NIST Draft Publication

NIST Framework and Roadmap for Smart Grid Interoperability Standards Release 1.0 (Draft)

Office of the National Coordinator for Smart Grid Interoperability

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

NIST Draft Publication

NIST Framework and Roadmap for Smart Grid Interoperability Standards Release 1.0 (Draft)

Office of the National Coordinator for Smart Grid Interoperability

September 2009

U.S. Department of Commerce
Gary Locke, Secretary

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

Table of Contents

Executive Summary 5
1 Purpose and Scope 8
1.1 Overview and Background 8
1.2 How This Report Was Produced 9
1.3 Key Concepts 11
1.3.1 Definitions 11
1.3.2 Applications and Requirements: Eight Priority Areas 12
1.4 Content Overview 13
2 Smart Grid Vision 15
2.1 Overview 15
2.2 Importance to National Energy Policy Goals 17
2.3 Key Attributes 19
2.3.1 Mature Requirements 19
2.3.2 Defined Architectures 19
2.3.3 Different Layers of Interoperability 20
2.3.4 Standards and Conformance 21
3 Conceptual Reference Model 23
3.1 Overview 23
3.2 Description of Conceptual Model 24
3.3 Models for Smart Grid Information Networks 26
3.3.1 Information Networks 26
3.3.2 Security for Smart Grid information networks 28
3.3.3 IP-Based Networks 29
3.3.4 Smart Grid and the Public Internet – Security Concerns 29
3.3.5 Technologies for Smart Grid Communication Infrastructure 30
3.4 Use Case Overview 30
4 Standards Identified for Implementation 32
4.1 Overview of the Process 32
4.2 List of Standards After Initial Comments 32
4.3 Standards for Further Consideration 38

5 Priority Action Plans 48
5.1 Overview 48
5.2 Develop Common Specification for Price and Product Definition 49
5.3 Develop Common Scheduling Mechanism for Energy Transactions 51
5.4 Develop Common Information Model (CIM) for Distribution Grid Management 52
5.5 Standard Demand Response Signals 54
5.6 Standards for Energy Usage Information 56
5.7 IEC 61850 Objects/DNP3 Mapping 57
5.8 Time Synchronization 59
5.9 Transmission and Distribution Power Systems Model Mapping 61
5.10 Guidelines for the Use of IP Protocol Suite in the Smart Grid 63
5.11 Guidelines for the Use of Wireless Communications 65
5.12 Energy Storage Interconnection Guidelines 66
5.13 Interoperability Standards to Support Plug-in Electric Vehicles 69
5.14 Standard Meter Data Profiles 71
6 Cyber Security Risk Management Framework and Strategy 73
6.1 Overview 73
6.2 Cyber Security and Critical Infrastructure 73
6.3 Scope, Risks, and Definitions 74
6.4 Smart Grid Cyber Security Strategy 75
6.5 Time Line and Deliverables 79
7 Next Steps 80
7.1 Phase 2 – Smart Grid Interoperability Panel 80
7.2 Smart Grid Conformity Testing 80
7.3 Other Issues that Must be Addressed 81
7.3.1 Affordability and Availability of Standards and Design Information 81
7.3.2 Electromagnetic Disturbances 82
7.3.3 Electromagnetic Interference 83
7.3.4 Privacy Issues in the Smart Grid 83
7.3.5 Safety 85
8 List of Acronyms 86

Executive Summary

Background

Under the Energy Independence and Security Act (EISA) of 2007, the National Institute of Standards and Technology (NIST) is assigned "primary responsibility to coordinate development of a framework that includes protocols and model standards for information management to achieve interoperability of Smart Grid devices and systems…" [EISA Title XIII, Section 1305]. There is an urgent need to establish these standards. Deployment of various Smart Grid elements, such as smart meters, is already underway and will be accelerated as a result of Department of Energy (DOE) Investment Grants. Without standards, there is the potential for these investments to become prematurely obsolete or to be implemented without necessary measures to ensure security.

