

	IEC/TR 61000-1-5 (2004-11) Ed. 1.0 IEC 61000-2-9 (1996-02) Ed. 1.0 IEC 61000-2-10 (1998-11) Ed. 1.0 IEC 61000-2-11 (1999-02) Ed. 1.0 IEC 61000-2-13 (2005-03) Ed. 1.0 IEC 61000-4-23 (2000-10) Ed. 1.0 IEC 61000-4-24 (1997-02) Ed. 1.0 IEC/TR 61000-4-32 (2002-10) Ed. 1.0	High-power electromagnetic (HPEM) effects on civil systems. Description of HEMP environment - Radiated disturbance. Basic EMC publication. Description of HEMP environment - Conducted disturbance. Classification of HEMP environments. High-power electromagnetic (HPEM) environments - Radiated and conducted. Test methods for protective devices for HEMP and other radiated disturbances. HEMP immunity test methods for equipment and systems. High-altitude electromagnetic	are Basic EMC publications. They include terminology, descriptions of electromagnetic phenomena and the EM environment, measurement and testing techniques, and guidelines on installation and mitigation. The specific standards listed here and others in the series may have application to Smart Grid equipment. http://www.iec.ch/emc/basic_emc/basic_61000.htm

Working Draft

		pulse (HEMP) simulator compendium.	
	IEC 61000-4-33 (2005-09) Ed. 1.0	Measurement methods for high-power transient parameters.	
	IEC/TR 61000-4-35 (2009-07) Ed. 1.0	HPEM simulator compendium.	
	IEC/TR 61000-5-3 (1999-07) Ed. 1.0	HEMP protection concepts.	
	IEC/TS 61000-5-4 (1996-08) Ed. 1.0	Specifications for protective devices against HEMP-radiated disturbance. Basic EMC Publication.	
	IEC 61000-5-5 (1996-02) Ed. 1.0	Specifications of protective devices for HEMP-conducted disturbance. Basic EMC Publication.	
	IEC 61000-5-6 (2002-06) Ed. 1.0	Mitigation of external EM influences.	
	IEC 61000-5-7 (2001-01) Ed. 1.0	Degrees of protection provided by enclosures against electromagnetic disturbances (EM code).	

Working Draft

	IEC/TS 61000-5-8 (2009-08) Ed. 1.0	HEMP protection methods for the distributed infrastructure.	
	IEC/TS 61000-5-9 (2009-07) Ed. 1.0	System-level susceptibility assessments for HEMP and HPEM.	
	IEC 61000-6-6 (2003-04) Ed. 1.0	HEMP immunity for indoor equipment.	
	IEC 61000-6-5	Electromagnetic compatibility (EMC) - Part 6-5: Generic standards - Immunity for power station and substation environments.	
	IEC 61000-2-5	Electromagnetic compatibility (EMC) - Part 2: Environment - Section 5: Classification of electromagnetic environments. Basic EMC publication.	
	IEC 61000-4-2	Electromagnetic compatibility (EMC)- Part 4-2: Testing and measurement techniques - Electrostatic	

Working Draft

		discharge immunity test.	
	IEC 61000-4-3	Electromagnetic compatibility (EMC) - Part 4-3 : Testing and measurement techniques - Radiated, radio-frequency, electromagnetic field immunity test.	
	IEC 61000-4-4	Electromagnetic compatibility (EMC) - Part 4-4: Testing and measurement techniques - Electrical fast transient/burst immunity test.	
	IEC 61000-4-5	Electromagnetic compatibility (EMC) - Part 4-5: Testing and measurement techniques - Surge immunity test.	
	IEC 61000-4-6	Electromagnetic compatibility (EMC) - Part 4-6: Testing and measurement techniques - Immunity to conducted disturbances, induced by radio-frequency fields.	
		Electromagnetic	

Working Draft

	IEC 61000-4-8 IEC 61000-4-11 IEC 61000-4-18	compatibility (EMC) - Part 4-8: Testing and measurement techniques - Power frequency magnetic field immunity test. Electromagnetic compatibility (EMC) - Part 4-11: Testing and measurement techniques - Voltage dips, short interruptions, and voltage variations immunity tests. Electromagnetic compatibility (EMC) - Part 4-18: Testing and measurement techniques - Damped oscillatory wave immunity test.	
22	IEC 62056 Device Language Message Specification (DLMS)/Companion Specification for Energy Metering (COSEM) Electricity metering - Data exchange for meter reading, tariff and load control	Energy metering communications.	An open standard, developed and maintained by an SDO. 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 User Association.

Working Draft

23	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 at the NIST May 2009 workshop and is used in several PAP tasks.
24	IEC 60870-2-1	Telecontrol equipment and systems - Part 2: Operating conditions - Section 1: Power supply and electromagnetic compatibility.	This is an open standard developed and maintained by an SDO. This section of IEC 60870 applies to telecontrol equipment and systems for monitoring and control of geographically widespread processes. This is a product standard for telecontrol equipment with specific references to EMC test levels and methods in the 61000 series of basic EMC standards. This standard is considered in the context of protecting Smart Grid equipment from electromagnetic interference.
25	IEC 60255- 22-x -1 : Relay immunity	Measuring relays and protection equipment - Part 22-2: Electrical disturbance tests.	This is an open standard developed and maintained by an SDO. Series of standards related to relays and protection equipment

Working Draft

	-2: ESD -3: RF immunity -4: EFT -5: Surge -6: Conducted Immunity		immunity to various electrical and electromagnetic disturbances. This standard is considered in the context of protecting Smart Grid equipment from electromagnetic interference.
26	IEC CISPR 22 and IEEE C63.022 - 1996	Information technology equipment - Radio disturbance characteristics - Limits and methods of measurement.	This is an open standard developed and maintained by an SDO. CISPR 22:2008 applies to information technology equipment (ITE). Procedures are given for the measurement of the levels of spurious signals generated by the ITE and limits are specified for the frequency range 9 kHz to 400 GHz for both class A and class B equipment. IEEE C63.022 is CISPR 22 republished an American National Standard. This standard is considered in the context of protecting Smart Grid equipment from electromagnetic interference.
27	IEC CISPR 24	Information technology equipment - Immunity characteristics - Limits and methods of measurement.	This is an open standard developed and maintained by an SDO. CISPR 24:2010 applies to

Working Draft

			information technology equipment (ITE) as defined in CISPR 22. The object of this publication is to establish requirements that will provide an adequate level of intrinsic immunity so that the equipment will operate as intended in its environment. The publication defines the immunity test requirements for equipment within its scope in relation to continuous and transient conducted and radiated disturbances, including electrostatic discharges (ESD). This standard is considered in the context of protecting Smart Grid equipment from electromagnetic interference.
28	IEC 61326x series	Electrical equipment for measurement, control, and laboratory use - EMC requirements.	This is an open standard developed and maintained by an SDO. The IEC 61326 suite specifies requirements for immunity and emissions regarding electromagnetic compatibility (EMC) for electrical equipment, operating from a supply or battery of less than 1 000 V a.c. or 1 500 V d.c. or from the circuit being measured, intended for professional, industrial-process, industrial-manufacturing and

Working Draft

			educational use, including equipment and computing devices. This standard is considered in the context of protecting Smart Grid equipment from electromagnetic interference.
29	IEEE 1560	Standard for Methods of Measurement of Radio-Frequency Power Line Interference Filter in the Range of 100 Hz to 10 GHz.	This is an open standard developed and maintained by an SDO. Uniform methods of measurements of radio-frequency power-line interference filter attenuation performance in the range of 100 Hz to 10 GHz are set forth. This standard is specifically for a particular product used to mitigate interference conducted on the power lines. This standard is considered in the context of protecting Smart Grid equipment from electromagnetic interference.
30	IEEE 1613	1613-2003 - IEEE Standard Environmental and Testing Requirements for Communications Networking Devices in Electric Power Substations	This is an open standard developed and maintained by an SDO. IEEE 1613 is the IEEE standard for the environmental and testing requirements for communications networking devices in electric power substations. This standard is under revision with the scope

Working Draft

			expanded from substations to all electric power facilities except office locations. It defines the EM immunity requirements for communications devices in the utility locations. This standard is considered in the context of protecting Smart Grid equipment from electromagnetic interference.
31	IEEE P1642	Recommended Practice for Protecting Public Accessible Computer Systems from Intentional EMI.	This is an open recommended practice guide developed and maintained by an SDO. This recommended practice will establish appropriate EM threat levels, protection methods, monitoring techniques, and test techniques for different classes of computer equipment. This standard is considered in the context of protecting Smart Grid equipment from intentional electromagnetic interference.
32	IEEE 473	IEEE Recommended Practice for an EM Site Survey. (10kHz-10GHz).	This is an open recommended practice guide developed and maintained by an SDO. An important step in developing EMC requirements for Smart Grid equipment is knowledge of the EM

Working Draft

			environment that the device will experience. This recommended practice may be useful as guidance on performing these surveys.
33	IEEE P1775/1.9.7, March 2009	1775-2010 - IEEE Standard for Power Line Communication Equipment--Electromagnetic Compatibility (EMC) Requirements--Testing and Measurement Methods.	This is an open standard developed and maintained by an SDO. Electromagnetic compatibility (EMC) criteria and consensus test and measurements procedures for broadband over power line (BPL) communication equipment and installations are presented. Existing national and international standards for BPL equipment and installations are referenced. This standard does not include the specific emission limits, which are subject to national regulations. This standard is considered in the context of protecting Smart Grid equipment from electromagnetic interference.
34	IEEE C63.16-1993	C63.16-1993 - American National Standard Guide for Electrostatic Discharge Test Methodologies and Criteria for Electronic Equipment.	This is an open standard developed and maintained by an SDO and harmonized with international ESD standards. Based upon ESD events on electronic equipment in actual-use environments, a process to

Working Draft

			establish ESD test criteria is provided. Test procedures for highly repeatable ESD immunity evaluation of tabletop and floor-standing equipment are described. This standard is considered in the context of protecting Smart Grid equipment from electromagnetic interference.
35	IEEE C37.90-2005 C37.90.1-2002 (electrical transient immunity) C37.90.2-2004 (radiated EM immunity) C37.90.3-2001 (electrostatic discharge immunity)	C37.90-2005 - IEEE Standard for Relays and Relay Systems Associated with Electric Power Apparatus.	This is an open standard developed and maintained by an SDO. This standard suite defines the EMC requirements, service conditions, electrical ratings, thermal ratings, and testing requirements for relays and relay systems used to protect and control power apparatus. This standard establishes a common reproducible basis for designing and evaluating relays and relay systems. This standard is considered in the context of protecting Smart Grid equipment from electromagnetic interference.
36	IEEE C37.2-2008 IEEE Standard Electric Power System Device Function Numbers	Protective circuit device modeling numbering scheme for various switchgear.	An open standard, developed and maintained by an SDO. The latest revision contains cross-references between C37.2 numbers and IEC 61850-7-4 logical nodes.

Working Draft

37	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.	An open standard, developed and maintained by an SDO. It facilitates the exchange of captured power system transient data using standardized format.
38	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.
39	IEEE 1159.3 Recommended Practice for the Transfer of Power Quality Data	Applications using power quality data.	An open standard, developed and maintained by an SDO. It is a recommended practice for a file format suitable for exchanging power quality-related measurement and simulation data in a vendor-independent manner.
40	IEEE 1379-2000	Substation Automation - Intelligent Electronic Devices (IEDs) and remote terminal units (RTUs) in electric utility substations.	An open standard, developed and maintained by an SDO. Recommends the use of DNP3 or IEC 60870-5 for substation IED communications.

Working Draft

41	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.	An open standard, developed and maintained by an SDO. This should be considered as standards for residential networks are established under present and future PAPs.
42	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.	An open standard, developed and maintained by an SDO.
43	ISO/IEC 18012, "Guidelines for Product Interoperability." http://www.iso.org/iso/catalogue_detail.htm?csnumber=46317	Specifies requirements for product interoperability in the home and building automation systems.	An open standard, developed and maintained by an SDO.
44	North American Energy Standards Board (NAESB) Open Access Same-Time Information Systems (referred to as "OASIS" by utilities and FERC, not to be confused with the SDO Organization for the Advancement of Structured Information Standard)	Utility business practices for transmission service.	All utilities subject to FERC jurisdiction must use the NAESB OASIS standard, which specifies the methods and information that must be exchanged between market participants and market operators for transactions in the wholesale electric power industry.
45	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 (PAP09:

Working Draft

			Standard DR and DER Signals - http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/PAP09DRDER).
46	Organization for the Advancement of Structured Information Standard (OASIS) EMIX (Energy Market Information eXchange)	EMIX provides an information model to enable the exchange of energy price, characteristics, time, and related information for wholesale energy markets, including market makers, market participants, quote streams, premises automation, and devices.	EMIX has been developed as part of PAP03. (PAP03: Develop Common Specification for Price and Product Definition - http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/PAP03PriceProduct).
47	OASIS Energy Interoperation (EI)	Energy interoperation describes an information model and a communication model to enable demand response and energy transactions. XML vocabularies provide for the interoperable and standard exchange of: DR and price signals, bids, transactions and options, and customer feedback on load predictability and generation information.	This standard uses the EMIX information model for price and product as payload information. The DR specification is built on a unified model of retail (OpenADR) and wholesale (input from the ISO/RTO Council) DR. OpenADR 2.0 is a profile on EI. Energy Interop was developed as part of PAP09 (PAP09: Standard DR and DER Signals - http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/PAP09DRDER).
48	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	This standard serves as a reference point for OASIS EMIX (see above) in the PAP03 effort (PAP03: Develop Common Specification

Working Draft

		widely used protocol for financial trading today.	for Price and Product Definition - http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/PAP03PriceProduct).
49	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.
50	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.	WS-Calendar describes a limited set of message components and interactions providing a common basis for specifying schedules and intervals to coordinate activities between services. The specification includes service definitions consistent with the OASIS SOA Reference Model and XML vocabularies for the interoperable and standard exchange of: • Schedules, including sequences of schedules • Intervals, including sequences of intervals This standard is the primary deliverable of the common schedules PAP04. (see PAP04: Develop Common Schedule Communication Mechanism for Energy Transactions -

Working Draft

			http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/PAP04Schedules) This specification is used by EMIX (see PAP03: Develop Common Specification for Price and Product Definition - http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/PAP03PriceProduct) and Energy Interoperation (see PAP09: Standard DR and DER Signals - http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/PAP09DRDER)
51	SAE J2847/1-3 Communications for PEV Interactions http://standards.sae.org/j2847/1_201006	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 series of standards will be considered when they are finalized. Only J2847/1 is published. J2847/2 and J2847/3 have not been published yet.
52	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

Working Draft

			be considered for use in the Smart Grid domain when such functionality is required.
53	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.
54	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.
55	W3C XSD (XML Definition)	Description of XML artifacts, which are 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.
56	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.
57	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	Development began 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

Working Draft

		communicating ground fault and arc fault interrupters.	formed the ELMS Working Group to further develop the control objects based on NTCIP.
58	OpenADE Energy Service Provider Interface	Open Automatic Data Exchange (OpenADE) provides business requirements, use cases, and system requirements specifications that allow a consumer to grant a third party access to their electric data, and, in accordance with that authorization, the utility delivers the consumer data to the third party using a standard interoperable machine-to-machine (M2M) interface. These recommendations will be developed according to guidelines provided by SDOs such as IEC, referenced in OpenADE documents, with the goal of gaining consensus and adoption as international standards.	The OpenADE is developed by a group of Smart Energy management vendors, utilities, and consumer interests as a task force under OpenSG User Group. The task force is developing recommendations toward building interoperable data exchanges that will allow customer authorization and sharing of utility consumption information with third-party service providers. The “OpenADE 1.0 Business and User Requirements” and “OpenADE 1.0 System Requirements” have been developed and approved by OpenSG.
59	UL-1741 The Standard for Static Inverters and Charge Controllers For use in Photovoltaic Power Systems	The standard specifies requirements for Inverters, Converters, Controllers, and Interconnection System Equipment for Use with	

Working Draft

		Distributed Energy Resources.	
Cyber-security			
60	ISA SP99 http://www.isa.org/MSTemplate.cfm?MicrositeID=988&CommitteeID=6821	Cybersecurity 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 cybersecurity management system. Smart Grid contains many control systems that require cybersecurity management.	This has been used in the development of the NIST Interagency Report NISTIR 7628, *Smart Grid Cyber Security Strategy:* (http://csrc.nist.gov/publications/nistir/ir7628/introduction-to-nistir-7628.pdf http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol1.pdf http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol2.pdf http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol3.pdf).
61	ISO27000 http://www.27000.org/	The ISO 27000 series of standards has been specifically reserved by ISO for information security matters.	This has been used in the development of the NIST Interagency Report NISTIR 7628, *Smart Grid Cyber Security Strategy;* (http://csrc.nist.gov/publications/ni

Working Draft

			stir/ir7628/introduction-to-nistir-7628.pdf http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol1.pdf http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol2.pdf http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol3.pdf).
62	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.
63	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.

Working Draft

4.5. Process of 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. Useful, widely accepted criteria and guidelines will aid identification and selection of standards. Clearly, any set of guidelines and processes for evaluating candidate standards will have to evolve as the Smart Grid is developed, new needs and priorities are identified, and new technologies emerge.

The future NIST Smart Grid standard identification process will be carried out through work with various SGIP committees, working groups, and PAPs, as well as with Interoperability Testing and Certification Authorities. The SGIP will serve as the forum to further develop and improve the standard identification process for Smart Grid standards. From its inception, the SGIP has incorporated the cybersecurity and architectural reviews into the standard-assessment and PAP-activity-assessment processes. Moving forward, standard conformance and interoperability testing results will also provide feedback to the standard identification process.

With the publication of NISTIR 7628, *Guidelines for Smart Grid Cyber Security*, all existing and new standards identified as supporting Smart Grid interoperability are required to undergo a thorough cybersecurity review as part of the current and future standard identification process. Results of these reviews are made publicly available on the CSWG Web site — over 20 standards have already been reviewed.[95] Standards organizations and prospective users of the reviewed specifications can identify gaps and other issues with this information.

Existing and new standards are also required to undergo a thorough architecture review. Mapping identified standards and the PAP activities to the conceptual architecture and the GWAC stacks helps to reveal gaps and areas that may need future standards development and/or priority actions. The standards identified in Table 4-1 and those emerging from PAP activities are undergoing architectural reviews conducted by the SGAC. The checklist and review process will continue to evolve. Upon adoption of the interoperability standard testing and certification framework developed by the SGTCC (see Chapter 7), NIST expects that feedback from the standard conformance and interoperability test results will become an important part of the future standard identification process. For example, the deficiencies and gaps of a standard, identified through the interoperability testing and certification process, could determine whether a candidate standard needs further review.

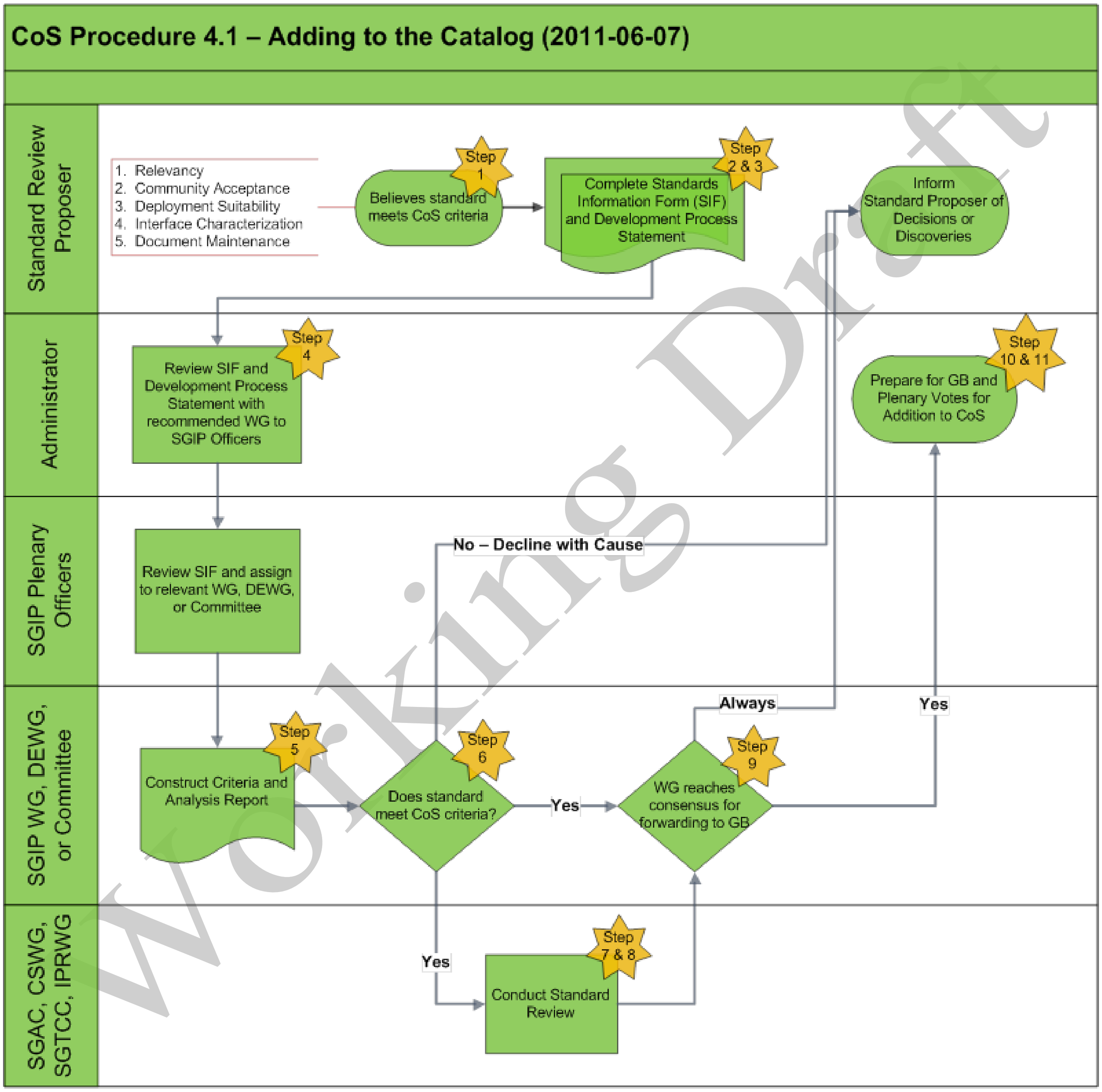
As described in Section 4.2 and Section 5.3, the SGIP has established the process for adopting and adding standards to the SGIP CoS. As standards are reviewed and added to the CoS, NIST will consider adding these standards to Table 4-1. As new candidate standards emerge through the ongoing work of the SGIP and its various working groups, these new standards will be considered for addition to Table 4-2, after NIST has applied an additional analysis based on the guiding principles given in Section 4.1 to the standards present in the SGIP (CoS).

SGIP Catalog of Standards

Working Draft

[95] http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/NISTStandardsSummaries.

As part of its Charter objectives, the SGIP produces and maintains a Catalog of Standards (CoS). This section describes the purpose and scope of the CoS, as well as the process and procedures for the management of the SGIP CoS. Procedures are described for the management of the life cycle of a standard's entry into the CoS, from its proposed inclusion, to its approval for inclusion, its periodic review for relevance, and its possible deprecation and removal from the Catalog.



CoS Procedure 4.1 – Adding to the Catalog (2011-06-07)
Standard Review Proposer
Administrator
SGIP Plenary Officers
SGIP WG, DEWG, or Committee
SGAC, CSWG, SGTCC, IPRWG
1. Relevancy
2. Community Acceptance
3. Deployment Suitability
4. Interface Characterization
5. Document Maintenance
Step 1
Believes standard meets CoS criteria
Step 2 & 3
Complete Standards Information Form (SIF) and Development Process Statement
Inform Standard Proposer of Decisions or Discoveries
Step 4
Review SIF and Development Process Statement with recommended WG to SGIP Officers
Step 10 & 11
Prepare for GB and Plenary Votes for Addition to CoS
Review SIF and assign to relevant WG, DEWG, or Committee
No – Decline with Cause
Always
Yes
Step 5
Construct Criteria and Analysis Report
Step 6
Does standard meet CoS criteria?
Yes
Step 9
WG reaches consensus for forwarding to GB
Yes
Step 7 & 8
Conduct Standard Review

Working Draft

Figure 4-1. CoS Procedure 4.1, Adding to the Catalog

Note that the SGIP CoS is anticipated to provide a key, but not exclusive, source of input to the NIST process for coordinating the development of a framework of protocols and model standards for the Smart Grid under its Energy Independence and Security Act of 2007 (EISA) responsibilities.

The CoS is a compendium of standards and practices considered to be relevant for the development and deployment of a robust and interoperable Smart Grid. The CoS may contain multiple entries that may accomplish the same goals and are functionally equivalent; similarly, a single CoS entry may contain optional elements that need not be included in all implementations. In general, compliance with a standard does not guarantee interoperability due to the reasons given above. Though standards facilitate interoperability, they rarely, if ever, cover all levels of agreement and configuration required in practice. As a part of its work program, the SGIP is defining a testing and certification program that may be applied to the equipment, devices, and systems built to the standards listed in the CoS and that, if applied, will substantiate that implementations designed to the respective standards not only have compliance with the standards, but are also interoperable with one another. The CoS entry will indicate when test profiles have been defined and testing organizations identified for a particular standard; this will be indicated in the Catalog entry.

5. Smart Grid Interoperability Panel (SGIP)

5.1. Overview: Smart Grid Interoperability Panel

Created in November 2009, the Smart Grid Interoperability Panel (SGIP) provides a framework to support stakeholder participation and representation in order to further the development and evolution of Smart Grid interoperability standards. The SGIP, which consists of organizations spread among 22 categories of Smart Grid stakeholders, has three primary functions:

- To oversee activities intended to expedite the development of interoperability and cybersecurity specifications by standards-setting organizations (SSOs);
- To provide technical guidance to facilitate the development of standards for a secure, interoperable Smart Grid; and
- To specify testing and certification requirements necessary to assess the interoperability of Smart Grid-related equipment.

The SGIP, a public-private partnership, is a membership-based organization that serves as a forum to coordinate the development of standards and specifications by many SSOs. The SGIP does not write standards, but rather it provides an open process for stakeholders to interact with the National Institute of Standards and Technology (NIST) in the ongoing coordination, acceleration, and harmonization of new and emerging standards for the Smart Grid. It also reviews use cases, identifies requirements and architectural reference models, coordinates and accelerates Smart Grid testing and certification, and proposes action plans for achieving these objectives. As of July 2011, the SGIP includes over 675 member organizations and over 1,790 member representatives in 22 Smart Grid stakeholder categories; 29 of these member representatives are from Canada and 47 more are from other countries, including China. These

Working Draft

member organizations and member representatives make up the SGIP Plenary, which meets several times each year, in both face-to-face and virtual meetings. Three Plenary Officers (Chair, Vice Chair, and Secretary) are elected by the Plenary. The Plenary Chair is selected by a majority vote of the SGIP Governing Board (SGIPGB). The Plenary Vice Chair is selected by a simple majority vote of the Stakeholders that compose the SGIP. The Plenary Secretary is nominated and elected by majority vote of the SGIP. The first officers elected as Chair, Vice Chair, and Secretary were Steve Widergren, Mark Klerer, and Paul Molitor. Widergren and Klerer continue in 2011 as Chair and Vice Chair. The SGIP Secretary can serve only for one year, and the current SGIP Secretary is David Mollerstuen.

The SGIP is guided by a Governing Board, elected by the Plenary member organizations. The Governing Board approves work programs for the SGIP to efficiently carry out its work, prioritizes objectives, and arranges for the necessary resources. The Governing Board's responsibilities include facilitating a dialogue with SDOs and other Smart Grid-related organizations including utilities, equipment manufacturers, consumers, government agencies, and regulators as well as others, to ensure that the action plans can be implemented. The members comprise representatives from the 22 stakeholder groups and maintain a broad perspective of the NIST Interoperability Framework and support NIST.

As established in the Bylaws, the SGIP has two permanent committees (see Section 5.2.1 below). The SGIP may also form additional permanent working groups (see Section 5.2.2 below) and ad hoc working groups (see Sections 5.3 and 5.4 below). All SGIP outputs are delivered to the public through the NIST Smart Grid Collaboration Site and the Interoperability Knowledge Base (IKB) Web site (see Section 5.5 below). The SGIP, its Governing Board, and its working groups are open organizations dedicated to balancing the needs of a variety of Smart Grid-related organizations. Any organization may become a member of the SGIP. Members are required to declare an affiliation with an identified stakeholder category; 22 stakeholder categories have thus far been identified by NIST and are listed here.[96]

Member organizations may contribute multiple member representatives, but only one Voting Member Representative. Participating members must regularly take part in order to vote on the work products of the SGIP. The SGIP Governing Board includes at least one member from each stakeholder category, the chairs of the two standing committees, several "members at large," and several ex officio members representing other stakeholders (e.g., key government agencies). Terms of SGIP Governing Board members are staggered to ensure regular turnover and continuity.

The SGIP does not intend to duplicate work being done in any other organization, but intends to fill a role that is not sufficiently addressed in other current Smart Grid forums—specifically advancing the goals of NIST in its EISA 2007 mission. As such, the SGIP focuses on two principal areas where value can be added:

[96] NIST Smart Grid Collaboration Site. Categories of SGIP Membership, See: http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/SGIPCategories.

Working Draft

- **Analysis** of cross-functional area applications requiring coordination between one or more technologies beyond the original scope of the technology itself.
- **Coordination** among all groups which must complement each other on the resolution of a gap or overlap in Smart Grid technologies.

The first of these focus areas, analysis, is provided in the SGIP through the working group structure, primarily through the Domain Expert Working Groups (DEWGs). The second of these focus areas, coordination, is provided in the SGIP through the origination and oversight of the Priority Action Plan (PAP) groups.

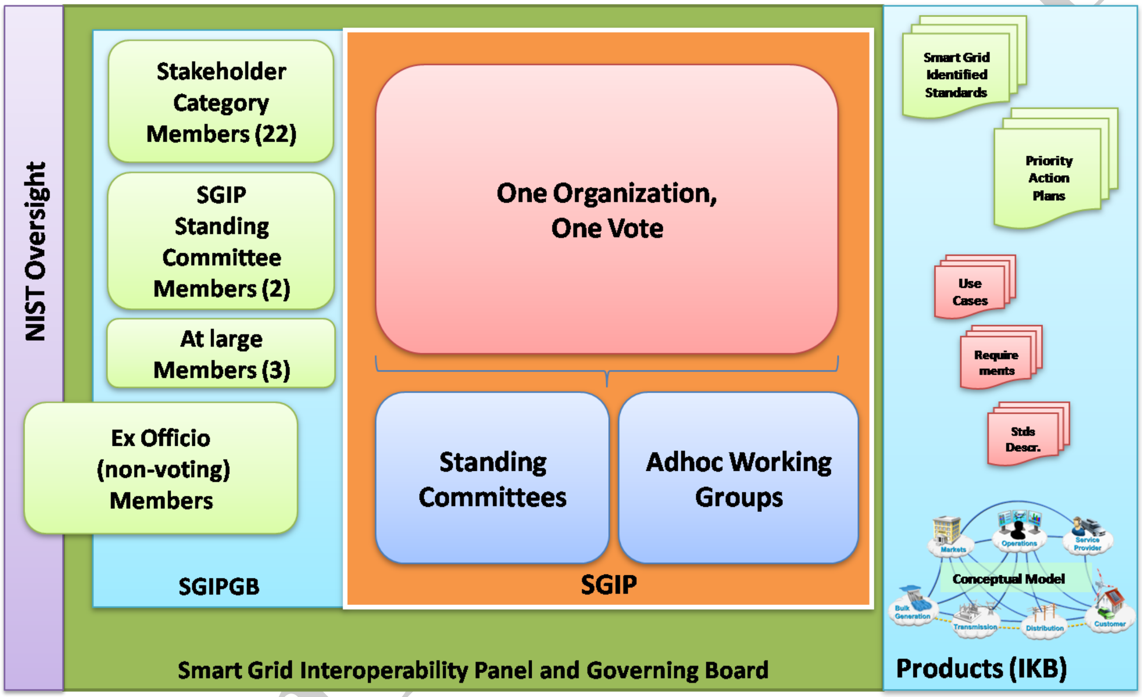


Figure 5-1. SGIP Structure (as of March 2011)

5.2. *SGIP Standing Committees and Permanent Working Groups*

The SGIP has two standing committees: the Smart Grid Architecture Committee (SGAC) and the Smart Grid Testing and Certification Committee (SGTCC). The SGIP also has a Cybersecurity Working Group (CSWG) and a number of ad hoc working groups, known as Domain Expert Working Groups (DEWGs) and Priority Action Plans (PAPs). At the present time, the SGIP has established one permanent working group, the Cybersecurity Working Group (CSWG).[97]

[97] http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/SGIPWorkingGroupsAndCommittees.

Working Draft

Smart Grid Architecture Committee (SGAC) and Smart Grid Testing and Certification Committee (SGTCC)

The SGAC is responsible for creating and refining a conceptual reference model. This effort includes the lists of the standards and profiles necessary to implement the vision of the Smart Grid. The SGTCC creates and maintains the necessary documentation and organizational framework for compliance, interoperability, and cybersecurity testing and certification for Smart Grid standards recommended by SGIP.

- Cybersecurity Working Group (CSWG)

The CSWG has the primary objective to assess standards for applicability and interoperability across the domains of the Smart Grid, rather than develop a single set of cybersecurity requirements that are applicable to all elements of the Smart Grid. These standards will be assessed within an overall risk management framework that focuses on cybersecurity within the Smart Grid. These objectives include:

- Assessing Smart Grid Interoperability Panel (SGIP)-identified standards within an overall risk assessment framework that focuses on cyber security within the Smart Grid;
- Developing a set of recommended security requirements that may be used by strategists, designers, implementers, and operators of the Smart Grid (e.g., utilities, equipment manufacturers, and regulators) as input to their risk assessment process and other tasks in the security life cycle of a Smart Grid information system. These security requirements are intended as a starting point for organizations;
- Identifying Smart Grid-specific problems and issues that currently do not have solutions;
- Creating a logical reference model of the Smart Grid, which will enable further work towards the creation of a logical architecture and a security architecture. This work is being performed in coordination with the SGIP SGAC;
- Identifying inherent privacy risk areas and feasible ways in which those risks may be mitigated while at the same time supporting and maintaining the value and benefits of the Smart Grid; and
- Developing a conformity assessment program for security requirements in coordination with activities of the SGIP SGTCC.

5.3. SGIP Catalog of Standards

The purpose and scope of the SGIP Catalog of Standards (CoS), as well as the process and procedures for its management, are described both in Section 4.5 and on the SGIP CoS Web site.[98] The CoS processes were finalized in May 2011, and the SGIP Project Management Office (PMO) has now assigned the standards from Tables 4-1 and 4-2 that have not been through the CoS process, to the relevant Domain Expert Working Groups (DEWGs) to apply the CoS processes to them. These processes include: 1) coordinating with the Standards Development Organization (SDO) and other groups that maintain the standards to get the Standards

[98] http://collaborate.nist.gov/twiki-sggrid/pub/SmartGrid/SGIPGBDocumentsUnderReview/Standards_Catalog_Process_and_Structure_V0_9_20110401.pdf.

Working Draft

Information Forms completed; 2) coordinating with the SGIP Cybersecurity Working Group (CSWG) and Smart Grid Architecture Committee (SGAC) to get their reviews completed; and 3) completing the Criteria and Analysis form to qualify the standard as meeting the CoS criteria. It is intended that all of the standards in Tables 4-1 and Table 4-2 be reviewed for the CoS.

5.4. Domain Expert Working Groups (DEWGs)

DEWGs provide expertise in specific application areas, as well as a rich understanding of the current and future requirements for Smart Grid applications. Due to their open membership and collaborative process, DEWGs integrate a wide array of stakeholder expertise and interests. Through their understanding of Smart Grid applications, DEWGs expose and model the applications in use cases, cataloged in the Interoperability Knowledge Base (IKB). The applications are analyzed against functional and nonfunctional requirements, and against the potential standards that fulfill them. Through their analysis, DEWGs can allocate functionality to actors, standards, and technologies, and thus support the fulfillment of Smart Grid applications. By this means, the DEWGs can discover the gaps and overlaps of standards for the Smart Grid, as well as identify which technologies best fit the requirements necessary for carrying out the applications. The results of these analyses are the identification of:

- Smart Grid standards and the nature of their fit to the applications;
- Additional PAPs that are needed to address the gaps and overlaps; and
- High-priority use cases that merit detailed analysis and development.

The DEWGs as of May 2011 include:

- **Transmission and Distribution (T&D)** – This DEWG works to enhance reliability and improve resilience to grid instabilities and disturbances. It also works to improve power quality to meet customer needs and efficiency, and to enable ready access for distributed generators to the grid. Recent activities include creating a list of phasor data concentrator requirements, conducting the initial discussions to determine if efforts related to electromagnetic interference should be a PAP or a Working Group and recommended to the SGIPGB that an Electromagnetic Interoperability Issues (EMII) Working Group be established, creating a white paper on weather-related standards, and providing technical comments to NIST on the Guiding Principles for Identifying Standards for Implementation from Release 1.0.
- **Home-to-Grid (H2G)** – This DEWG is investigating communications between utilities and home devices to facilitate demand response programs that implement energy management. The DEWG has agreed on a set of goals and has written white papers for the four target segments: government, electric industry, consumers, and residential product manufacturers. The DEWG has produced six white papers: Requirements; The Key Starting Point for a Business-Level Roadmap to Achieve Interoperable Networks, Systems, Devices in the Smart Grid; Privacy of Consumer Information in the Electric Power Industry; Free Market Choice for Appliance Physical Layer Communications; Appliance Socket Interface; and Electromagnetic Compatibility Issues for Home-to-Grid Devices.
- **Building-to-Grid (B2G)** – This DEWG represents the interests and needs of building consumers. It envisions conditions that enable commercial buildings to participate in energy

Working Draft

markets and perform effective energy conservation and management. The DEWG is responsible for identifying interoperability issues relevant to the building customer and providing direction on how to address those issues. The B2G DEWG has examined use cases for weather data exchange and proposed an approach for standard weather data exchange, and has participated in the formation and further development of the concept of the Energy Services Interface (ESI) and definition of the customer interface. The DEWG has also explored energy management beyond electricity (e.g., combined heat and power [CHP], district energy, thermal storage, etc.).

- **Industry-to-Grid (I2G)** – This DEWG identifies business and policy objectives and requisite interactions, and also identifies standard services and interfaces needed for interoperability (e.g., syntax and semantics of information transfer, service interface protocols). This DEWG is preparing a transition strategy for future energy transfers between industrial facilities and the electric grid, in various manifestations, to meet fluctuating demand at predictable quality and price. This should be accomplished while acknowledging variable supplier delivery capability and regulatory requirements, and while optimizing energy conservation. This DEWG developed a presentation, on the Organization for the Advancement of Structured Information Systems (OASIS) Energy Interoperation Technical Committee (EITC), which defines the interaction between the Smart Grid and smart facilities.
- **Vehicle-to-Grid (V2G)** – This DEWG identifies the service interfaces and standards needed (e.g., syntax and semantics of information transfer, service interface protocols, cross-cutting issues, business- and policy-level issues) to create the infrastructure to make plug-in electric vehicles (PEV) a reality. This DEWG defines business objectives and prioritizes corresponding PEV-grid interactions (discharging as well as charging) that can occur at different locations under one billing account. The goal for this DEWG is to ensure that the basic infrastructure will be implemented in time to support one million PEVs by 2015.
- **Business and Policy (BnP)** – This DEWG assists business decision makers and legislative/regulatory policymakers in implementing Smart Grid policies relevant to interoperability by providing a structured approach that may be used by state and federal policymakers and by trade organizations to implement Smart Grid policies, and helps to clearly define the interoperability implications and benefits of Smart Grid policy. This DEWG serves as an educational resource and develops tools and supporting materials. The BnP DEWG sponsored a presentation to members of the National Association of Regulatory Utility Commissioners (NARUC) on behalf of NIST and the SGIP.

Additional SGIP Working Groups:

- **Terminology (TERM)** – This working group seeks to establish a common process and approach around current and developing terms and definitions in use within each of the SGIP working groups. A review and compilation of terms used by the various SGIP working groups will minimize misunderstandings and inconsistent approaches, and it will provide a common foundation and understanding for all stakeholders. Using a wide variety of sources, the group will collect the definitions of existing and new terms, and this lexicon of SGIP- and

Working Draft

Smart Grid-related terms. The collection of terms will be located on the Interoperability Knowledge Base (IKB) site[99].

- **Electromagnetic Interoperability Issues (EMII)** – This working group investigates strategies for enhancing the immunity of Smart Grid devices and systems to the detrimental effects of natural and man-made electromagnetic interference, both radiated and conducted. It addresses these electromagnetic compatibility (EMC) issues and develops recommendations for the application of standards and testing criteria to ensure EMC for the Smart Grid. In particular, the group focuses on issues directly related to interoperability of Smart Grid devices and systems, including impacts, avoidance, and generation of electromagnetic interference, as well as mitigation of and immunity to electromagnetic interference. With its focus on interoperability, this effort is not a general review of electromagnetic- and electric power-related issues, such as power quality. These issues are addressed by different groups outside the SGIP.
- **Internet Protocol Standards (IPS)** – This working group promotes the availability of IPS to support Smart Grid functionality. The goal is to enable interoperability by providing guidance and best practices to vendors, utilities, and implementers of the Smart Grid. This working group will also consider functionality related to the use of the Internet Protocol Suite in the Smart Grid.