Recognizing the urgency, NIST developed a three-phase plan to accelerate the identification of standards while establishing a robust framework for the longer-term evolution of the standards and establishment of testing and certification procedures. In May 2009, U.S. Secretary of Commerce Gary Locke and U.S. Secretary of Energy Steven Chu chaired a meeting of nearly 70 executives from the power, information technology, and other industries at which they expressed their organizations' commitment to support NIST's plan.

This report is the output of Phase 1. It describes a high-level reference model for the Smart Grid, identifies nearly 80 existing standards that can be used now to support Smart Grid development, identifies 14 high priority gaps, plus cyber security, for which new or revised standards are needed, documents action plans with aggressive timelines by which designated Standards Development Organizations are tasked to fill these gaps, and describes the strategy being pursued to establish standards for ensuring cyber security of the Smart Grid.

Input to this report was provided through three public workshops, in April, May and August 2009, in which more than 1500 individuals representing hundreds of organizations participated. It is being released for public review and comment prior to finalization in the fourth quarter of 2009.

Summary of Key Elements Included in the Report

Smart Grid Conceptual Reference Model

The Smart Grid is a very complex system of systems. There needs to be a shared understanding of its major building blocks and how they inter-relate (an architectural reference model) in order to analyze use cases, identify interfaces for which interoperability standards are needed, and to develop a cyber security strategy. The NIST Smart Grid Conceptual Reference Model identifies seven domains (bulk generation, transmission, distribution, markets, operations, service provider, and customer) and major actors and applications within each. The reference model also identifies interfaces among domains and actors and applications over which information must be exchanged and for which interoperability standards are needed. The Smart Grid Conceptual Reference Model described in this report will be further developed and maintained by a Smart Grid Architecture Board, to be established as a subcommittee of the Smart Grid Interoperability Panel (the Panel being established by NIST).

Priorities for Standardization

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 standards needed to address the priorities identified in the Federal Energy Regulatory Commission (FERC) Policy Statement plus four additional items representing cross-cutting needs or major areas of near-term investment by utilities. The priority areas are:

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

Standards Identified for Implementation

In April 2009 NIST identified 16 initial standards for the Smart Grid for which it believed there was strong stakeholder consensus. As a result of public comments on this list and subsequent analysis, this list has now been expanded to 31 standards. An additional 46 standards were also identified as potentially applicable to the Smart Grid through the workshop process; however NIST seeks further public comment on these additional standards before deciding on their inclusion in the final version of this document.

Priority Action Plans

Through the NIST workshops, it was determined that many of the standards noted above require revision or enhancement to satisfactorily address Smart Grid requirements. In addition, gaps requiring new standards to be developed were identified. A total of 70 gaps and issues were identified. Of these, NIST selected 14 for which resolution is most urgently needed to support one or more of the Smart Grid priority areas. For each, an action plan has been developed, specific organizations tasked, and aggressive milestones in 2009 or early 2010 established. One action plan has already been completed. The Priority Action Plans and targets for completion are:

- Smart meter upgradeability standard (completed)
- Common specification for price and product definition (early 2010)
- Common scheduling mechanism for energy transactions (year-end 2009)
- Common information model for distribution grid management (year-end 2010)
- Standard demand response signals (January 2010)
- Standard for energy use information (January 2010)
- IEC 61850 Objects / DNP3 Mapping (2010)
- Time synchronization (mid-2010)

- Transmission and distribution power systems models mapping (year-end 2010)
- Guidelines for use of IP protocol suite in the Smart Grid (mid-year 2010)
- Guidelines for use of wireless communications in the Smart Grid (mid-year 2010)
- Electric storage interconnection guidelines (mid-2010)
- Interoperability standards to support plug-in electric vehicles (December 2010)
- Standard meter data profiles (year-end 2010)

Cyber Security

Ensuring cyber security of the Smart Grid is a critical priority. To achieve this requires that security be designed in at the architectural level. A NIST-led Cyber Security Coordination Task Group consisting of more than 200 participants from the private and public sectors is leading the development of a cyber security strategy and requirements for the Smart Grid. The task group is identifying use cases with cyber security considerations, performing a risk assessment including assessing vulnerabilities, threats and impacts, developing a security architecture linked to the Smart Grid conceptual reference model, and documenting and tailoring security requirements to provide adequate protection. Results of the task group’s work to date are in a companion 240 page document, NIST IR 7628 (draft), which will be available soon.