Working Draft

[99] http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/InteroperabilityKnowledgeBase.

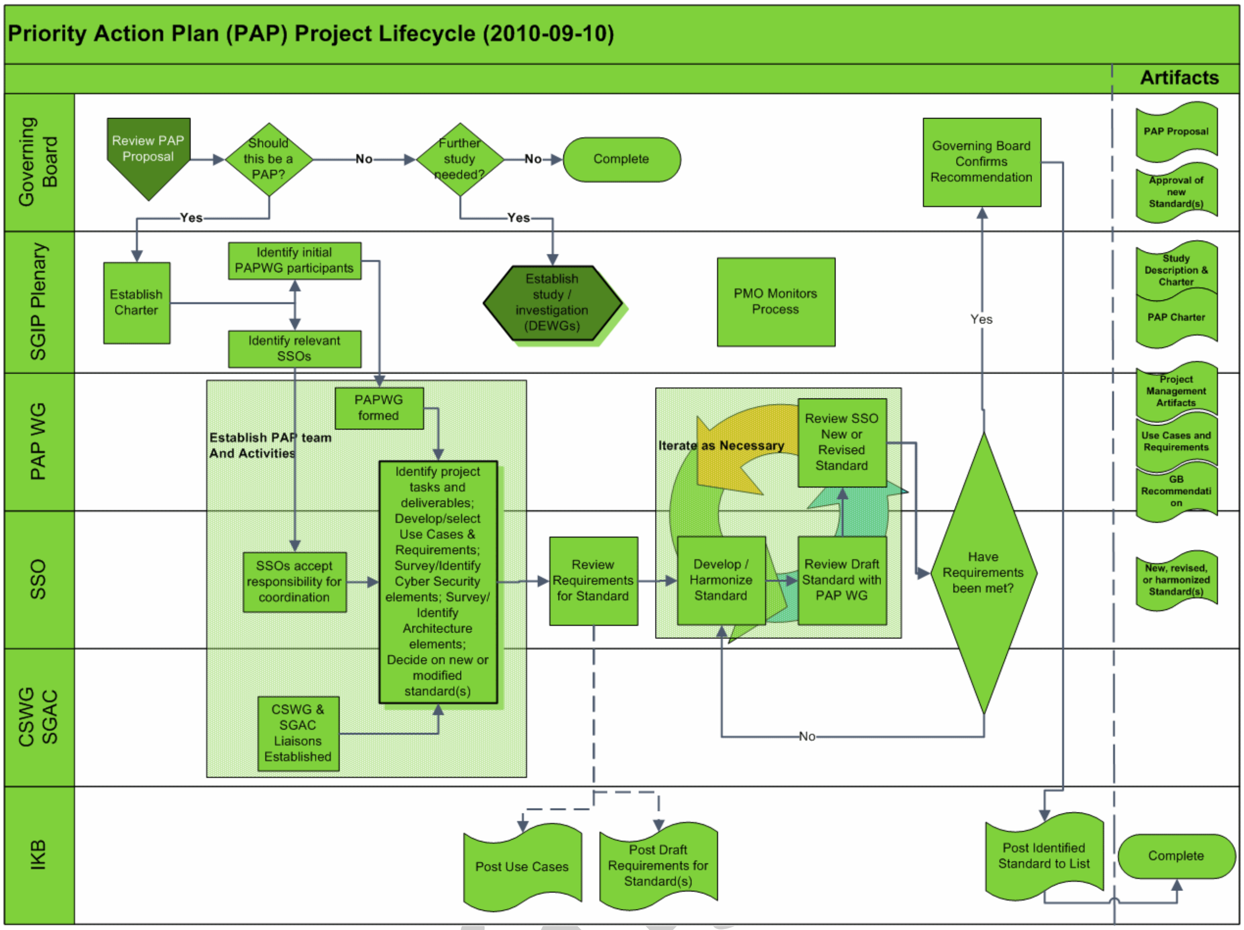

Priority Action Plan (PAP) Project Lifecycle (2010-09-10)
Artifacts
Governing Board
SGIP Plenary
PAP WG
SSO
CSWG SGAC
IKB
Review PAP Proposal
Should this be a PAP?
No
Further study needed?
No
Complete
Yes
Yes
Governing Board Confirms Recommendation
Establish Charter
Identify initial PAPWG participants
Identify relevant SSOs
Establish study / investigation (DEWGs)
PMO Monitors Process
Yes
PAPWG formed
Establish PAP team And Activities
Identify project tasks and deliverables; Develop/select Use Cases & Requirements; Survey/Identify Cyber Security elements; Survey/ Identify Architecture elements; Decide on new or modified standard(s)
SSOs accept responsibility for coordination
CSWG & SGAC Liaisons Established
Review Requirements for Standard
Iterate as Necessary
Review SSO New or Revised Standard
Develop / Harmonize Standard
Review Draft Standard with PAP WG
Have Requirements been met?
No
Post Use Cases
Post Draft Requirements for Standard(s)
Post Identified Standard to List
Complete
PAP Proposal
Approval of new Standard(s)
Study Description & Charter
PAP Charter
Project Management Artifacts
Use Cases and Requirements
GB Recommendation
New, revised, or harmonized Standard(s)

Figure 5-2. PAP Project Life Cycle

5.5. Priority Action Plans (PAPs)

PAPs are a key activity of the SGIP. They arise from the analysis of the applicability of standards to Smart Grid use cases and are targeted to resolve specific critical issues. PAPs are created only when the SGIP determines there is a need for interoperability coordination on some urgent issue.

Specifically, a PAP addresses one of the following situations:

- A gap exists, where a standard or standard extension is needed. (The need for meter image-download requirements is an example of a nonexisting standard needed to fill an identified gap.)
- An overlap exists, where two complementary standards address some information that is in common but different for the same scope of an application. An example of this is metering information, where the Common Information Model (CIM), 61850, the American National Standards Institute (ANSI) C12.19, Smart Energy Profile (SEP) 1.0, and SEP 2.0 all have nonequivalent methods of representing revenue meter readings.

PAPs are created when the SGIPGB receives proposals from SGIP members, working groups, committees, or other interested parties who have identified issues with interoperability standards, such as a gap or overlap among standards. The SGIPGB approves the PAP proposal, and experts in relevant Standards Development Organizations (SDOs) and SSOs are brought together to create the PAP working group management team. The PAPs themselves are executed within the scopes of participating SDOs and users groups that sign up for tasks that implement the plans. The SGIP facilitates this process and ensures that all PAP materials are publicly available promptly on the NIST Smart Grid Collaboration Site.

The SGIP also offers guidance to the PAP team to move difficult discussions toward resolution. Although PAPs and SDOs work together closely, there may be times when the SDOs and PAPs disagree based on their constituent viewpoints. Specific PAP tasks may diverge from the original intent of the PAP due to the SDOs' natural, and correct, orientation towards their own specific goals and needs. The PAPs, on the other hand, arise from the broader stakeholder involvement in the Smart Grid problem space, and the goals identified for a PAP reflect this broader scope. In these cases, the parties are brought together under the auspices of the SGIP, and an attempt to resolve the differences is pursued.

Working Draft

There are 19 PAPs as of July 2011, including the following:

#	Priority Action Plan	Comments
0	Meter Upgradeability Standard http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/PAP00MeterUpgradability	**Scope:** PAP00 defined requirements including secure local and remote upgrades of smart meters. **Output:** National Electrical Manufacturers Association (NEMA) Meter Upgradeability Standard SG-Advanced Metering Infrastructure (AMI) 1-2009. **Date:** Completed 2009.
1	Role of IP in the Smart Grid http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/PAP01InternetProfile.	**Scope:** For interoperable networks it is important to study the suitability of Internet networking technologies for Smart Grid applications. PAP01's work area investigates the capabilities of protocols and technologies in the Internet Protocol Suite by working with key SSO committees to determine the characteristics of each protocol for Smart Grid application areas and types. **Output:** This PAP's work culminated in publication of a Request for Comment (RFC) cataloguing a core Internet Protocol Suite for IP-based Smart Grid and its acceptance by the SGIPGB in December 2010 as a Smart Grid standard. **Date:** Completed 2010.
2	Wireless Communications for the Smart Grid http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/PAP02Wireless.	**Scope:** This PAP's work area investigates and evaluates existing and emerging standards-based physical media for wireless communications. The approach is to work with the appropriate SDOs to determine the communication requirements of Smart Grid applications and how well they can be supported by wireless technologies. Results are used to assess the appropriateness of wireless communications technologies for meeting Smart Grid applications.

Working Draft

#	Priority Action Plan	Comments
		Output: PAP02 compiled Smart Grid communication requirements and a catalog for wireless standards and their characterizations. The PAP developed an evaluation methodology published in "Guidelines for Assessing Wireless Communications for Smart Grid Applications, Version 1.0" in July 2011. **Date:** 2011.
3	Common Price Communication Model http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/PAP03PriceProduct.	**Scope:** 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. 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. PAP03 builds on existing work in financial energy markets and existing demand response programs to integrate with schedule and interval specifications under development. This PAP overlaps with others that include price and product information (4, 6, 8, 9, 10, and 11). **Expected Outputs:** OASIS Energy Market Information Exchange standard version 1.0, Zigbee Smart Energy 2.0. **Date:** 2011.
4	Common Schedule Communication	**Scope:** Under this plan, NIST and collaborators will develop a standard for

Working Draft

#	**Priority Action Plan**	**Comments**
	Mechanism http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/PAP04Schedules .	how schedule and event information is passed between and within services. The output will be a specification that can then be incorporated into price, demand-response, and other specifications. This Project Plan was developed in conjunction with PAP03 (Develop Common Specification for Price and Product Definition). Participants include, but are not limited to, International Electrotechnical Commission (IEC), North American Energy Standards Board (NAESB), other OASIS Technical Committees, and ZigBee Smart Energy Profile. **Expected Outputs:** A common standard for transmitting calendaring information will enable the coordination necessary to improve energy efficiency and overall performance. The Calendar Consortium will complete its current work in 2011 on eXtensible Markup Language (XML) serialization of iCalendar into a Web-service component (OASIS Web Services-(WS)-Calendar). **Date:** 2011.
5	Standard Meter Data Profiles http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/PAP05MeterProfil	**Scope:** The Smart Grid recognizes that several clients may require local access to meter data, and these data may be on the same order of complexity as the meter itself. Such potential clients might range from thermostats to building automation systems. Other potential clients will exist inside and outside of the customers' premises. Meter interface will reach across various domains including Operations (e.g., Metering System), Customer (e.g., Customer Energy Management System (EMS) and Submeter), and Distribution (e.g., Workforce Tool and Field Devices). The ANSI C12.19 standard contains an

Working Draft

#	Priority Action Plan	Comments
		extensive set of end device (e.g., meter) data tables. This large set of tables makes it time-consuming for utilities (and other service providers) to understand the standard and specify the proper tables for specific applications. The objective of this Priority Action Plan is to develop a smaller set of data tables that will meet the needs of most utilities and simplify the meter procurement process. **Expected Outputs:** Minimize variation and maximize interoperability of application services and behaviors within ANSI C12.18-2006, ANSI C12.19-2008, ANSI C12.21-2006, and ANSI C12.22-2008. **Date:** 2011.
6	Common Semantic Model for Meter Data Tables http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/PAP06Meter.	**Scope:** There are currently several "meter models" in standard existence. These include ANSI C12.19, Device Language Message Specification (DLMS)/ Companion Specification for Energy Metering (COSEM)/IEC 62056, IEC 61968 CIM, and IEC 61850. As the Smart Grid requires interoperation between meters and many other applications and services, the existence of unique forms of data representation pertinent to a single actor is problematic, requiring complex gateways to translate this representation into alternate formats for information sharing. PAP06 works with industry stakeholders to translate the ANSI C12.19 End Device (meter) data model to and from a common form that will allow the semantics of this and End Device models in other standards to be more readily harmonized. The objective is to allow the lossless translation from the common form to the various syntactic representations prevalent in each domain. Details will include the

Working Draft

#	Priority Action Plan	Comments
		representation of the Decade/Table/Element model. PAP06 develops an exact and reusable representation of the ANSI C12.19 data model in the presentation form of Unified Markup Language (UML). **Expected Outputs:** A side-by-side comparison of the ANSI C12.19 UML model and the IEC 61968-9 UML model to illustrate gaps and overlaps. **Date:** 2011.
7	Energy Storage Interconnection Guidelines http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/PAP07Storage	**Scope:** Energy storage is expected to play an increasingly important role in the evolution of the power grid, particularly to accommodate increasing penetration of intermittent renewable energy resources and to improve electrical power system (EPS) performance. Coordinated, consistent, electrical interconnection standards; communication standards; and implementation guidelines are required for energy storage devices (ES), power-electronics-connected distributed energy resources (DER), hybrid generation-storage systems (ES-DER), and the ES-DER aspects of plug-in electric vehicles (PEV). A broad set of stakeholders and SDOs are needed to address this coordination and evolution in order to update or augment the IEEE 1547 electrical interconnection standards series as appropriate to accommodate Smart Grid requirements and to extend the ES-DER object models in IEC 61850-7-420 as needed. Coordination with Underwriters Laboratories (UL), Society for Automotive Engineers (SAE), National Electrical Code-(NEC-) National Fire Protection Association (NFPA)70, and Canadian Standards Association (CSA) will be required to ensure safe and reliable implementation. This effort will need to

Working Draft

#	Priority Action Plan	Comments
		address residential, commercial, and industrial applications at the grid distribution level and utility/Regional Transmission Operator (RTO) applications at the grid transmission level. **Expected Outputs:** IEEE 1547.8, IEC 61850-7-420. **Date:** 2012.
8	CIM for Distribution Grid Management http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/PAP08DistrObjMultispeak.	**Scope:** 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 their wide-scale deployment, which is radically changing how the power system must operate. The use of standardized object models, such as the CIM and 61850, will support the interoperability of information exchanges that is critically needed to ensure a more reliable and efficient grid. PAP08 will coordinate with: PAPs 3, 4, 9, or 10 on any use cases involving Demand Response (DR), pricing signals, and other customer interactions; PAP07 on any use cases involving energy storage and Distributed Energy Resources (DER); PAP11 on any use cases involving PEVs; PAP14 on any use cases involving "CIM wires models" or transmission-related interactions; and CSWG on security efforts. **Expected Outputs:** IEC 61968, IEC 61970, and IEC 61850. **Date:** 2011.
9	Standard DR and DER Signals http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/PAP09DRDER.	**Scope:** Demand Response 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.

Working Draft

#	Priority Action Plan	Comments
		While the value of DR is generally well understood, the interaction patterns, semantics, and information conveyed vary. Defining consistent signal semantics for DR will make the information conveyed more consistent across Smart Grid domains. **Expected Outputs:** OASIS Energy Interoperation standard version 1.0, Zigbee Smart Energy 2.0. **Date:** 2011.
10	Standard Energy Usage Information http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/PAP10EnergyUsagetoEMS.	**Scope:** This action plan led to data standards to exchange detailed information about energy usage in a timely manner. The first goal was agreement on the 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 energy efficiency. **Outputs:** Implementation of a plan to expedite harmonized standards development and adoption: OASIS, IEC61970/61968, IEC61850, ANSI C12.19/22, PAP17/ American Society of Heating, Refrigerating and Air Conditioning Engineers (ASHRAE) SPC201, and ZigBee Smart Energy Profile (SEP) 2.0.

Working Draft

#	Priority Action Plan	Comments
		Date: Completed 2011.
11	Common Object Models for Electric Transportation http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/PAP11PEV.	**Scope:** PAP11 ensures that the grid can support the massive charging of cars and help to popularize the adoption of PEVs. Standards will optimize charging capabilities and vendor innovation, allowing for more creative engineering and automobile amenities. This PAP also supports energy storage integration with the distribution grid as addressed by PAP07. **Expected Outputs:** SAE J1772, SAE J2836/1, and SAE J2847/1. SAE J1772 and SAE J2836/1 standards have been completed and approved, and they are included in the Catalog of Standards. SAE J2847/1 will be submitted for approval later in 2011. **Date:** 2011.
12	Mapping IEEE 1815 (DNP3) to IEC 61850 Objects http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/PAP12DNP361850.	**Scope:** This action plan focuses on developing the means to enable transport of select Smart Grid data and related services over legacy Distributed Network Protocol (DNP)3 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. This is to be published as IEC 61850-80-2, Standard for Exchanging Information between Networks Implementing IEC 61850 and IEEE Std 1815 (DNP3). DNP3 was adopted by IEEE as Standard 1815 in 2010. IEEE is now developing Standard 1815.1 which includes upgraded security. **Expected Outputs:** IEC 61850-80-2, IEEE

Working Draft

#	Priority Action Plan	Comments
		1815.1. **Date:** 2011.
13	Harmonization of IEEE C37.118 with IEC 61850 and Precision Time Synchronization http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/PAP1361850C27118HarmSynch	**Scope:** The current primary standard for the communication of phasor measurement unit (PMU) and phasor data concentrator (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 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, 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. **Expected Outputs:** IEEE C37.118.2 (updated version), IEC 61850-90-5, and IEEE C37.238. **Date:** 2011.
14	Transmission and Distribution Power Systems Model Mapping http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/PAP14TDModels.	**Scope:** PAP14's work defines strategies for integrating standards across different environments to support different real-time and back-office applications. Strategies call for defining key applications and evaluating the available standards for meeting the requirements of such applications. Modeling of the electric power system, multifunctional Intelligent Electronic Devices (IEDs), and definition of standard methods for reporting events

Working Draft

#	Priority Action Plan	Comments
		and exchanging relay settings will meet the requirements for improvements of the efficiency of many protection, control, engineering, commissioning, and analysis tasks. Field equipment can supply the raw data for objects and measured parameters used across the enterprise based on the standard models and file formats defined. **Expected Outputs:** updates to IEC 61850, IEC 61970, IEC 61968, IEEE C37.239, IEEE C37.237, and MultiSpeak v1-v4. **Date:** 2011.
15	Harmonize Power Line Carrier Standards for Appliance Communications in the Home http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/PAP15PLCForLowBitRates.	**Scope:** The goal of this PAP is to enable the development of an interoperable profile containing common features for home appliance applications where the resulting implementation of this profile leads to interoperable products. **Expected Outputs:** Updates to relevant standards including ITU G.Hn (G.9960, G.9961, G.9972), IEEE P1901 (HomePlug ™, High Definition Power Line Communication (HD-PLC™), and Inter-System Protocol (ISP)), and ANSI/ Consumer Electronics Association (CEA) 709.2 (Lonworks™). **Date:** 2011.
16	Wind Plant Communications http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/PAP16WindPlantCommunications	**Scope:** The goal of PAP16 is development of a wind power plant communications standard. **Expected Output:** IEC 61400-25, Wind Plant Communications, based on IEC 61850. **Date:** 2011.
17	Facility Smart Grid Information Standard http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/PAP17FacilitySmartGridInformationStandard	**Scope:** This priority action plan will lead to development of a data model standard to enable energy-consuming devices and control systems in the customer premises to manage electrical loads and generation sources in response to communication with

Working Draft

#	Priority Action Plan	Comments
		the Smart Grid. It will be possible to communicate information about those electrical loads to utilities, other electrical service providers, and market operators. This PAP will leverage the parallel PAP10 effort and other related activities and models, such as IEC CIM, SEP 2.0, IEC 61850.7-420, and PAPs 3, 4, and 9. **Expected Output:** Development of an ANSI-approved Facility Smart Grid Information Standard that is independent of the communication protocol used to implement it. **Date:** 2011.
18	SEP 1.x to SEP 2 Transition and Coexistence http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/PAP18SEP1To2TransitionAndCoexistence	**Scope:** This action plan focuses on developing specific requirements to allow the coexistence of SEP 1.x and 2.0 and to support the migration of 1.x implementations to 2.0. Because it is a deployment-specific issue, the PAP will not address whether new deployments should be 1.x or 2.0. The effort assumes 1.x in the field as the starting point and assumes that the meters themselves are capable of running SEP 1.x or 2.0 via remote firmware upgrade. **Expected Output:** The PAP has produced a white paper summarizing the key issues with migration and making specific recommendations and a requirements document to be submitted to the ZigBee Alliance for consideration in developing the technology-specific recommendations, solutions, and any required changes to the SEP 2.0 specifications themselves. **Date:** 2011.

2201

Working Draft

5.6. The Interoperability Knowledge Base and the NIST Smart Grid Collaboration Site

All SGIP outputs are available to the public through the NIST Smart Grid Collaboration Site (also referred to as “the wiki” or “the Twiki”) and through the Interoperability Knowledge Base (IKB) Web site.

The wiki site allows for interactive communication of information among stakeholders and other interested parties.

The goal of the IKB is to create a comprehensive repository for Smart Grid technical knowledge. As such, the IKB must provide mechanisms to capture and collate information from the broad stakeholder composition of the SGIP. Figure 5-2 shows how the committees and working groups of the SGIP feed content into the IKB.

Working Draft

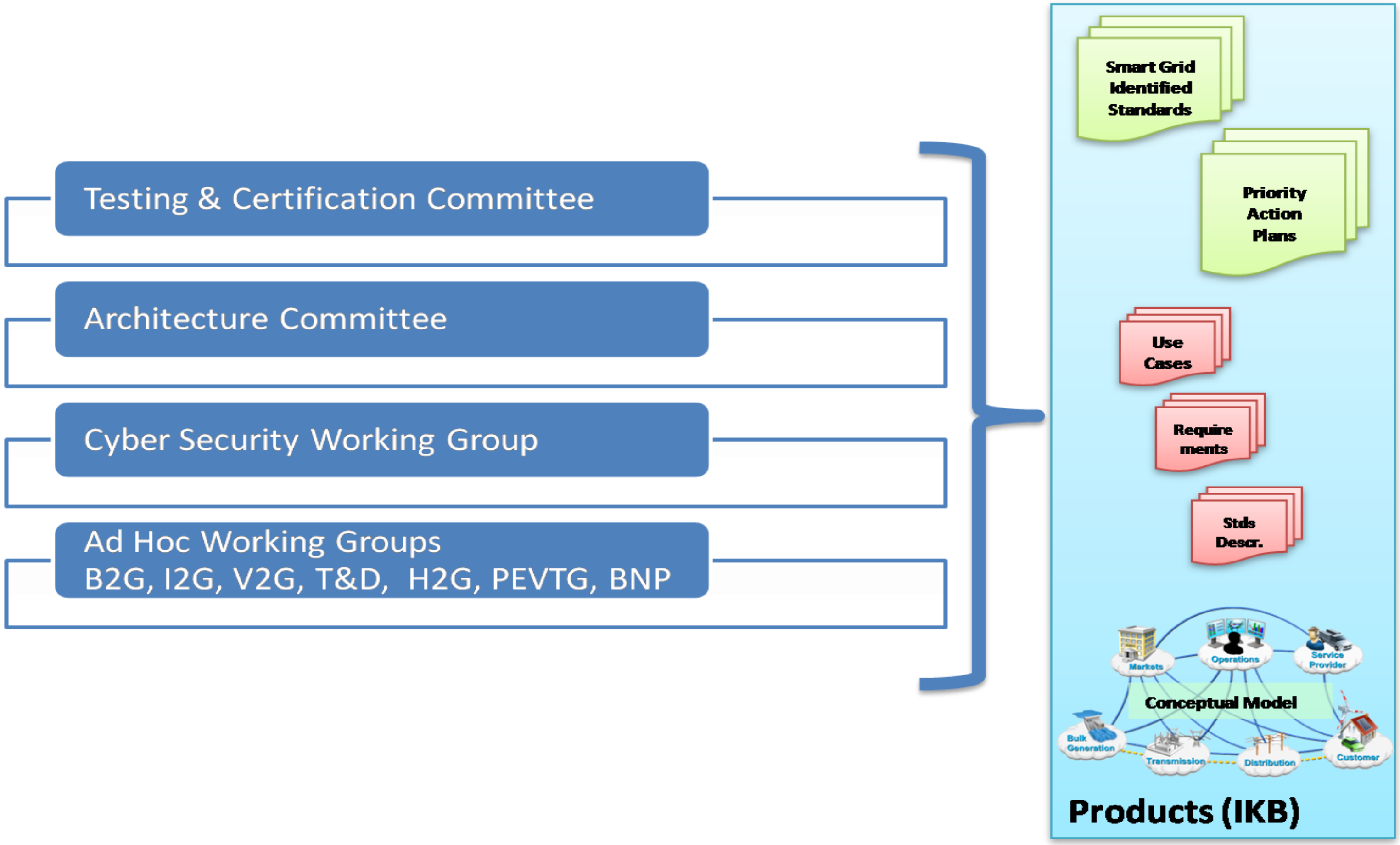


Figure 5-2. The Flow of Content from SGIP Committees and Working Groups into the IKB

5.7. Future SGIP Activities

5.7.1. SEP1.x Migration (PAP18)

Over the past few years, smart meter deployments have been steadily increasing, with millions of meters both being installed. Concurrent with this widespread deployment and the NIST-established SGIP standards acceleration effort, the Department of Energy (DOE) awarded $3.4 billion in Smart Grid Investment Grants in 2009. In late 2006, an effort was undertaken in the ZigBee Alliance, an SSO that develops wireless standards and certifies wireless products, to define a smart energy application profile based on interest from meter companies, utilities and in-home device manufacturers. The application profile was designated as the "ZigBee Smart Energy Profile (SEP)." This profile was released in 2008 and was based on the existing ZigBee PRO stack, a binary application protocol unique to the ZigBee Alliance for networking over the IEEE 802.15.4 standard, and using elliptic curve cryptography from a single supplier. Currently, over 100 products have been certified to SEP 1.0.

In late 2009, a liaison was launched between the ZigBee Alliance and the HomePlug Alliance to define the next evolution of the profile, dubbed "SEP 2.0." In this version, ZigBee addressed several key features, including support of multiple Media Access Control/Physical (MAC/PHY) layers, multiple security protocols, and requirements from the Open Home Area Network (OpenHAN) organization. As a result of significant architectural changes and feature upgrades, SEP 2.0 is not backwards-compatible with SEP 1.x at the network and application layers or in the security architecture. This is a known issue and has been broadly communicated as the development of SEP 2.0 has progressed. Because many meters are being or have already been deployed using SEP 1.x, there is much discussion on whether an upgrade is necessary and, if so, what that transition and migration path should look like. The main focus and outputs of the PAP are:

- PAP 18 was formed to develop specific requirements that must be met to allow for the coexistence of SEP 1.x and 2.0 and to support the migration of SEP 1.x implementations to SEP 2.0. This effort will not address the issue of whether new deployments should be SEP 1.x or SEP 2.0, which is a deployment-specific issue. The effort assumes 1.x in the field as the starting point. Further, this effort assumes that the meters themselves are capable of running SEP 1.x or SEP 2.0 via remote firmware upgrade. The focus of the effort is on the events leading up to and impact of such an upgrade.
- The primary outputs of the PAP are 1) a white paper that summarizes the key issues with migration from SEP 1.x to SEP 2.0 and makes specific recommendations; and 2) a requirements document that will be submitted to the ZigBee Alliance for consideration in developing the technology specific recommendations, solutions, and any required changes to the SEP 2.0 specifications themselves.

5.7.2. New Distributed Renewables, Generators, and Storage Domain Expert Working Group

The SGIP has created a Distributed Renewables, Generators, and Storage (DRGS) Domain Expert Working Group (DEWG) to provide a forum within the SGIP to identify standards and

Working Draft

interoperability issues and gaps related to Smart Grid integration of distributed renewable/clean energy generators and electric storage, and to initiate priority action plans and task groups to address these issues and gaps. Resolution of these issues and gaps is essential to enable high penetration of renewables and storage while also enhancing grid stability, resiliency, power quality, and safety.

Of particular importance are Smart Grid functions that 1) enable grid integration of intermittent distributed renewable generators, 2) enable distributed generator/storage devices to provide valuable grid supportive ancillary services, 3) prevent unintentional islanding of clustered distributed generator/storage devices, and 4) provide acceptable distributed generator/storage device fault response without cascading events. The DRGS DEWG will also address communication needed for distributed control of generator/storage devices within weak grids and microgrids, including the interaction of devices having high-bandwidth power electronics-based grid interfaces (such as photovoltaic generators and battery storage) with rotating machine devices having high intrinsic inertia.

5.7.3. Addition of Reliability and Implementation Inputs to Catalog of Standards Life Cycle Process

The SGIP is considering methods to solicit additional inputs and guidance from Smart Grid stakeholders regarding reliability and implementation issues raised by standards completing the Catalog of Standards (CoS) life cycle process. Stakeholders engaged in this fashion would review documents and standards that are considered for addition to the CoS. These reviews would provide analysis to industry and regulators of the potential impacts to system reliability and implementation. It is believed that this approach will facilitate greater involvement by utilities in the SGIP CoS's life cycle process.

Working Draft

6. Cybersecurity Strategy

6.1. Cybersecurity in the Smart Grid

Traditionally, cybersecurity for information technology (IT) focuses on the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability. Cybersecurity for the Smart Grid requires an expansion of this focus to address the combined power system, IT, and communication systems in order to maintain the reliability and the security of the Smart Grid to reduce the impact of coordinated cyber-physical attacks,[100] and to protect the privacy of consumers. Smart Grid cybersecurity must include a balance of both power- and cyber-system technologies and processes in IT and in power system operations and governance. Care must be taken to apply practices directly from one sector, such as the IT or communications sector, to the power sector because doing so may degrade reliability and increase risk. This is because the requirements for the power sector, for timing of communications, for example, may be different from the IT and communications sectors.

Therefore, cybersecurity for the power industry must cover all issues involving automation and communications that affect the operation of electric power systems and the functioning of the utilities that manage them. Education of the power industry about cybersecurity policy, procedures, and techniques—as well as on the various management, operational, and technical requirements that are necessary and available to secure power system resources—must be conducted. In the power industry, the focus has been on implementation of equipment that could improve power system reliability. Communications and IT equipment were formerly viewed as just supporting power system reliability. However, both the communications and IT sectors are becoming more critical to the reliability of the power system.

Cybersecurity must address deliberate attacks, industrial espionage, and inadvertent compromises of the information infrastructure due to user errors, equipment failures, and natural disasters. Vulnerabilities might allow networks to be penetrated, control software to be accessed, and load conditions to be altered, thus destabilizing the electric grid in unpredictable ways. Many electric sector infrastructures were designed and installed decades ago with limited cybersecurity consideration. Increasing connectivity, integration with legacy systems, the proliferation of access points, escalating system complexity, and wider use of common operating systems and platforms may contribute to increased risks for the Smart Grid. The potential risk to critical infrastructure as a result of coordinated attacks against the Smart Grid or cyber-attacks in conjunction with natural disasters/phenomena is another reason why a defense-in-depth approach to Smart Grid cybersecurity should be adopted.

[100] Government Accountability Office (GAO) Report 11-117, *"Electricity Grid Modernization: Progress Being Made on Cybersecurity Guidelines, but Key Challenges Remain to Be Addressed"* defines cyber-physical attack as using both cyber and physical means to attack a target. Available at: http://www.gao.gov/products/GAO-11-117.

Working Draft

6.2. NIST's Role in Smart Grid Cybersecurity

To address the cross-cutting issue of cybersecurity, the National Institute of Standards and Technology (NIST) established the Cybersecurity Coordination Task Group (CSCTG) in early 2009. This group was integrated into the NIST Smart Grid Interoperability Panel (SGIP) as a standing working group and was renamed the SGIP Cybersecurity Working Group (CSWG). The CSWG has designated liaisons within the Smart Grid Architecture Committee (SGAC), the Smart Grid Testing and Certification Committee (SGTCC), and the Priority Action Plans (PAPs). Some members of the CSWG are also active participants in the SGAC, the SGTCC, the PAPs, and the Domain Expert Working Groups (DEWGs) in the SGIP.

As specified in the SGIP Charter and Bylaws, a NIST representative chairs the CSWG. The CSWG management team also includes three vice chairs and a secretariat—volunteers from the membership who are able to commit on average 20 hours a week to CSWG activities. In addition, three full-time support staff serve on the team. Currently, there are eight subgroups, with each subgroup containing one or two leads. Table 6-1 provides a description of the subgroups and their activities. The CSWG now has more than 650 participants, comprising national and international members from 22 Smart Grid stakeholder categories including utilities, vendors, and service providers, academia, regulatory organizations, state and local government, and federal agencies. Members of the CSWG assist in defining the activities and tasks of the CSWG, attend the SGIP and SGIP Governing Board (SGIPGB) meetings, and participate in the development and review of the CSWG subgroups' projects and deliverables.

A biweekly conference call is held by the CSWG chair to update the membership on the subgroups' activities, SGIP activities, and other related information. Subgroups hold regular conference calls while actively working on a project. An active outreach program was established in August 2010, with members participating in the all-day events held across the country. Information on the CSWG, subgroups, outreach, and all associated documents can be found on the NIST Smart Grid Collaboration Site.[101]

Table 6-1. Cybersecurity Working Group Subgroups

CSWG Subgroup	Subgroup Description
AMI Security Subgroup	The Advanced Metering Infrastructure (AMI) Security subgroup operates under the SGIP's CSWG and in collaboration with the Utility Communications Architecture International Users Group (UCAIug) Open Smart Grid (OpenSG) Technical Committee Smart Grid Security Working Group (SG Security). This subgroup was created in late 2010 to accelerate the standardization of a set of AMI security requirements by a formally recognized standards development

[101] http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/CyberSecurityCTG.

Working Draft

CSWG Subgroup	Subgroup Description
	organization (SDO) or a selected standards-setting organization (SSO).
Architecture Subgroup	The Architecture subgroup has initiated the development of a conceptual Smart Grid cybersecurity architecture based on the high-level requirements, standards analysis, overall Smart Grid architecture, and other cybersecurity information from NIST Interagency Report (NISTIR) 7628. (Note: NISTIR 7628 is discussed further below, in Section 6.3.1.)
Design Principles Subgroup	The Design Principles subgroup (DPG) was created after publishing NISTIR 7628 to continue the work of identifying bottom-up problems and design considerations developed by the former Bottom-up, Vulnerability, and Cryptography and Key Management subgroups.
High-Level Requirements Subgroup	The High-Level Requirements (HLR) subgroup developed an initial set of security requirements applicable to the Smart Grid, published in NISTIR 7628. The security requirements are specified for logical interface categories rather than for individual logical interfaces. To create the initial set of security requirements, this subgroup reviewed security source documents, and then identified and tailored existing security requirements applicable to the Smart Grid.
Privacy Subgroup	The Privacy subgroup conducted a privacy impact assessment (PIA) for the consumer-to-utility portion of the Smart Grid to include an initial set of issues and guidelines for protecting privacy within the Smart Grid environment. The Privacy subgroup continues to investigate privacy concerns including interfaces between consumers and non-utility third parties, as well as utilities and other third parties.
Research and Development (R&D) Subgroup	The R&D subgroup identifies problems that arise or are expected to arise in the Smart Grid that do not yet have commercially viable solutions. The R&D subgroup identified in NISTIR 7628 an initial set of high-priority R&D challenges, as well as R&D themes that warrant further discussion. Many of the topics are now being addressed by other industry groups, by federal agencies, and by the Design Principles subgroup.
Standards Subgroup	The Standards subgroup assesses standards and other documents with respect to the cybersecurity and privacy requirements from NISTIR 7628. These assessments are performed on the standards contained in the Framework or when PAPs are finalizing their recommendations.
Testing and Certification Subgroup	Created in late 2010, the Testing and Certification (TCC) subgroup establishes guidance and methodologies for cybersecurity testing of Smart Grid systems, subsystems, and components. The subgroup

Working Draft

CSWG Subgroup	Subgroup Description
	focuses on developing cybersecurity testing guidance and test cases for Smart Grid systems, subsystems, and components for their hardware, software, and processes, and assisting the SGIP's SGTCC and internal NIST Smart Grid conformance projects.

6.3. Progress to Date

Since early 2009, the working group has been actively addressing the cybersecurity needs of the Smart Grid. This section describes three major work efforts that the working group has completed.

6.3.1. Release of National Institute of Standards and Technology Interagency Report (NISTIR) 7628

The first draft of NISTIR 7628 was released in September 2009. The preliminary report distills use cases collected to date, requirements and vulnerability classes identified in other relevant cybersecurity assessments and scoping documents, as well as other information necessary for specifying and tailoring security requirements to provide adequate protection for the Smart Grid.

The NISTIR 7628 second draft was released in February 2010 and contains sections on the overall security strategy for the Smart Grid, updated logical interface diagrams, privacy, bottom-up analysis, and vulnerability class analysis sections. New chapters on research and development themes, the standards assessment process, and a functional logical Smart Grid architecture are also included.

The NISTIR 7628 v1.0,[102] released in August 2010, addresses documented comments submitted on the second draft and includes chapter updates. The new content contains basic information on security architecture and a section on cryptography and key management. The responses to the comments received on the second draft of the NISTIR were also posted on a CSWG Web site.[103]

An introduction to the NISTIR 7628,[104] released in September 2010, provides a high-level summary of the three-volume report, and serves as an introduction and background to the technical report. This document was written for an audience that is not familiar with cybersecurity.

Working Draft

[102] http://www.nist.gov/smartgrid/upload/nistir-7628_total.pdf.

[103] http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/NISTIR7628Feb2010.

[104] http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/CyberSecurityCTG#NISTIR_7628_v1_0_and_Related_Doc.

6.3.2.Standards Reviews

The Standards subgroup assesses standards and related documents with respect to the cybersecurity and privacy requirements from NISTIR 7628. These assessments are performed on the standards contained in the Framework or on PAP recommendations in final process. During these assessments, the subgroup determines if a document does or should contain privacy or cybersecurity requirements, correlates those requirements with the cybersecurity requirements found in NISTIR 7628, and identifies any gaps. Finally, recommendations are made for further work needed on the reviewed documents to mitigate any gaps. Standards listed in the SGIP Catalog of Standards (CoS) have a 30-day public review process.

To date, the Standards subgroup has produced detailed reports that contain analysis and recommendations for improvements in the following standards:

- Association of Edison Illuminating Companies (AEIC) Metering Guidelines;
- American National Standards Institute (ANSI) C12.1: American National Standard for Electric Meters Code for Electricity Metering; ANSI C12.18: : American National Standard Protocol Specification for ANSI Type 2 Optical Port;
- ANSI C12.19: American National Standard For Utility Industry End Device Data Tables; ANSI C12.21: American National Standard Protocol Specification for Telephone Modem Communication;
- ANSI C12.22: American National Standard Protocol Specification For Interfacing to Data Communication Networks;
- International Electrotechnical Commission (IEC) 60870-6/ Telecontrol Application Service Element (TASE).2/ Inter-Control Centre Communications Protocol (ICCP): Control Center to Control Center Information Exchanges;
- IEC 61850: Communications Networks and Systems for Power Utility Automation;
- IEC 61968: Common Information Model (CIM) and Messaging Interfaces for Distribution Management;
- IEC 61970: CIM for Wires Models;
- IEC 62351: Power Systems Management and Associated Information Exchange - Data and Communications Security, Parts 1 through 7;
- North American Energy Standards Board (NAESB) Energy Usage Information;
- National Electrical Manufacturers Association (NEMA) Upgradeability Standard (NEMA SG AMI 1-2009);
- Organization for the Advancement of Structured Information Standards (OASIS) Web Services (WS)-Calendar;
- Role of Internet Protocol Suite (IPS) in the Smart Grid, an Internet Engineering Task Force (IETF)-proposed document;
- SAE J1772-TM: Society of Automotive Engineers (SAE Electric Vehicle and Plug in Hybrid Electric Vehicle Conductive Charge Coupler;
- SAE J2847/1: Communication between Plug-in Vehicles and the Utility Grid;

Working Draft

- SAE J2836/1: Use Cases for Communication between Plug-in Vehicles and the Utility Grid;
- Institute of Electrical and Electronic Engineers (IEEE) C37.238/D5.7, Draft Standard Profile for Use of IEEE Std. 1588 Precision Time Protocol in Power System Applications;
- International Electrotechnical Commission (IEC) 61850-90-5, Harmonization of IEEE C37.118 with IEC 61850 and Precision Time Synchronization; and
- IEEE 1588, IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems.

6.3.3. Cybersecurity Working Group (CSWG) Three-Year Plan

In 2011, the CSWG updated a CSWG Three-Year Plan,[105] which describes how the CSWG will continue to implement the strategy defined in NISTIR 7628 and address the outstanding issues and remaining tasks defined in Section 1.4 of the NISTIR. The Three-Year Plan provides an introduction to the CSWG and a detailed description of the eight subgroups, including their goals, milestones, and activities over the next three years. The document also specifies additional activities such as outreach, coordination, and collaboration with various key stakeholders, including international organizations, private sector organizations, and state regulatory bodies.

6.4. CSWG Current and Future Activities

The activities listed in this section supplement the activities that are conducted by the CSWG subgroups listed in Table 6-1. Many of the activities will include active participation of subgroup members. For example, when the CSWG management participates in the full or multi-day outreach events, a member of the Privacy subgroup briefs the privacy portion. The meter testing and certification project, begun with members of the SGTCC in 2010, requires multiple CSWG subgroups to participate.

6.4.1. Risk Management Framework

The CSWG is participating in a Department of Energy (DOE), Office of Electricity Delivery and Energy Reliability (OE), public-private initiative to develop a harmonized energy sector enterprise-wide risk management process, based on organization missions, investments, and stakeholder priorities. The initiative leadership team includes NIST, the North American Electric Reliability Corporation (NERC), and the CSWG. The initiative will comprise an open collaborative process with participants from the Department of Homeland Security (DHS), the National Rural Electric Cooperatives Administration (NRECA), the National Association of Public Utility Commissioners (NARUC, which represents State Public Utility Commissions/Public Service Commissions), Municipal Electric Systems (American Public Power Association), the Federal Energy Regulatory Commission (FERC), and Investor-Owned Utilities (Edison Electric Institute). Starting with the existing electric grid and transitioning to the evolving Smart Grid, this effort will provide guidance for an integrated organization-wide approach to managing cybersecurity risks for operations, assets, data, personnel, and organizations across the United States electric grid and the interconnections with Canada and

[105] http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/CSWGRoadmap.