The Advanced Metering Infrastructure (AMI) is a key part of the Smart Grid that has raised security concerns. These are being addressed by the Advanced Security Acceleration Project – Smart Grid. The ASAP-SG is a collaborative effort of EnerNex Corporation, multiple major North American utilities, the NIST, and the DOE, including resources from Oak Ridge National Laboratory and the Software Engineering Institute of Carnegie Mellon University. A detailed set of security requirements for the AMI are included in the companion NIST IR 7628 (draft).

Next steps

The reference model, standards, gaps and action plans described in this document provide an initial foundation for a secure, interoperable Smart Grid. However it is only the beginning of an ongoing process that is needed to create the full set of standards that will be needed and manage their evolution in response to new requirements and technologies. A public-private partnership, the Smart Grid Interoperability Panel will be established by the end of 2009 to provide a more permanent organizational structure to support the ongoing evolution of the framework.

A robust framework for testing and certification of Smart Grid devices and systems must also be established to ensure interoperability and cyber security. NIST has initiated work to plan such a framework in consultation with stakeholders and will initiate implementation steps in 2010.

1 Purpose and Scope

1.1 Overview and Background

Under the Energy Independence and Security Act (EISA) of 2007, the National Institute of Standards and Technology (NIST) is assigned "*primary responsibility to coordinate development of a framework that includes protocols and model standards for information management to achieve interoperability of smart grid devices and systems…*" [EISA Title XIII, Section 1305]

There is an urgent need to establish standards. Some Smart Grid devices, such as smart meters, are moving beyond the pilot stage into large-scale deployment. DOE investment grants will accelerate this. In the absence of standards, there is a risk that these investments will become prematurely obsolete or, worse, be implemented without adequate security measures. Lack of standards may also impede the realization of promising applications, such as smart appliances that are responsive to price and demand response signals. In early 2009, recognizing the urgency, NIST intensified and expedited efforts to accelerate progress in identifying and actively coordinating the development of the underpinning interoperability standards.

NIST Plan for Interoperability Standards

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

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

In May 2009, U.S. Secretary of Commerce Gary Locke and U.S. Secretary of Energy Steven Chu chaired a meeting of nearly 70 executives from the power, information technology, and other industries at which they expressed their organizations' commitment to support NIST's plan.

This report, *NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0* (draft for public review and comment), is an output of NIST's approach to expediting development of key standards and requirements that will enable the networked devices and systems that make up the envisioned Smart Grid to communicate and work with each other. This approach constitutes the NIST framework and is based on a three-phase plan to accelerate development and implementation of key standards essential to progress toward realizing the Smart Grid vision. (See box above.)

This report is an output of the first phase. The majority of the document is devoted to presenting the initial standards and priorities to *achieve interoperability of smart grid devices and systems.*

It contains:

- a conceptual reference model to facilitate design of an architecture for the Smart Grid overall and for its networked domains;
- an initial set of 77 identified standards for the Smart Grid;
- priorities for additional standards and revisions to existing standards necessary to resolve important gaps and to assure the interoperability, reliability, and security of Smart Grid components;
- initial steps toward a Smart Grid cyber security strategy and requirements document using a high-level risk assessment process; and
- action plans with aggressive timelines by which designated standards development organizations (SDOs) with expertise in Smart Grid domains or technology areas are tasked to fill gaps.

This document is a draft release— in an ongoing standards and harmonization process that ultimately 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. The final version of *Release 1.0*, which will be issued later in 2009, also will serve to guide the work of a Smart Grid Interoperability Panel that also is being established as part of the NIST framework for achieving end-to-end interoperability. A key component of the second phase of the NIST Plan for Interoperability Standards, the panel, which will be composed of representatives of Smart Grid stakeholders, will support NIST to identify, prioritize and address new and emerging requirements for Smart Grid interoperability and security beyond Release 1.0.