Working Draft

Mexico. This guideline will leverage the NISTIR 7628, *Guidelines for Smart Grid Cybersecurity,*[106] the NERC Critical Infrastructure Protection (CIP) reliability standards,[107] NIST cybersecurity publications (especially NIST SP 800-39, Managing Information Security Risk: Organization, Mission, and Information System View[108],), the National Infrastructure Protection Plan (NIPP) Risk Management Framework,[109] and lessons learned within the federal government and private industry.

6.4.2. Cyber-Physical Attack Research

As described in NISTIR 7628 and in the Government Accountability Office (GAO) Report[110] mentioned earlier, the Smart Grid is vulnerable to coordinated cyber-physical attacks against its infrastructure. Assessing the impact of coordinated cyber-physical attacks will require expertise in cybersecurity, physical security, and the electric infrastructure. The CSWG recognizes that collaboration is critical to effective identification of cyber and physical vulnerabilities and threats. During Fiscal Year (FY) 2012, the CSWG will actively pursue collaborations with other organizations already starting to address the combined cyber-physical attack vector. By providing critical cybersecurity expertise, the CSWG can identify this challenge and take steps to mitigate the potential impact these types of attacks could have on the Smart Grid.

6.4.3. Smart Grid Cybersecurity Test Guidance

The CSWG continues to expand coordination with the SGTCC to develop guidance and recommendations on Smart Grid conformance, interoperability, and cybersecurity testing. The guidance and processes developed apply to the utility sector laboratories and utilities conducting cybersecurity and/or interoperability testing to evaluate Smart Grid systems, subsystems, and components.

6.4.4. NISTIR 7628 Updates

As threats and risks change, as SSOs create new and update existing standards, and as regulatory bodies create new and update existing regulations relative to the electric sector, the CSWG will review and assess how these changes should be reflected in NISTIR 7628. Depending upon the topic discussed, new CSWG subgroups and NISTIR 7628 document sections may be created. The CSWG will review NISTIR 7628 approximately every 18 months. The topics under consideration for a future update of NISTIR 7628 include:

Working Draft

[106] http://csrc.nist.gov/publications/nistir/ir7628/introduction-to-nistir-7628.pdf.

[107] http://www.nerc.com/page.php?cid=2|20.

[108] http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf.

[109] http://www.dhs.gov/files/programs/editorial_0827.shtm#0.

[110] GAO Report 11-117, *"Electricity Grid Modernization: Progress Being Made on Cybersecurity Guidelines, but Key Challenges Remain to Be Addressed"* defines cyber-physical attack as using both cyber and physical means to attack a target. Available at: http://www.gao.gov/products/GAO-11-117.

- Creating a matrix of privacy concerns in multiple settings and expanding the section on the Smart Grid impact on privacy concerns;
- Initiating a task within the SGIP SGAC to ensure the conceptual security architecture is harmonized with the SGAC conceptual architecture during its development; and
- Adding additional high-level cybersecurity requirements that are identified during the standards reviews and supplemental work that the subgroups undertake. The list of potential new cybersecurity requirements resides on the NIST Smart Grid Collaboration Site.[111] CSWG members are encouraged to periodically review and provide comment and feedback on the list to the High-Level Security Requirements subgroup.

6.4.5. Outreach and Education

The CSWG will meet with asset owners, private sector companies, specific regulatory bodies, and other stakeholders to provide explanatory information about uses and applications for NISTIR 7628. The CSWG has established outreach and education activities with private companies, academia, and public utility commissions (PUCs). Meetings have been held with the PUCs in California, Ohio, Texas, and Colorado. [112]

The CSWG outreach activities will continue, and as new guidelines are developed, the outreach briefing material will be updated. CSWG management, as well as subgroup leads, frequently brief CSWG-related information at conferences held throughout the United States and internationally. The calendar of current CSWG outreach activities may be found online.[113]

6.4.6. Coordination with Federal Agencies and Industry Groups

The goal of interagency and other industry group communication is to promote coordination among participants of the various Smart Grid cybersecurity programs and projects, including other cybersecurity working groups, local, state and federal governments, and international organizations. The objective is to keep all individuals informed and aware of activities of the CSWG, allowing for collaboration between the various groups. Current and future coordination activities will include information exchanges with the Department of Defense, DOE, Federal Bureau of Investigation, FERC, NERC, National Electric Sector Cybersecurity Organization (NESCO), and Smart Grid Security. Other federal agencies and industry groups will be added as information exchanges and requirements continue to be developed.

6.4.7. Face-to-Face (F2F) Meetings

In 2009, a series of working sessions to develop NISTIR 7628, version 1.0, constituted the initial set of CSWG face-to-face meetings. The CSWG will continue to schedule face-to-face meetings

[111] http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/CyberSecurityCTG.

[112] http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/CSWGOutreach.

[113] http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/CSWGOutreach.

Working Draft

on an as-needed basis and during SGIP events in order to provide a venue for the following activities:

- Have technical working sessions on specific cybersecurity areas;
- Plan future activities of the CSWG; and
- Coordinate tasks that fall under multiple subgroups.

6.4.8. SGIP Liaisons

The SGIP consists of a Governing Board, Program Management Office, standing committees, DEWGs, and PAPs. The CSWG has established a liaison with each of these groups to exchange information and to ensure that the cross-cutting issue of cybersecurity is addressed. Because there are numerous PAPs established, significant CSWG resources are spent as liaisons to the PAPs. The liaisons must answer a list of questions created by the CSWG which, along with subsequent activities to ensure good cybersecurity coverage in each PAP, results in a considerable investment in time.

6.4.9. CSWG Future Activities

The CSWG Three-Year Plan provides detailed planned deliverables. Completion of the activities and milestones listed in the Three-Year Plan is contingent on the availability of the numerous CSWG members and on the resources available from NIST. Over the coverage period, some of the deliverables contained in the Three-Year Plan may change and new ones be added due to additional mandates.

Working Draft

7. Framework for Smart Grid Interoperability Testing and Certification

7.1. NIST-Initiated Efforts Supporting the Framework Development

The National Institute of Standards and Technology (NIST) recognizes the importance of ensuring the development and implementation of an interoperability testing and certification[114] framework for Smart Grid 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 standard conformance and interoperability testing process.

Within NIST's three-phase plan to expedite the acceleration of interoperable Smart Grid standards, developing and implementing a framework for Smart Grid interoperability testing and certification constitutes Phase III. In recognition of the importance of Smart Grid interoperability testing and certification and the need to couple it to standards identified for the Smart Grid, developing and implementing a framework for Smart Grid interoperability testing and certification is an integral part of the Smart Grid Interoperability Panel (SGIP) activities, including establishing a permanent Smart Grid Testing and Certification Committee (SGTCC) within the SGIP. The SGTCC has assumed the responsibility for constructing an operational framework, as well as the action plans for development of documentation and associated artifacts supporting testing and certification programs that support Smart Grid interoperability.

In today's standards development and testing environment, NIST understands the importance of eliminating duplication of work activities related to Smart Grid standards and interoperability testing and certification of products and services based on standards. Recognizing that some efforts exist today to test products and services based on certain Smart Grid standards, and others are under way, NIST will work with stakeholders and actors through the SGIP to develop and implement an operational framework for interoperability testing and certification that supports, augments, and leverages existing programs wherever practical.

To support the accelerated development of an operational framework, NIST initiated and completed the following two major efforts in calendar year 2010: 1) performed an assessment of existing Smart Grid standards testing programs, and 2) provided high-level guidance for the development of a testing and certification framework. Taking input from NIST, the SGTCC has developed a comprehensive roadmap for developing and implementing the operational framework and related action plans, and has launched a number of focused efforts to develop various documents, tools, and components for the framework. Further development and

[114] The term "conformity assessment" was used in Release 1.0 of the NIST Framework and Roadmap for Smart Grid Interoperability Standards to describe this NIST program. However, the term "interoperability testing and certification" is considered more accurate and appropriate in describing the nature of the program and the objective of Phase III of NIST's three-phase plan for ensuring the interoperability of Smart Grid standards. Release 2.0 will use the term "interoperability testing and certification" to describe this program and the framework hereafter.

Working Draft

implementation of the operational framework by the SGTCC is an ongoing evolutionary process with a number of activities planned for calendar year 2011 and beyond.

Once implemented, feedback from interoperability testing and certification programs to standards-setting organizations (SSOs) and other relevant bodies will become another important aspect of the Smart Grid interoperability testing and certification framework. Errors, clarifications, and enhancements to existing standards are typically identified throughout the normal interoperability testing and certification process. In order to improve the interoperability of the Smart Grid, an overall process is critical to ensure that changes and enhancements are incorporated continuously, and this process has been included in the framework development by the SGTCC.

The SGTCC provides continuing visibility for Smart Grid interoperability testing and certification efforts and programs. The SGTCC will engage all stakeholders to recommend improvements and means to fill gaps, and will work with current standards bodies and user groups to develop and implement new test programs to fill voids in Smart Grid interoperability testing and certification. NIST will continue to work closely with the SGTCC in these efforts.

7.1.1. Assessment of Existing Smart Grid Standards Testing Programs

NIST initiated and completed an in-depth study in early calendar year 2010 to assess the existing testing and certification programs associated with priority Smart Grid standards identified by NIST. The results of the study are summarized in a report titled "Existing Conformity Assessment Program Landscape."[115] In this report, the testing and conformity assessment programs relevant to 31 identified Smart Grid standards were evaluated in detail. The programs evaluated are based on standards identified in Table 4-1 and a selected number of standards listed in Table 4-2 of *NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0.*[116]

The results of this study provided NIST and the SGIP's SGTCC with the current status of existing testing programs for ensuring interoperability, cybersecurity, and other relevant characteristics. Information gathered for these programs include all elements of a conformity assessment system, including accreditation bodies, certification bodies, testing and calibration laboratories, inspection bodies, personnel certification programs, and quality registrars. The study also helped to uncover present gaps and deficiencies in the evaluated programs.

Assessment Metrics Used in the Study

The study was conducted using a set of metrics for an ideal testing and certification program. These metrics are derived from the best practices found among standards testing and certification

[115] "Existing Conformity Assessment Program Landscape" by EnerNex for NIST, http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/SGIPDocumentsAndReferencesSGTCC.

[116] http://www.nist.gov/public_affairs/releases/upload/smartgrid_interoperability_final.pdf.

Working Draft

programs from a variety of organizations both related and unrelated to the power system. The metrics used in the study are:[117]

- Conformance vs. Interoperability vs. Security testing—assessing whether there is a testing and conformity assessment program for a standard that addresses these three areas:
    - whether an implementation conforms to the standard as published—conformance;
    - whether multiple implementations are interoperable with each other—interoperability; and
    - whether the implementation correctly makes use of any security features from the standard or other security features available in the device or computer system housing the implementation—security.
- Published test procedures—assessing whether there is a published/publicly reviewed test procedure for the standard;
- Independent test labs—assessing whether there are any independent test labs not operated by product vendors;
- Lab accreditation—assessing whether there is a lab accreditation process for the lab performing the tests (The accreditation could be done by the lab itself or by another entity.);
- Certification/logo—assessing whether there is a certification or logo program for the standard;
- Feedback to standard—assessing whether there is a mechanism to improve the quality of the standard, the test procedures, and/or the operation of the test labs;
- Conformance checklist—assessing whether implementers are provided with a checklist or template in a standardized, published format to indicate what portions of the standard they have implemented;
- Self-certification—assessing whether it is possible for technology providers to self-certify its implementations;
- Reference implementation—assessing whether a reference or "golden" implementation of the standard is available; and
- Mature standard—assessing whether the standard is considered as a mature one according to several aspects (e.g., how long it has been published (> 5 years), number of implementations (> 1), mandated (by government, etc.), revisions made, etc.).

Assessment Results

The study resulted in several findings of major gaps in existing conformity testing programs. The study results show that:[118]

Working Draft

[117] From "Existing Conformity Assessment Program Landscape" by EnerNex for NIST, http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/SGIPDocumentsAndReferencesSGTCC.

- Only about one-third of the evaluated standards have a testing program at all. A few more than that had written test procedures, but no formal testing program;
- About the same number, one-third, have a users group or other means for providing feedback on the standard, updating it, and asking questions about conformity;
- Almost all of the available testing programs are for conformity to the standard only; they do not test for interoperability between systems;
- Only a few of the programs test security of communications; and
- Several of the standards are either too vague to be effectively tested or are catalogs or guidelines that were never intended to be tested.

The gaps uncovered in this study show the urgent and important need for developing and implementing an interoperability testing and certification framework to provide a comprehensive approach to close these gaps and to accelerate the development and implementation of industry programs that enable Smart Grid interoperability. NIST and the SGTCC have used the insights resulting from the study to direct subsequent interoperability testing and certification framework development efforts.

7.1.2.High-Level Framework Development Guide

In addition to the assessment of existing testing and certification programs, a development guide[119] was produced to accelerate the development of a comprehensive operational framework. The essential goal of such a framework is to present a comprehensive approach to help close the gaps uncovered in the NIST-initiated study. The guide defined and discussed the scope, the rationale, and the need for developing a comprehensive framework and action plan for Smart Grid interoperability testing and certification. The document also described various actors that have a primary role in ensuring that interoperability is achieved and presented a high-level workflow and framework artifacts for guiding the framework development.

Goals of the Framework

As stated in the guide, the primary goal of creating a testing and certification framework is to have a comprehensive approach to close the gaps uncovered in the NIST-initiated study and to accelerate the development and implementation of industry programs that enable Smart Grid interoperability. The goals of the framework are that it must:

- Help ensure a consistent level of testing for products based on the same Smart Grid standards, as well as ensure consistency in the implementation of test programs among different standards;

Working Draft

[118] From “Existing Conformity Assessment Program Landscape” by EnerNex for NIST, http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/SGIPDocumentsAndReferencesSGTCC.

[119] http://collaborate.nist.gov/twiki-sggrid/pub/SmartGrid/SGIPDocumentsAndReferencesSGTCC/SGIP-Administrator_Report_to_NIST_on_SGTCC_Framwork.pdf.

- Address test implementation and execution issues, including qualification criteria for test laboratories and accrediting organizations, and recommend best practices to ensure that test results achieve their desired intent and are used in an appropriate and consistent manner; and
- Take into consideration the evolutionary progression of the Smart Grid, and be structured to allow maturation of existing technologies and introduction of emerging technologies.

In addition, the broad adoption and success of any framework for testing and certification program for Smart Grid systems and devices require that these programs be financially viable. Two key factors to a successful new testing and certification program are:

- The cost of testing must be reasonable relative to other product costs and volume of deployment, because any testing cost becomes part of the total cost of a product. This is critical for containing the total cost of a product.
- The cost of testing must be reasonable relative to the risk of product failure in the field. Product failures in the field create cost because they may require technical remedies to be performed in the field, equipment to be replaced, service interruptions, and reduced customer satisfaction. Testing may identify these problems before the product is deployed. However, the testing costs should be justified by the risk of the potential costs associated with the failed product after deployment so that overall cost is minimized.

Elements of the Framework for Testing and Certification

To meet the guide's stated goals, NIST outlined a final operational framework for Smart Grid interoperability standards testing and certification that should, minimally, include the following elements:

- Qualification criteria for test laboratories and development of test reports;
- Qualification criteria for issuing certification documents;
- Example processes (i.e., use cases and case studies) and documentation associated with testing and certification activities that can mature over time and in concert with in-the-field deployments and technology evolution;
- Example processes that can be used in providing feedback, including best practices, to the various industry-recognized standards groups, vendors, legislators, and regulators—in order to improve standards and conformance documentation, such as test reports and certifications;
- Processes to address standards testability gaps and test capability issues that can be used to identify and communicate the need for additional working groups in support of interoperability standards development, testing, and certification;
- Recommended practices to evaluate and assess the depth of testing requirements, both for individual standards and for collections of standards that combine to address specific deployment issues;
- Recommended practices on test method and procedures documentation, as well as the use of test cases and test profiles, where applicable, in addressing interoperability issues;
- Recommended practices for the development of testing and certification profiles based upon industry-developed use cases;

Working Draft

- Recommended practices on the validation of test plans and test cases to help ensure alignment with the intent of standards and appropriate representation of expected usage in deployment. This should also include processes on the use of standardized test references or test beds (e.g. "golden" reference models and test platforms); and
- Where feasible and appropriate, these framework elements should be adopted and/or derived from existing international standards for conformance testing frameworks.

Common Processes and Tools

The framework development guide emphasizes the importance of establishing common processes and test tools to help ensure consistency and repeatability of test results. A number of terms and variants are used in commonly describing these test tools, such as "common test harness," "golden reference test equipment," and "golden reference test products." Generally, these terms represent test tools available to a test lab or end user to provide a consistent baseline test either as a stand-alone implementation or in concert with the many other types of test tools available.

A "common test harness" is essentially an automated software-based test tool that is designed to test a particular system under sets of specified conditions. Using such a tool, comparative results can be generated in which the tool provides the consistency, and the effects of changes in the system under test can be evaluated. "Golden reference test equipment" often refers to test tools that be configured in a laboratory to provide a constant ("reference") such that there is assurance that changes to the products making up a system under test or configuration variants are consistently tested in the same manner,

Testing and certification programs supporting Smart Grid interoperability are anticipated to take place across multiple test facilities. The SGTCC has cited the importance of implementing processes and test tools to provide confidence to end users, assuring that test data and measurements are generated using a common known reference to achieve repeatable results regardless of location.

7.2. SGTCC Framework Development Activities

The SGTCC is charged with the development of the operational framework and action plan for Smart Grid interoperability testing and certification. Since its establishment, SGTCC has undertaken a number of activities in the framework development process. The action plan of the SGTCC is included in a "Testing & Certification Roadmap"[120] document, which describes the plans and deliverables to be developed through the SGTCC. It is a living document that evolves through close collaboration with industry stakeholders to ensure that identified issues and needs in framework development and implementation are addressed by the SGTCC.

[120] http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/SGTCCRoadMap.

Working Draft

The SGTCC's mission is "to coordinate creation of documentation and organizational frameworks relating to compliance testing and certification to Smart Grid interoperability and cybersecurity standards."[121] The SGTCC's objectives include "the development of an action plan, with the support of relevant parties, to establish a standardized framework (e.g., tools, materials, components, and examples) that can be used by those performing testing for and certification of compliance with interoperability and cybersecurity standards."[122]

In December 2010, SGTCC completed the development of an Interoperability Process Reference Manual (IPRM), which is a critical part of the framework. The IPRM outlines the conformance, interoperability, and cybersecurity testing and certification requirements for products and services based on the Smart Grid standards. This document has been designed to capture testing and certification processes and best practices needed to verify product interoperability amongst two or more products using the same standards-based communications technology. These processes and best practices are intended for use by an Interoperability Testing and Certification Authority (ITCA) in the design and management of a testing and certification program.

In calendar year 2010, as part of the framework development, the SGTCC also worked on the development of an evaluation tool—the Interoperability Maturity Assessment Model (IMAM)—for assessing the maturity of a standard-setting activity relative to the achievement of interoperable products.

The following sections provide a brief overview of the results of these two SGTCC framework development activities.

7.2.1. Summary of the Interoperability Process Reference Manual (IPRM)

Framework of the Interoperability Process

The framework of the interoperability testing and certification process centers on the concept of having an Interoperability Testing and Certification Authority (ITCA) for each identified Smart Grid standard. As defined in the IPRM by SGTCC, an ITCA will be "the organization whose function is to promote and facilitate the introduction of interoperable products based on a standard into the marketplace."[123] In its study, NIST identified that "standards [that] moved from release to market adoptions very frequently had this type of organization defined. Those that moved slowly from standards release to market did not."[124] SGTCC believes that "the formation and maintenance of this organization, ad hoc or formal, is key to increasing the velocity of the adoptions of interoperable standards in the marketplace."[125]

Working Draft

[121] Ibid.

[122] Ibid.

[123] http://collaborate.nist.gov/twiki-sggrid/pub/SmartGrid/SGTCCIPRM/SGTCC_IPRM_Version_1.0_Updated.pdf.

[124] Ibid

[125] Ibid

Recognizing this, the Interoperability Process Reference Manual (IPRM) was developed for adoption by ITCAs. The IPRM outlines the roles and requirements of an ITCA and specifies the mandatory testing and certification processes associated with achieving interoperability for a specific standard. The IPRM also includes the recommended best practices for interoperability test constructs.

The IPRM is intended to be adopted by any ITCA that is responsible for coordinating testing and certification on a Smart Grid technology standard and driving adoption of the technology within the industry. The SGTCC has concluded that those organizations that incorporate the IPRM guidelines into their conformity testing programs will have a greater opportunity to ensure the product interoperability coming out of their conformity testing programs.

As stated in the IPRM, once an ITCA is in place, "The ITCA shall provide governance and coordination for the maintenance and administration of Interoperability Testing Laboratories and Certification Bodies in cooperation with the relevant SSOs and user groups."[126]

The roles and requirements of an ITCA, and the best practices described in the IPRM, are summarized in the following sections.

Summary of Roles and Requirements of an ITCA

The role of an ITCA is to provide governance and coordination for the maintenance and administration of Interoperability Testing Laboratories and Certification Bodies in cooperation with the relevant SSOs and user groups. It manages the end-to-end processes associated with interoperability testing and certification with appropriate infrastructure in place to support this function.

The requirements for an ITCA as specified in the IPRM are divided into the following five categories:

- **Governance** defines the structures, policies, rules, and regulations associated with the ITCA certification program. A governance process example would require the ITCA to establish and maintain an independent and vendor-neutral testing and certification oversight authority.
- **Lab Qualification** defines the requirements that shall be applied by ITCAs when recognizing testing laboratories. It should be noted that additional requirements are further detailed in International Organization for Standardization (ISO) 17025.
- **Technical Design for Interoperability and Conformance Program Design** defines the requirements needed to effectively manage the procedures and processes associated with interoperability and conformance testing.
- **Improvements** covers the controls that will need to be in place to support the interoperability testing processes.
- **Cybersecurity** covers the requirements that shall be used by the ITCA to validate the security-related components of the interoperability testing program.

[126] Ibid

Working Draft

Adoption of these requirements by an ITCA is essential for implementing a successful interoperability testing and certification program.

Leverage on Industry Best Practices

In addition to meeting the governance, lab qualification, technical design, improvements, and cybersecurity requirements, ITCAs should also leverage the industry best practices in their implementations. The IPRM has included a list of recommended best practices and guidelines for ITCAs in their development and operation of interoperability and conformance testing programs. The recommendations provided in the IPRM were generated based on input from experienced testing organizations that have evolved interoperability and conformance programs through lessons learned in executing tests for both software and hardware applications.

The recommendations may not apply directly to all testing applications; however, NIST and the SGTCC recommend that ITCAs consider them for interoperability and conformance test programs, as these practices have proven to be valuable in executing a broad cross-section of program types. Each ITCA should evaluate how these recommendations, observations, and practices apply to their specific programs and should incorporate the recommendations into their programs where applicable.

The recommended best practices in interoperability test constructs in the IPRM address three main areas:

- General test policies—include policies related to information that product vendors need to know, such as:
    - Eligibility of a product for testing and certification, and knowledge of the certification process;
    - Minimum requirements of a test report;
    - Use of valid period of a certification;
    - Conformance for interoperability;
    - Balances between cost and testing and certification; and
    - Possession of proper testing tools.
- Test suite specification (TSS)— includes the need to establish a common TSS for use by multiple test labs; TSS being test tool agnostic; and revision control of TSS. These characteristics will:
    - Ensure that the TSS defines conventions required to achieve the interoperability, and defines exact attributes and associations required for interoperability;
    - Ensure that the TSS removes or clarifies any ambiguities of a standard;

Working Draft

    - Ensure that the TSS becomes a standard managed by an SSO;
    - Associate test tools with the TSS;
    - Map test cases clearly to feature sets, use cases, and requirements;
    - Provide a mechanism for the TSS to feed back the test results to profile;
    - Ensure the repeatability of sufficient tests for all areas of conformance and interoperability; and
    - Ensure that the TSS defines test data required to execute test cases, and identifies issues with a standard that affect the interoperability.
- Attributes of a test profile in lieu of complete test suite specification—include the following recommendations for attributes of a test profile:
    - That it must be a subset of the TSS;
    - That it specify mandatory and optional elements;
    - That it specify restrictions;
    - That it restrict the standard but cannot be added to the standard;
    - That it clearly define the type of the profile and provide a name that clearly defines the objective/scope of the profile; and
    - That it be a companion document or incorporated by the SSO into its standard.

The recommendations provided in the IPRM may not apply directly to all testing applications. However, it is recommended by the SGTCC that ITCAs consider them for their interoperability and conformance test programs, as these practices have proven to be valuable in executing a broad cross-section of program types. Each ITCA should evaluate how these recommendations, observations, and practices apply to their specific programs, and should incorporate the recommendations into their programs where applicable.

7.2.2.Interoperability Maturity Assessment Model

The SGTCC has been working to further develop and refine the assessment metrics into a more rigorous Interoperability Maturity Assessment Model (IMAM).[127] The IMAM, developed and refined by the SGTCC, includes associated metrics and tools for quick and high-level maturity assessment of a standard's testing and certification program. The IMAM is an extension and refinement of the process used in the NIST study report. It includes "filtering" metrics for evaluating critical characteristics of a successful test program, and "assessment" metrics for deeper evaluation of specific strengths and weaknesses of a test program. These metrics can be

[127] SGTCC Working Group 3 internal documents: "SGIP TCC Interoperability Maturity Assessment, V0.92" and "SGIP TCC Interop Assessment Questionnaire, V0.52".

Working Draft

evaluated through a spreadsheet questionnaire developed by the SGTCC, which includes more detailed questions for each metric.

The “filtering” metrics measure a test program with respect to the following four areas:

- Interoperability Testing and Certification Authority (ITCA) as defined in the IPRM–The existence of a functional ITCA that meets ITCA requirements indicates the maturity and stability of a test program.
- Technical Specification Structure—The existence of a standard/specification that has clear conformance requirements and few options/extensions makes it much easier to develop a test and certification program.
- Product Development/Deployment Status–If products based on a standard are successfully developed and deployed with the help of a test program, it indicates a maturity of the test program.
- Customer Experience—If customers experience few interoperability issues in deploying the products, it indicates the maturity of a test program.

The “assessment” metrics evaluate the strength and weakness of a test program with respect to the following eight areas:

- Customer Maturity and Discipline—Customers’ insistence that their vendors adhere to standards and meet stringent criteria for interoperability is critical for the success of interoperability standards.
- Conformance vs. Interoperability vs. Security Testing—Conformance testing determines if an implementation conforms to a standard as written. Interoperability testing verifies if two or more implementations of a standard can successfully communicate with each other. Security testing analyzes whether the implementation correctly makes use of any security features from the standard or other security features available in the device or computer system housing the implementation. A mature test program should include all three tests.
- Published Test Procedures/Reference—A publicly published and reviewed test procedure/reference is, in general, more mature, more comprehensive, and more complete than one which is not publicly published.
- Independent Test Labs—Independent test labs are preferred, because they are more likely to be unbiased in their testing, and are likely to incorporate lessons learned from testing one implementation into the next set of tests.
- Feedback on Standards—The existence of a mechanism to provide feedbacks to standard development helps improve the quality of the standard, the test procedures, and/or the operation of the test labs.
- Conformance/Interoperability Checklist—A standard conformance/interoperability checklist can improve interoperability by allowing users to easily specify and compare implementations.

Working Draft

- Supplemental Test Tools and Test Suites—The existence of independently developed testing tools and test suites that also cover optional features and requirements is an important feature to avoid issues in standard conformance and interoperability among different implementations.

- Sustainability of Test Programs—A sustainable test program has these characteristics:

    - Customers are willing to pay a premium for a certified product;

    - Vendors are willing and motivated to pay for a thorough set of test tools and certifications; and

    - Independent test labs and test-writing organizations can make a reasonable return on investments in the standard.

The Interoperability Maturity Assessment Model, once finished and refined, could provide a unique set of tools for assessing the maturity of a Smart Grid Testing and Certification program for products conforming to a standard.

7.3. Further Development and Implementation of the Frameworks

NIST and the SGTCC are working on a number of activities to resolve related issues for supporting the interoperability testing and certification framework. These activities include the following:

- Developing ITCA evaluation processes—The SGTCC is developing processes/tools to enable testing and certification bodies to be considered as ITCAs that conform to the IPRM requirements. The processes may include establishing liaison relationships between the SGTCC and ITCAs, developing auditing process for ITCAs, and other necessary functions to support IPRM implementation.
    - This activity targets the development of guidance documents and/or assessment tools. The ITCA evaluation process is an ongoing activity, supporting ITCAs as they become ready to undergo the assessment process**.**

- Developing end-to-end or system testing methodology—End-to-end testing and/or system testing typically involves verifying the interoperability of multiple standards. The SGTCC has formed a new working group to develop an end-to-end testing approach for interoperability tests that involve multiple standards/domains. The development may start with developing use cases for such test scenarios.

    - This activity is anticipated to be ongoing through 2011 as the new working group compiles, discusses, and agrees on critical use cases that require SGIP implementation support to help achieve end-to-end interoperability.

- Performing outreach, marketing, and education—The SGTCC will make efforts in building awareness for end users, advocating that end users use IPRM conformance in their purchasing specifications.

Working Draft

  - This activity is an ongoing effort, including the development of market-facing information on testing and certification considerations, as well as SGTCC recommendations and communication with industry stakeholders on the details of these issues via workshops, white papers, and conference presentations.

- Collaborating with the Cybersecurity Working Group (CSWG) on security testing: Cybersecurity is one area that affects all Smart Grid standards and crosses all domains. The SGTCC has formed a new working group to work with CSWG in addressing cybersecurity-related testing.
  - This activity enhances the existing work products of the SGTCC to provide more targeted best practices for testing on cybersecurity issues. These enhancements are targeted for completion by end of calendar year 2011.

- Provide ongoing support to ITCAs by SGTCC members: The SGTCC plans to provide continued support to ITCAs to comply with requirements specified in the IPRM and to assist in resolving any specific issues in their implementation of the conformance and interoperability testing and certification programs.
  - This activity is ongoing, with the SGTCC supporting ITCAs as they proceed in implementing recommended practices.

- Preparing for the transition: The SGTCC is currently collaborating with the American National Standards Institute (ANSI) to support their interest in offering assessment and accreditation services based on the IPRM. Dialogue has also taken place with other organizations offering certification body and test lab accreditation services to develop their interest in offering IPRM-related services. An SGTCC working group is focused on IPRM implementation processes to support this transition to professional and independent assessments, publishing initial guidance material on the SGIP Web site, and continuing discussion with both ITCAs and accrediting organizations to better understand the tools and processes that will help accelerate implementation of these assessments.
  - This activity had been a focus during the summer of 2011 and continues.

- Prioritizing Test Program Needs: The SGTCC is focused on identifying gaps in available test programs associated with the NIST list of priority standards for Smart Grid interoperability. Through stakeholder input, the SGTCC will endeavor to develop a set of priority program needs, and will support and help facilitate the establishment of industry programs that address the identified gaps.
  - This activity will be a focus area during 2011-2012.

The SGIP's SGTCC has made significant progress in its first year of activity, establishing the basic infrastructure of a testing and certification framework in accordance with the goals of Phase III of the NIST plan in accelerating interoperable Smart Grid standards. The SGTCC is transitioning towards support of the implementation activities associated with the framework. The success of broader industry implementation of testing and certification programs will require industry recognition and acceptance of the value of these programs, active stakeholder

Working Draft

participation in demonstrating interoperability through test programs, and the integration by end users of these test programs to support their technology selection and deployment initiatives.

Developing and implementing a framework for testing and certification of Smart Grid interoperability standards is a long-term process. NIST plans to continue working with SGIP, the SGTCC, and industry stakeholders in refining the framework and providing necessary support for its implementation.

Working Draft

8. Next Steps

The execution of the Priority Action Plans presently under way will continue until their objectives to fill identified gaps in the standards portfolio have been accomplished. As new gaps and requirements are identified, the SGIP will continue to initiate Priority Action Plans to address them. NIST and the SGIP will work with SSOs and other stakeholders to fill the gaps and improve the standards that form the foundation of the Smart Grid.

Work on the SGIP Catalog of Standards will continue to fully populate the Catalog and ensure robust architectural and cybersecurity reviews of the standards. The cybersecurity guidelines will be kept up to date to stay ahead of emerging new threats. Efforts will continue to partner with the private sector as it establishes testing and certification programs consistent with the SGIP testing and certification framework. Work will continue to coordinate with related international Smart Grid standards efforts to maintain U.S. leadership.

Many of the Department of Energy (DOE) Smart Grid Investment Grants will come to fruition in the near future. Principal investigators were required to include in their proposals a description of how the projects would support the NIST Framework. As the experiences with new Smart Grid technologies are gained from these projects, NIST will use these ”lessons learned” to further identify the gaps and shortcomings of applicable standards.

NIST will continue to support the needs of regulators as they address standardization matters in the regulatory arena. Under EISA, the Federal Energy Regulatory Commission (FERC) is charged with instituting rulemaking proceedings to adopt the standards and protocols as may be necessary to ensure Smart Grid functionality and interoperability once, in FERC's judgment, the NIST-coordinated process has led to sufficient consensus.[128] FERC obtained public input through two Technical Conferences on Smart Grid Interoperability Standards in November 2010 and January 2011,[129] and through a supplemental notice requesting comments in February 2011.[130] As a result, FERC issued an order in July 2011[131] stating that there was insufficient consensus for it to institute a rulemaking at that time to adopt the initial five families of standards identified by NIST as ready for consideration by regulators.[132]

In that July 2011 order, however, FERC expressed support for the NIST interoperability framework process, including the work done by the SGIP, for development of Smart Grid interoperability standards. The Commission's order stated that the NIST Framework is comprehensive and represents the best vehicle for developing standards for the Smart Grid.

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

[129] http://ferc.gov/EventCalendar/EventDetails.aspx?ID=5571&CalType=%20&CalendarID=116&Date=01/31/2011&View=Listview.

[130] http://ferc.gov/EventCalendar/Files/20110228084004-supplemental-notice.pdf.

[131] http://www.ferc.gov/EventCalendar/Files/20110719143912-RM11-2-000.pdf.

[132] These standards include IEC 61850, 61970, 61968, 60870-6, and 62351. To find more information about these standards, see Table 4-1 in Section 4.3.

Working Draft

FERC's order also encourages stakeholders to actively participate and look to the NIST-coordinated process for guidance on Smart Grid standards. NIST supported the Commission's order, which notes that "In its comments, NIST suggests that the Commission could send appropriate signals to the marketplace by recommending use of the NIST Framework without mandating compliance with particular standards. NIST adds that it would be impractical and unnecessary for the Commission to adopt individual interoperability standards."[133]

Although the NIST framework and roadmap effort is the product of federal legislation, broad engagement of Smart Grid stakeholders at the state and local levels is essential to ensure the consistent voluntary application of the standards being developed. Currently, many states and their utility commissions are pursuing Smart Grid-related projects. Ultimately, state and local projects will converge into fully functioning elements of the Smart Grid "system of systems." Therefore, the interoperability and cybersecurity standards developed under the NIST framework and roadmap must support the role of the states in modernizing the nation's electric grid. The NIST framework can provide a valuable input to regulators as they consider the prudency of investments proposed by utilities.

A key objective of the NIST work is to create a self-sustaining, ongoing standards process that supports continuous innovation as grid modernization continues in the decades to come.[134] NIST envisions that the processes being put in place by the SGIP, as they mature, will provide the mechanism to evolve the Smart Grid standards framework as new requirements and technologies emerge. The SGIP processes will also evolve and improve as experience is gained.

8.1. Additional Issues to be Addressed

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

8.1.1. Electromagnetic Disturbances and Interference

The foundation for the new Smart Grid is built on increasingly sophisticated sensing and control of all aspects of the grid. The expected rise in the use of distributed renewable energy sources, plug-in electric vehicles and smart appliances in the home, wired and wireless communications, and other "smart" systems throughout the grid, along with the increasing electromagnetic sources in the general environment, will result in unprecedented exposure to possible electromagnetic disturbances and interference. These "smart" systems are being deployed throughout the power grid in locations ranging from single-family homes to complex industrial facilities. These environments will require a broad array of measures to protect the grid and other electronic systems from interference.

The possible interference phenomena include common events such as switching and fast transients, electrostatic discharge, lightning bursts, radio frequency interference, as well as

[133] See reference http://www.ferc.gov/EventCalendar/Files/20110719143912-RM11-2-000.pdf, p. 6.

[134] As part of this process, the SGIP will help to prioritize and coordinate Smart Grid-related standards. See Chapter 5 for further discussion.

Working Draft

infrequent, but potentially catastrophic, events such as severe geomagnetic storms and Intentional Electromagnetic Interference (IEMI) threats from a range of narrowband and broadband sources, with interference both conducted or radiated. Intense electromagnetic fields can be generated by a repeatable (non-explosive) high-power generator, which are directed to the target by an antenna, or High-Altitude Electromagnetic Pulse (HEMP). The Congressional Electromagnetic Pulse (EMP) Commission has `documented some of the more severe electromagnetic-disturbance-based risks and threats to critical U.S. national infrastructures, including the electric power grid upon which other infrastructures depend.[135] These threats and their potential impacts provide impetus to evaluate, prioritize, and protect/harden the new Smart Grid.

The possible interference phenomena include common events such as switching and fast transients, electrostatic discharge, lightning bursts, and conducted or radiated radio frequency interference. Another concern is interference or damage from possible high-power electromagnetic events such as Intentional Electromagnetic Interference (IEMI) from a range of narrowband and broadband sources, with interference both conducted or radiated. Intense electromagnetic fields can be generated by a repeatable (non-explosive) high-power generator, which are directed to the target by an antenna,[136] or from criminal or terrorist activities,[137] as well as infrequent, but potentially catastrophic, severe geomagnetic disturbances initiated by solar activity [138, 139] and threats such as High-Altitude Electromagnetic Pulse (HEMP). The Congressional Electromagnetic Pulse (EMP) Commission has documented some of the more severe electromagnetic-disturbance-based risks and threats to critical U.S. national infrastructures, including the electric power grid upon which other infrastructures depend.[140] These threats and their potential impacts provide impetus to evaluate, prioritize, and protect/harden the new Smart Grid.

The term "electromagnetic compatibility" (EMC) describes the ability to withstand electromagnetic interference and function properly in a given environment. EMC within the Smart Grid systems and in the external environment, along with immunity to serious natural and man-made threats, must be systematically addressed for reliable operation of the Smart Grid. Also, immunity to interference, coexistence with other devices, and fault tolerance should be

Working Draft

[135] http://www.empcommission.org/.

[136] http://www.futurescience.com/emp/ferc_Meta-R-323.pdf.

[137] Radasky, W.A., Baum, C.E. and Wik, M.W., "Introduction to the Special Issue on High-Power Electromagnetics (HPEM) and Intentional Electromagnetic Interference (IEMI)", IEEE Transactions on Electromagnetic Compatibility, Vol. 46, No. 3, August 2004.

[138] Kappenman, J. G. and Radasky W. A., "Too Important to Fail: The Looming Threats of Large Geomagnetic Storms and Other High-Altitude Disturbances with Modern Electric Power Grids May Produce Significant Damage to Critical Infrastructure," Space Weather Journal, 18 May 2005. http://www.agu.org/journals/sw/swa/feature/article/?id=2005SW000152

[139] Radasky, W. A. and Kappenman, J. G., "Impacts of Geomagnetic Storms on EHV and UHV Power Grids," 2010 Asia-Pacific International Symposium on Electromagnetic Compatibility, April 12 - 16, 2010, Beijing, China.

[140] See footnote 135

considered early in the design of Smart Grid systems to avoid costly remedies and redesigns after the systems are widely deployed.

Standards and testing criteria for electromagnetic compatibility, coexistence, and immunity to serious electromagnetic disturbances should be specified as appropriate for components and systems in the Smart Grid. Because the Smart Grid components are so diverse, there is not a one-size-fits-all solution. Therefore, a range of standards or recommendations specific to particular environments or devices is anticipated. The criteria for smart appliances in the home will be quite different from systems located in substations or industrial facilities. Many of the EMC specifications and requirements already exist in various standards. The task ahead is to identify appropriate existing standards that are, or should be, applied to the Smart Grid and to identify potential areas that need standards development.

The Smart Grid Interoperability Panel (SGIP) has recognized this situation and chartered a Domain Expert Working Group (DEWG) to “investigate enhancing the immunity of Smart Grid devices and systems to the detrimental effects of natural and man-made electromagnetic interference, both radiated and conducted. The focus is to address these EMC issues and to develop recommendations for the application of standards and testing criteria to ensure EMC for the Smart Grid, with a particular focus on issues directly related to interoperability of Smart Grid devices and systems, including impacts, avoidance, generation, and mitigation of and immunity to electromagnetic interference.” (Electromagnetic Interoperability Issues Working Group (EMII WG) Charter[141]). The primary goal of the working group is to identify and focus on the critical parts of the Smart Grid and develop a strategy to implement effective EMC, including standards, testing, and conformity assessment, with particular focus on issues directly affecting interoperability of Smart Grid devices and systems. This strategy should provide for growth and change as the Smart Grid evolves. The EMII WG’s approach will be to work with power industry and EMC experts, SDOs, and other stakeholders, in addition to the SGIP’s Priority Action Plans (PAPs) and working groups, to identify, evaluate, and/or initiate development of the appropriate EMC standards and testing criteria to ensure interoperability of the various Smart Grid devices and systems. The Home-to-Grid (H2G) DEWG has written a white paper, "Electromagnetic Compatibility (EMC) Issues for Home-to-Grid Devices, and submitted it to EMII WG, which has adopted it. [142]

8.1.2. Reliability, Implementability, and Safety of Framework Standards

Working Draft

[141] http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/ElectromagneticIssuesWG#Electromagnetic_Issues_WG_Charte.