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

1.2 How This Report Was Produced

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

In addition, NIST drew on the technical contribution of domain expert working groups (DEWGs) that it established in 2008 in partnership with DOE's GridWise Architecture Council (GWAC) to provide an open, regular means of collaboration among technical experts interested in furthering the goal of Smart Grid interoperability.[1] Involving more than 350 people representing 100 different organizations, the DEWGs developed domain-specific requirements for Smart Grid functionality and interoperability, identified cyber security risks and vulnerability, and engaged in other technical, foundation-setting activities

Also, in April 2009, NIST awarded a contract to the Electric Power Research Institute, Inc. (EPRI), a private non-profit research organization to facilitate the April and May stakeholder workshops. Following the workshops, EPRI—using its technical expertise—then compiled, distilled, organized and refined stakeholder contributions, and integrated the results with previously prepared information, and produced a *Report to NIST on the Smart Grid Interoperability Standards Roadmap.*[2] Delivered to NIST in mid-June 2009, the report identified issues and proposed priorities for developing interoperability standards and conceptual reference models for a U.S. Smart Grid. The report listed more than 80 existing standards that might be applied or adapted to Smart Grid interoperability or cyber security needs, and identified more than 70 standardization gaps and issues.

The EPRI-prepared document was made available for public review and comment.[3] NIST consulted the report and evaluated the comments received as it drafted this standards roadmap. A key intermediate NIST output was a distillation of 15 priorities[4] that, in addition to the long-standing, cross-cutting requirement for cyber security, NIST proposed for immediate, focused action by standards development organizations (SDOs) and stakeholder groups. The priority action plans (PAPs) and the status of cyber-security efforts were reviewed and further developed

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

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

[3] Request for Comments on "Report to NIST on the Smart Grid Interoperability Standards Roadmap"

[4] One of these priority areas, Data Tables Common Semantic Model for Meter Data Tables, was deemed important; however, the consensus with stakeholders was to address this PAP after some of these other pressing needs have been met.

at a public workshop, held on August 3 and 4, 2009. With representatives of more than 20 standards organizations among the participants, the workshop was devoted to discussing individual SDO and stakeholder perspectives on the evolving roadmap for Smart Grid interoperability standards, reaching agreement on which organizations should resolve specific standards needs, and developing plans and setting timelines for meeting these responsibilities as described in the PAPs. Progress on the PAPs and cyber security is summarized in Chapters 5 and 6.

1.3 Key Concepts

Although it only makes up one aspect of building a Smart Grid infrastructure, the expedited development of an interoperability framework and a roadmap for underpinning standards is key to the realization of a modernized, smart electric power grid.

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

This report contributes to achieving the widely shared understanding of standards-related priorities, strengths and weaknesses of individual standards, and inter-domain functionality and cyber security requirements that are critical to realization of the Smart Grid.

1.3.1 Definitions

Several important terms appear throughout the roadmap. Definitions of some may vary among stakeholders. To facilitate clear stakeholder discourse, NIST has defined five key terms as follows:

Architecture: Philosophy and structural patterns encompassing 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.[5]

Cyber Security: The protection required to ensure confidentiality, integrity and availability of the electronic information communication systems.

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

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

no inconvenience to the user.[6] 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.[7]

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

Requirement: (1) A condition or capability needed by a user to solve a problem or achieve an objective. (2) A condition or capability that must be met or possessed by a system or system component to satisfy a contract, standard, specification, or other formally imposed documents.[8]

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.

Voluntary consensus standards are developed by organizations following formal rules. Government regulations may incorporate or reference voluntary standards.

1.3.2 Applications and Requirements: Eight Priority Areas

The Smart Grid will ultimately require hundreds of standards. Some are more urgently needed than others. To prioritize its work, NIST chose to focus on six key functionalities plus cyber security and network communications, aspects that are especially critical to ongoing and near-term deployments of Smart Grid technologies and services. Four priority applications were recommended by FERC in its policy statement:[9]

[6] 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.