[142] See Appendix A.3 in the EMIIWG_EMC_report_DRAFT_20Sept2011 at http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/MinutesOfEMCIIWGmeetings.

Implementability covers not only whether each proposed interoperability standard would enhance functionality of the development of Smart Grid technologies, but also the impacts on consumers. Implementability addresses the potential impacts upon the electric industry associated with implementing Smart Grid standards and protocols. It also addresses whether the standard/protocol pertains to interoperability and functionality of the implementations of these standards and protocols and whether the standard is ready to be implemented by utilities.

At a Federal Energy Regulatory Commission (FERC) Technical Conference on Smart Grid Interoperability Standards held in January 2011[143] and in subsequent filings, concerns were expressed by presenters at the meeting and in comments submitted to FERC regarding how new standards and technologies will impact the reliability and security of the national power grid. Additionally, concerns about the maturity of implementations and maturity of the underlying technologies used in a particular standard were also raised, including legacy issues. The standards information forms and posted narratives described in Chapter 4 contain some of the information regarding maturity of the standards and implementations, as well as the FERC-approved North American Energy Reliability Corporation (NERC) reliability standards that may be impacted by adoption of the standards, but formal reviews related to the reliability and implementability issues were not part of the original NIST or SGIP Catalog of Standards processes. During the evolution of the legacy grid to the Smart Grid, the introduction of new standards and technologies may pose implementation and transition challenges as well as possibly affect the reliability and safety of the grid.

The SGIP is now considering the addition of reviews for reliability, implementability, and safety considerations to the Catalog of Standards process described in Sections 4.5 and 5.3. New working groups that would conduct these reviews would analyze candidate standards for:

- Potential for unintended consequences for existing protection and control schemes, and other market or grid operational systems;
- Potential impacts of complexities introduced into the electric system and market management complexities;
- Possible reliability enhancements by utilizing the capabilities of the candidate standard; and
- Impacts of the candidate standard on the safety of the electrical grid.

In addition, depending on the existing legacy technologies and processes, there are various implementation and migration challenges present in adopting new standards and integrating their implementations with legacy technologies. Regulatory commissions, utilities, and others will consider implementation factors, such as sufficient maturity of a standard as demonstrated in standards-compliant commercially available products, effective technology transition plans to maintain reliable operations, and cost-effective deployment.

Presently the SGIP provides a means of addressing such issues, upon identification by an industry participant, by assigning resolution to an existing working group or forming a new PAP

[143] See http://ferc.gov/EventCalendar/EventDetails.aspx?ID=5571&CalType=%20&CalendarID=116&Date=01/31/2011&View=Listview.

Working Draft

to scope out the resolution. An example of this is PAP18, which was formed to address the issue of Smart Energy Profile (SEP) 1.x migration to SEP 2.0. The SGIP is now considering alternatives to this approach, such as creating a new review process within the Catalog of Standards process to assess implementation considerations and prepare guidance for each new standard proposed or included in the Catalog of Standards. This review would analyze the issues involved in implementation of new standards potentially including:

- Technology transition risks and any potential stranded equipment implications;
- Business process changes required ;
- Relative implementation maturity of the standard and related implementation consideration;
- Cost drivers that facilitate evaluation of relative cost-effectiveness of alternate solutions; and
- Applicable federal and state policy considerations related to standards implementation.

These additional reliability, implementability and safety reviews would be included in the SGIP Catalog of Standards process.

8.2. 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 continue to publish Interoperability Framework documents updates as needed. As of August 2011, three PAPs (1, 10, and 11) have completed their work, and further work has been identified by the SGIP. 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. Details about future meetings, workshops, and public comment opportunities will appear on the NIST Smart Grid Collaboration Site.[144]

Working Draft

[144] NIST Smart Grid Collaboration Site. http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/WebHome.

9. Appendix: List of Acronyms

ACSE	Association Control Service Element
AEIC	Association of Edison Illuminating Companies
AES	Advanced Encryption Standard
AMI	Advanced Metering Infrastructure
AMI-SEC	Advanced Metering Infrastructure Security
AMR	Automated Meter Reading
ANSI	American National Standards Institute
API	Application Programming Interface
ARRA	American Recovery and Reinvestment Act
AS	Australian Standard
ASHRAE	American Society of Heating, Refrigerating and Air Conditioning Engineers
ASN	Abstract Syntax Notation
ATIS	Alliance for Telecommunications Industry Solutions
B2B	Business to Business
BAN	Business Area Network
BAS	Building Automation System
BS	British Standard
CA	Contingency Analysis
CEIDS	Consortium for Electric Infrastructure to Support a Digital Society
CEMPC	Congressional EMP Commission
CIM	Common Information Model
CIGRE	International Council on Large Electric Systems
CIP	Critical Infrastructure Protection
CIS	Customer Information System

Working Draft

CM	Configuration Management
CoBIT	Control Objectives for Information and related Technology
COSEM	Companion Specific for Energy Metering
CPP	Critical Peak Pricing
CSCTG	Smart Grid Cyber Security Coordination Task Group
CSRC	Computer Security Resource Center
CSWG	Cybersecurity Working Group
CWE	Common Weakness Enumeration
DA	Distribution Automation
DALI	Digital Addressable Lighting Interface
DDNS	Dynamic Domain Name System
DER	Distributed Energy Resources
DES	Data Encryption Standard
DEWG	Domain Expert Working Group
DG	Distributed Generation
DGM	Distribution Grid Management
DHCP	Dynamic Host Configuration Protocol
DHS	Department of Homeland Security
DLC	Direct Load Control
DLMS	Device Language Message Specification
DMS	Distribution Management System
DNS	Domain Name System
DNP	Distributed Network Protocol
DOD	Department of Defense
DOE	Department of Energy
DP	Dynamic Pricing
DPG	Design Principles Group

Working Draft

DR	Demand Response
DTR	Derived Test Requirements
DWML	Digital Weather Markup Language
ECWG	Electronic Commerce Working Group
EDL	Exchange Data Language
EISA	Energy Independence and Security Act of 2007
ELMS	Electrical Lighting and Management Systems
EMCS	Utility/Energy Management and Control Systems
EMIX	Energy Market Information Exchange
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
F2F	Face to Face
FCC	Federal Communications Commission
FERC	Federal Energy Regulatory Commission
FIPS	Federal Information Processing Standards
FIXML	Financial Information Exchange Markup Language
FTP	File Transfer Protocol
GAPP	Generally Accepted Privacy Principles
GHG	Greenhouse Gases
GIC	Geomagnetically Induced Currents

Working Draft

GID	Generic Interface Definition
GIS	Geographic Information System
GML	Geography Markup Language
GOOSE	Generic Object-Oriented Substation Event
GSA	General Services Administration
GSMA	Global System for Mobile Communications Association
GWAC	GridWise Architecture Council
HAN	Home Area Network
HEMP	High-Altitude Electromagnetic Pulse
HTTP	Hypertext Transfer Protocol
HVAC	Heating, Ventilating, and Air Conditioning
IATFF	Information Assurance Technical Framework Forum
ICCP	Inter-Control Centre Communications Protocol
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
IESNA	Illumination Engineering Society of North America
IETF	Internet Engineering Task Force
IHD	In-Home Display
IKB	Interoperability Knowledge Base
IMAM	Interoperability Maturity Assessment Model
INCITS	InterNational Committee for Information Technology Standards
INL	Idaho National Labs
IOSS	Interagency OPSEC Support Staff
IP	Internet Protocol

Working Draft

IPS	Internet Protocol Suite
IPRM	Interoperability Process Reference Manual
IRM	Interface Reference Model
ISA	International Society of Automation
ISO	International Organization for Standardization
ISO	Independent Systems Operator
IT	Information Technology
ITCA	Interoperability Testing and Certification Authority
ITIL	Information Technology Infrastructure Library
ITU	International Telecommunication Union
KPI	Key Point of Interoperability
LAN	Local Area Network
LMS	Load Management System
LTC	Load Tap Changer
MAC	Medium Access Control
MDMS	Meter Data Management System
MGI	Modern Grid Initiative
MIB	Management Information Base
MIL	Military
MIME	Multipurpose Internet Mail Extensions
MFR	Multilevel Feeder Reconfiguration
MMS	Manufacturing Messaging Specification
MPLS	MultiProtocol 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

Working Draft

NERC	North American Electric Reliability Corporation
NIAP	National Information Assurance Partnership
NIPP	National Infrastructure Protection Plan
NIST	National Institute of Standards and Technology
NISTIR	NIST Interagency Report
NISTSP	NIST Special Publication
NOAA	National Oceanic and Atmospheric Administration
NOPR	Notice of Proposed Rulemaking
NRECA	National Rural Electric Administration Cooperatives Association
NSA	National Security Agency
NSM	Network and System Management
NSTIC	National Strategy for Trusted Identities in Cyberspace
OASIS	Organization for the Advancement of Structured Information Standards
OECD	Organization for Economic Cooperation and Development
OGC	Open Geospatial Consortium
OID	Object Identifier
OMB	Office of Management and Budget
OMG	Object Management Group
OMS	Outage Management System
OpenSG	Open Smart Grid
OSI	Open Systems Interconnection
OWASP	Open Web Application Security Project
PAP	Priority Action Plan
PEV	Plug-in Electric Vehicles
PDC	Phasor Data Concentrator
PHY	Physical Layer
PIA	Privacy Impact Assessment

Working Draft

PLC	Power Line Carrier
PMO	Program Management Office
PMU	Phasor Measurement Unit
PSRC	Power System Relaying Committee
PUC	Public Utility Commission
QOS	Quality of Service
RAS	Remedial Automation Schemes
RBAC	Role-Based Access Control
RFC	Request for Comments, Remote Feedback Controller
RTO	Regional Transmission Operator
RTP	Real-Time Pricing
RTU	Remote Terminal Unit
SABSA	Sherwood Applied Business Security Architecture
SAE	Society of Automotive Engineers
SAML	Security Assertion Markup Language
SCADA	Supervisory Control and Data Acquisition
SCAP	Security Content Automation Protocol
SCE	Southern California Edison
SCL	Substation Configuration Language
SCP	Secure Copy Protocol
SDO	Standards Development Organization, Standards Developing Organization
SGAC	Smart Grid Architecture Committee
SGIP	Smart Grid Interoperability Panel
SGIP-CSWG	Smart Grid Interoperability Panel - Cybersecurity Working Group
SGIPGB	Smart Grid Interoperability Panel Governing Board
SGTCC	Smart Grid Testing and Certification Committee
SHA	Secure Hash Algorithm

Working Draft

SNMP	Simple Network Management Protocol
SNTP	Simple Network Time Protocol
SOA	Service-Oriented Architecture
SOAP	Simple Object Access Protocol
SP	Special Publication
SPS	Standard Positioning Service
SSO	Standards-Setting Organization
SSH	Secure Shell
SSP	Sector-Specific Plan
TASE	Telecontrol Application Service Element
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
UDP	User Datagram Protocol
UID	Universal Identifier
UML	Unified Modeling Language
VA	Volt-Ampere
VAR	Volt-Ampere Reactive
VVWC	Voltage, VAR, and Watt Control
WAMS	Wide-Area Measurement System
WAN	Wide-Area Network
WASA	Wide-Area Situational Awareness
WG	Working Group

Working Draft

WS	Web Services
XACML	eXtensible Access Control Markup Language
XML	eXxtensible Markup Language

Working Draft

10. Appendix: Specific Domain Diagrams

10.1. Introduction

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. 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 bidirectional. 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 10-1. 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).

Working Draft

Table 10-1. Domains in the Smart Grid Conceptual Model

Domain	Description
Customer	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 sub-domain: home, commercial/building, and industrial.
Markets	The operators and participants in electricity markets.
Service Provider	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 Independent Systems Operator (ISO) or Regional Transmission Operator (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 (DMS), and in the Customer domain, such as meters. The Smart Grid Domain Diagrams are presented at two levels of increasing detail, as shown in Figure 10-1. 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.

Working Draft

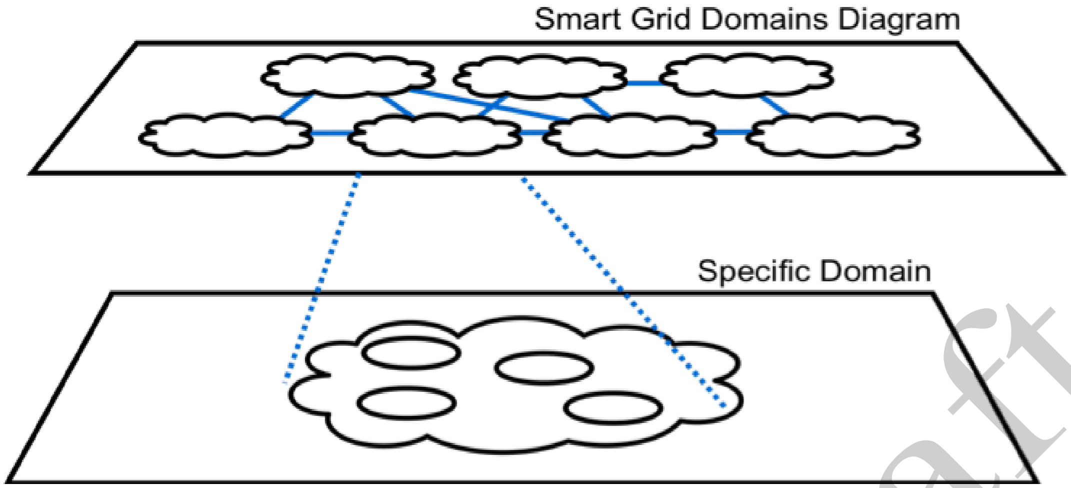


Figure 10-1. Examining the Domains in Detail

The purpose of the domain diagram 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 are achieved by stakeholder activities that are ongoing.

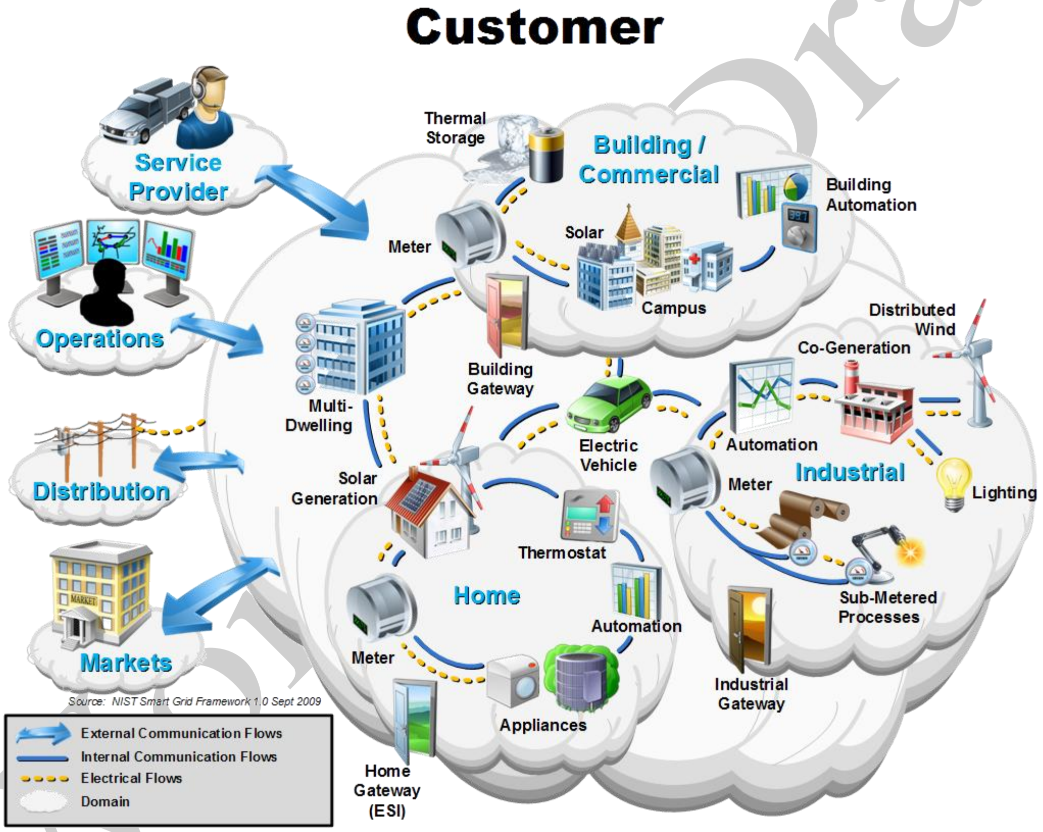
It is important to note that the domain diagram (or the conceptual model) of the Smart Grid is not limited to a single domain, single application, or single use case. For example, the use of "Smart Grid" in some discussions has been applied to only distribution automation or in other discussions to only advanced metering or demand response. 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 the Federal Energy Regulatory Commission (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.[145]

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

Working Draft

10.2. 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 10-2). 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).



Source: NIST Smart Grid Framework 1.0 Sept 2009

Figure 10-2. Overview of the Customer Domain

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 20kW of demand for Home, 20-200 kW for Commercial/Building, and over 200kW 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, which may reside in the meter, in an EMS, or outside the premises, or at an end-device. The ESI is the primary service interface to the Customer domain. The ESI may communicate with other domains via the Advanced Metering

Working Draft

Infrastructure (AMI) or via another means, such as the Internet. The ESI provides the interface to devices and systems within the customer premises, either directly or via a Home Area Network (HAN) or other Local Area Network (LAN).

There may be more than one EMS—and therefore more than one communications path—per customer. An EMS may be an 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 cybersecurity purposes. The Customer domain is electrically connected to the Distribution domain. It communicates with the Distribution, Operations, Market, and Service Provider domains.

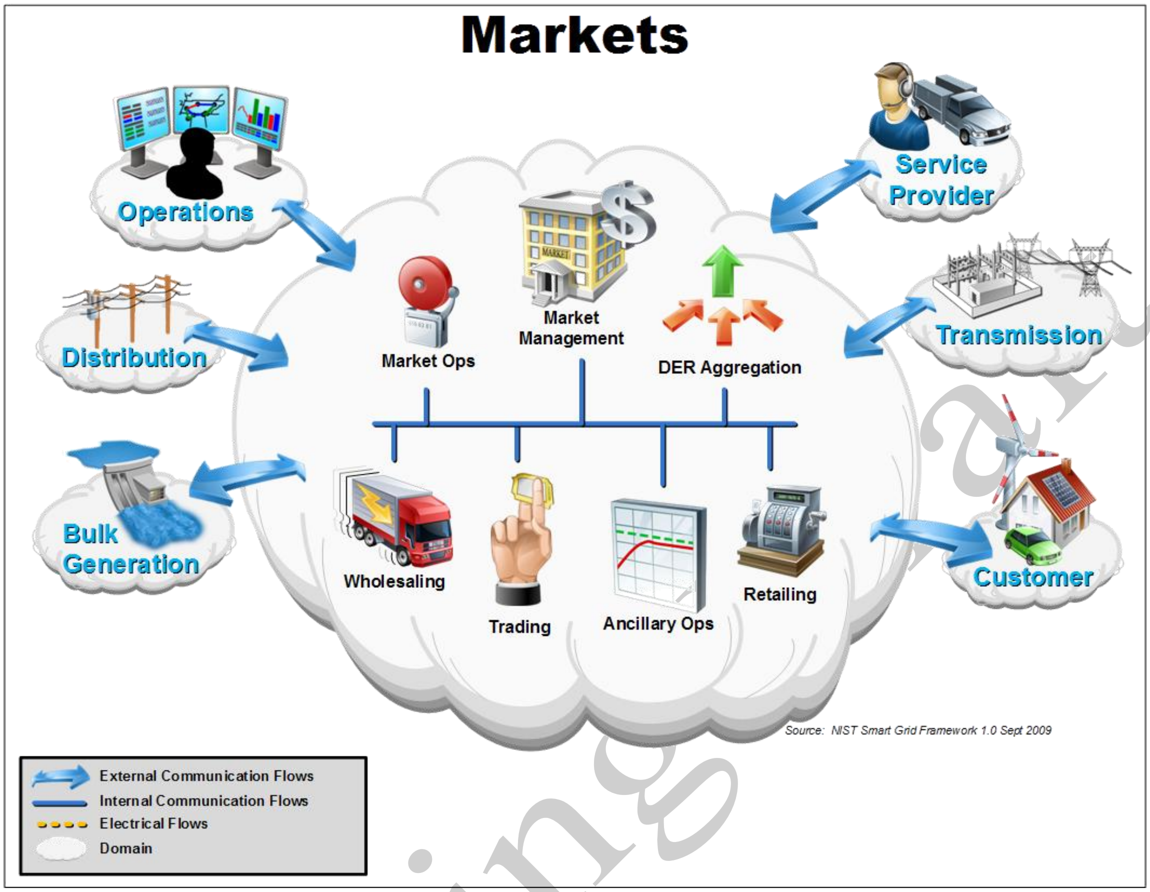
Table 10-2. Typical Application Categories in the Customer Domain

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 hydroelectric generators. Generation harnesses energy for electricity at a customer location. May be monitored, dispatched, or controlled via communications.