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

[8] IEEE Std 610.12

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

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

- **Demand response:** Mechanisms and incentives for utilities, business 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.

- **Electric storage:** Means of storing electric power, directly or indirectly. The significant bulk electric energy storage technology available today is pumped storage hydroelectric 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.

Besides the FERC priority applications, two cross-cutting priorities—cyber security and network communications—were included, and two other priority applications—advanced metering infrastructure and distribution grid management—were added because they represent major areas of near-term investment by utilities:

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

- **Network communications:** Encompassing public and non-public networks, the Smart Grid will require implementation and maintenance of appropriate security and access controls tailored to the networking and communication requirements of different applications, actors and domains.

- **Advanced metering infrastructure (AMI):** Primary means for utilities to interact with meters at customer sites. In addition to basic meter reading, AMI systems provide two-way communications that can be used by many functions and, as authorized, by third parties to exchange information with customer devices and systems. AMI enables customer awareness of electricity pricing on a real-time (or near real-time) basis, and it can help utilities achieve necessary load reductions.

- **Distribution grid management:** Maximizing performance of feeders, transformers, and other components of networked distribution systems and integrating with transmission systems and customer operations.

1.4 Content Overview

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

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

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

Chapter 5 describes 14 “Priority Action Plans,” to address standard-related gaps and issues for which resolution is most urgently needed to support one or more of the Smart Grid priority areas. For each, an action plan has been developed, specific organizations tasked, and aggressive milestones in 2009 or early 2010 established. One—a plan to develop a smart meter upgradeability standard—already has been completed. The full set of detailed priority action plans, which are works in progress undergoing continuing development and refinement, can be reviewed on-line at the NIST Smart Grid wiki.[10]

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

The report concludes with a discussion, in Chapter 7 “Next Steps” of plans to establish a Smart Grid Interoperability Panel to deal with the ongoing evolution of the framework, plans to establish a testing and certification framework, and additional issues impacting standardization efforts and progress toward realizing a safe, secure, innovation-enabling Smart Grid.

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

2 Smart Grid Vision

2.1 Overview

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

Definitions and terminology vary somewhat. But whether called "Smart," "smart," "smarter," or even "supersmart," all notions of an advanced power grid for the 21st century hinge on adding and integrating many varieties of digital computing and communication technologies and services with the power-delivery infrastructure. Bi-directional flows of energy and two-way communication and control capabilities will enable an array of new functionalities and applications that go well beyond "smart" meters for homes and businesses. The Energy Independence and Security Act (EISA) of 2007, which directed NIST to coordinate development of this framework and roadmap, states that support for creation of a Smart Grid is the national policy. Distinguishing characteristics of the Smart Grid cited in the act include:[11]

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

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:

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

> The application of advanced digital technologies (i.e., microprocessor-based measurement and control, communications, computing, and information systems) are expected to greatly improve the reliability, security, interoperability, and efficiency of the electric grid, while reducing environmental impacts and promoting economic growth. Achieving enhanced connectivity and interoperability will require innovation, ingenuity, and different applications, systems, and devices to operate seamlessly with one another, involving the combined use of open system architecture, as an integration platform, and commonly-shared technical standards and protocols for communications and information systems. To realize smart grid capabilities, deployments must integrate a vast number of smart devices and systems**.** [12]

To monitor and assess progress of deployments in the United States, DOE is tracking activities grouped under six chief characteristics of the envisioned Smart Grid:[13]

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

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

The framework described in the EISA describe several important characteristics. They include[14]:

- that it be “flexible, uniform and technology neutral, including but not limited to technologies for managing smart grid information,”
- that it “accommodate traditional, centralized generation and transmission resources and consumer distributed resources,”
- that it be “flexible to incorporate regional and organizational differences, and technological innovations,” and
- that it “consider the use of voluntary uniform standards” that “incorporate appropriate manufacturer lead time.”