10.3. 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 10-3). The boundaries of the Markets domain include the edge of the Operations domain where control happens, the domains supplying assets (e.g., Generation, Transmission, etc.), and the Customer domain.

Working Draft



Source: NIST Smart Grid Framework 1.0 Sept 2009

Figure 10-3. Overview of the Markets Domain

Communication flows 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 resides in the Transmission, Distribution, and Customer domains. The North American Electric Reliability Corporation (NERC) Critical Infrastructure Protections (CIP) standards consider suppliers of more than 300 megawatts to be Bulk Generation; most DER is smaller and is typically served through aggregators. DER participates 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, traceable, and auditable. Also, these communications 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: extending price and DER signals to each of the Customer sub-domains; simplifying market rules; expanding the capabilities of aggregators; ensuring interoperability across all providers and consumers of market information; managing the growth (and regulation) of retailing and wholesaling of energy; and evolving

Working Draft

communication mechanisms for prices and energy characteristics between and throughout the Markets and Customer domains.

Table 10-3. Typical Applications in the Markets Domain

Example Application	**Description**
Market Management	Market managers include ISOs for wholesale markets or New York Mercantile Exchange (NYMEX)/ Chicago Mercantile Exchange (CME) for forward markets in many ISO/RTO regions. There are transmission, services, and demand response ma rkets 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, customers, or curtailment) to enable distributed resources to play in the larger markets.
Trading	Traders are participants in markets, which include aggregators for provision, 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	Market operations make a particular market function smoothly. Functions include financial and goods-sold clearing, price quotation streams, audit, balancing, and more.
Ancillary Operations	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 normally function on a regional or ISO basis.

Working Draft

10.4. 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 10-4). 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.

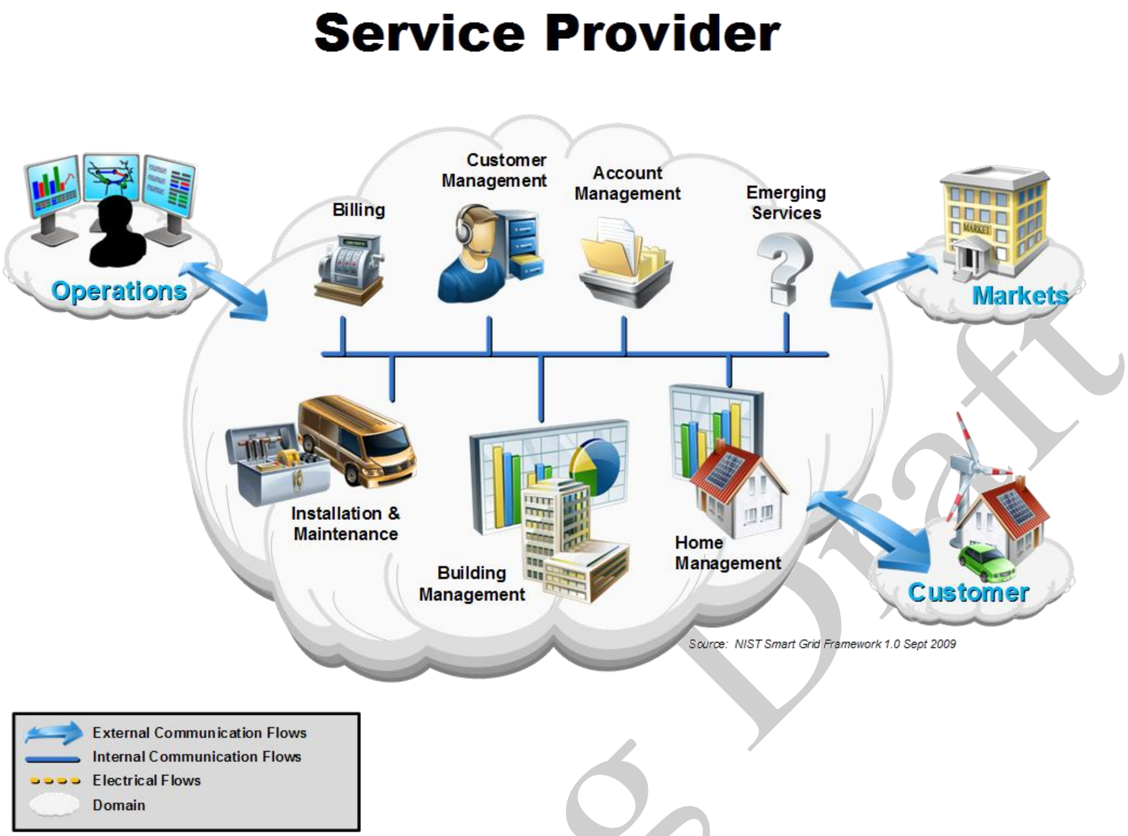


Figure 10-4. Overview of the Service Provider Domain

The service provider must not compromise the cybersecurity, 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 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

Working Draft

while maintaining consistent messaging semantics. Some benefits to the Service Provider domain from the deployment of the Smart Grid include:

- 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;
- The decrease in cost of business services for other Smart Grid domains; and
- A decrease in power consumption and an increase in power generation as customers become active participants in the power supply chain.

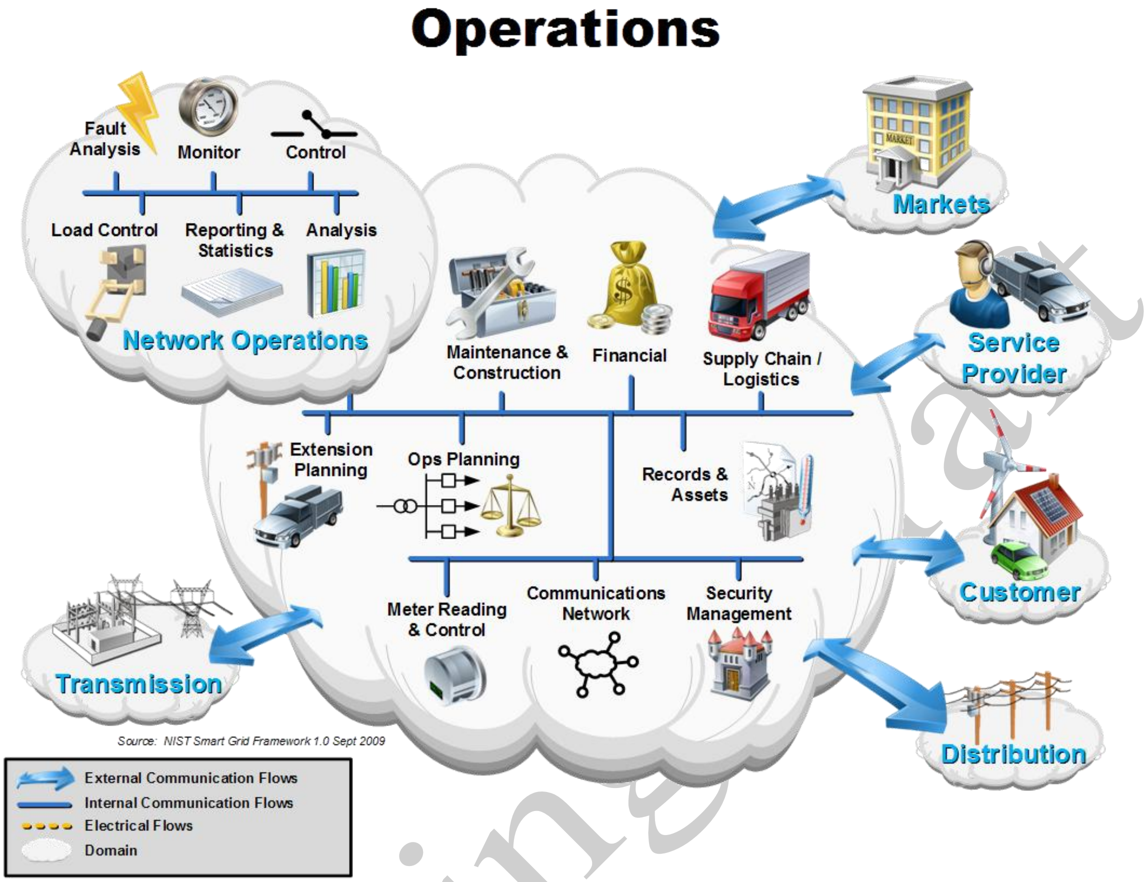
Table 10-4. Typical Applications in the Service Provider Domain

Example Application	Description
Customer Management	Managing customer relationships by providing point-of-contact and resolution for customer issues and problems.
Installation & Maintenance	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 the services and innovations that have yet to be created. These will be instrumental in defining the Smart Grid of the future.

10.5. 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 10-5). The Smart Grid will enable more of these functions 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.

Working Draft



Source: NIST Smart Grid Framework 1.0 Sept 2009

Figure 10-5. 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; 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 10-5. These applications are derived from the International Electrotechnical Commission (IEC) 61968-1 Interface Reference Model (IRM) for this domain.

Working Draft

Table 10-5. Typical Applications in the Operations Domain

Example Application	Description
Monitoring	Network Operation Monitoring actors supervise network topology, connectivity, and loading conditions, including breaker and switch states, as well as 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 the speed at which 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 online 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 (not shown) provide facilities for dispatchers that simulate the actual system they will be using.
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

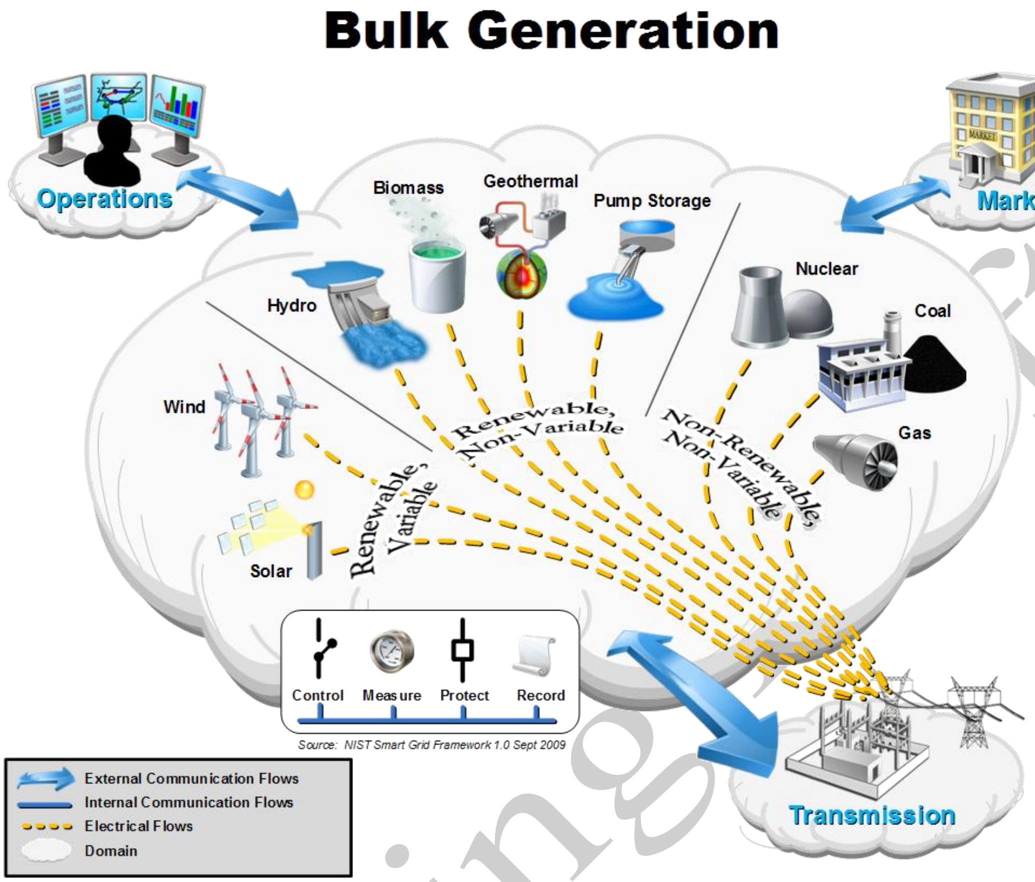
Working Draft

	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. They also relay and record customer trouble reports.

10.6. Bulk Generation Domain

Applications in the Bulk Generation domain are the first processes in the delivery of electricity to customers (see Figure 10-6). Electricity generation is the process of creating electricity from other forms of energy, which may include a wide variety of sources, including chemical combustion, 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.

Working Draft



Source: NIST Smart Grid Framework 1.0 Sept 2009

Figure 10-6. 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 solar, which are variable sources) 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 controls for greenhouse gas emissions, 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.

Working Draft

Table 10-6. Typical Applications in the Bulk Generation Domain

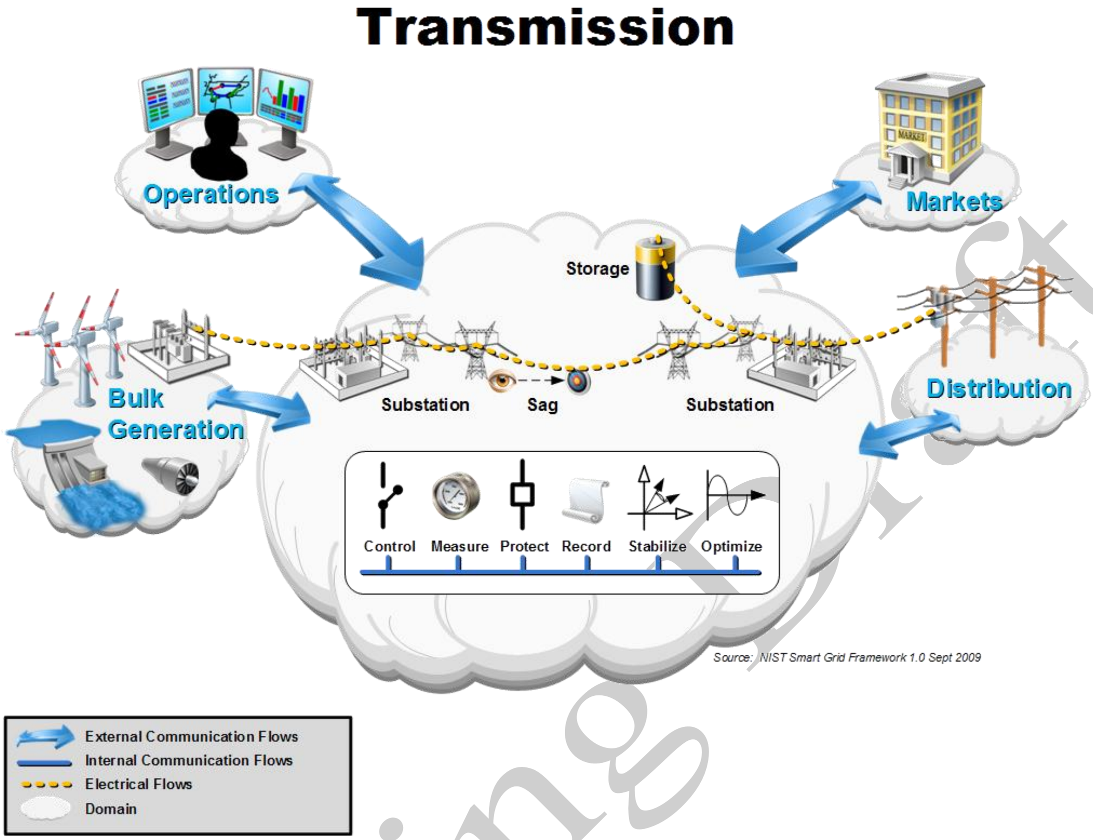
Example Application	Description
Control	Performed by actors that permit the Operations domain to manage the flow of power and reliability of the system. An example is the use of phase-angle regulators within a substation to control power flow between two adjacent power systems.
Measure	Performed by actors 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 supervisory control and data acquisition (SCADA) system from a remote terminal unit and provided 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	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.

10.7. Transmission Domain

Transmission is the bulk transfer of electrical power from generation sources to distribution through multiple substations (see Figure 10-7). 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

Working Draft

include remote terminal units, substation meters, protection relays, power quality monitors, phasor measurement units, sag monitors, fault recorders, and substation user interfaces.



Source: NIST Smart Grid Framework 1.0 Sept 2009

Figure 10-7. Overview of the Transmission Domain

Actors in the Transmission domain typically perform the applications shown in the diagram (Figure 10-7) and described in the table (Table 10-7). 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 domain and ultimately to the Customer domain.

Most activity in the Transmission domain is in a substation. An electrical substation uses transformers to step up or step down voltage across the electric supply chain. Substations also contain switching, protection, and control equipment. Figure 10-7 depicts both step-up and step down substations 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

Working Draft

monitored and controlled through a SCADA system composed of a communication network, monitoring devices, and control devices.

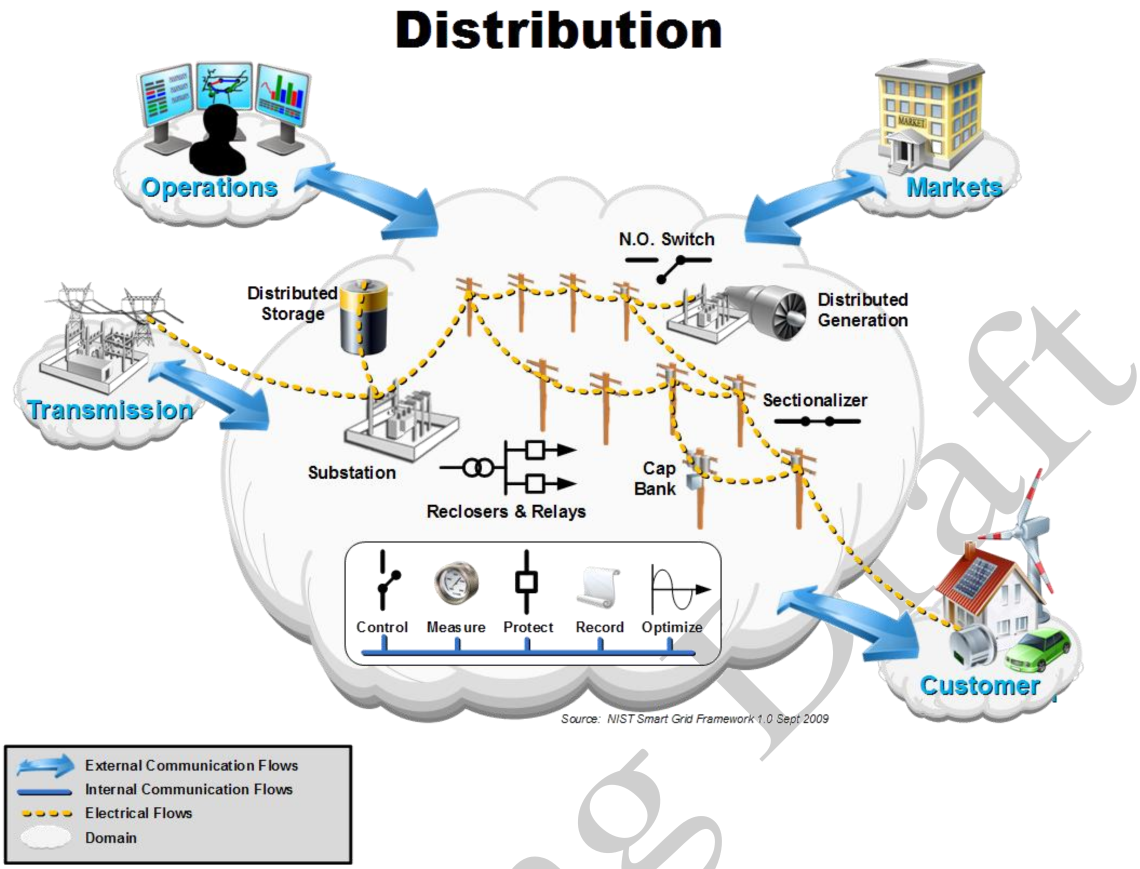
Table 10-7. Typical Applications in the Transmission Domain

Example Application	Description
Substation	The control and monitoring 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.

10.8. 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 10-8). 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.

Working Draft



Source: NIST Smart Grid Framework 1.0 Sept 2009

Figure 10-8. 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.

Working Draft

Table 10-8. Typical Applications within the Distribution Domain

Example Application	Description
Substation	The control and monitoring systems within a substation.
Storage	A system that controls the 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.

Working Draft