[12] 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.

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

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

2.2 Importance to National Energy Policy Goals

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

The American Recovery and Reinvestment Act of 2009 (ARRA) includes $11 billion in investments to "jump start the transformation to a bigger, better, smarter grid."[15] These investments and associated actions to modernize the nation's electricity grid will result, for example, in more than 3,000 miles of new or modernized transmission lines and 40 million "smart meters" in American homes.[16] In addition, progress toward realization of the Smart Grid will contribute to accomplishing the President's goal of putting one million plug-in hybrid vehicles on the road by 2015.[17] 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.*[18]

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 include:

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

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

[15] "The American Reinvestment and Recovery Plan—By the numbers," http://www.whitehouse.gov/assets/documents/recovery_plan_metrics_report_508.pdf.

[16] Ibid.

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

[18] 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.

primary greenhouse gas.[19] If the current power grid were just 5 percent more efficient, the resultant energy savings would be equivalent to permanently eliminating the fuel consumption and greenhouse gas emissions from 53 million cars.[20]

In its *National Assessment of Demand Response Potential*, FERC estimated the potential for peak electricity demand reductions to be equivalent to up to 20 percent of national peak demand—enough to eliminate the need to operate hundreds of back-up power plants.[21]

Anticipated Smart Grid Benefits

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

President Obama has called for a national effort to reduce, by 2020, the nation's greenhouse gas emissions to 14 percent below the 2005 level and to about 83 percent below the 2005 level by 2050. [22] Reaching these targets will require an ever-more capable Smart Grid with end-to-end interoperability.

The transition to the Smart Grid already is under way, and it is gaining momentum, spurred by ARRA investments. In late June, DOE announced that it is requesting proposals for its Smart Grid Investment Grant Program. The program will provide $3.3 billion for cost-shared grants to support manufacturing, purchasing and installation of existing Smart Grid technologies that can be deployed on a commercial scale. The DOE

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

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

[21] 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.

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

announcement instructs grant applicants that their project plans should describe their technical approach to “addressing interoperability,” including a “summary of how the project will support compatibility with NIST’s emerging Smart Grid framework for standards and protocols.”

2.3 Key Attributes

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

2.3.1 Mature Requirements

Requirements that drive and specify the functions and how they are applied are foundational to the realization of the Smart Grid. Requirements define what the Smart Grid is and does. The following are some of the key requirements:

- Industry policies and rules of governance are well-developed, mature, and can be consistently applied.
- Requirements are well-developed by domain experts and well-documented following mature systems-engineering principles.
- Requirements define support for applications and are well-developed enough to support their management and cyber security as well.

2.3.2 Defined Architectures

An architecture describes how systems and components interact. It embodies high-level principles and requirements that Smart Grid applications and systems must satisfy. An architecture enables technical and management governance and can be used to direct ongoing development work.

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

Thus, it is not the intent of this framework to describe a single architecture for the Smart Grid. Rather, it describes a conceptual reference model for discussing the characteristics, uses, behavior, and other elements of Smart Grid domains and for showing relationships among these elements. The model is a tool for identifying the standards and protocols needed to ensure interoperability and cyber security, and defining and developing architectures for systems and subsystems within the Smart Grid.

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

- Support for a broad range of technology options—legacy and new.

- Architecture artifacts include well-defined interfaces across industries external to the utility industry.
- Modern system-modeling tools and techniques are used to manage the documentation and complexity of the system.
- Architectural interfaces are well-defined. Each architectural element must be appropriate for the applications which reside within it. The architectures must support development of massively scaled, well-managed and secure networks with life-spans of 30 years or more.
- The infrastructure supports third-party products that are interoperable and can be integrated into the management and cyber security infrastructures.

Architectures must be flexible enough to incorporate evolving technologies. They also must support interfacing with legacy applications and devices in a standard way, avoiding as much additional capital investment and/or customization as possible.

2.3.3 Different Layers of Interoperability

Large, integrated, complex systems require different layers of interoperability, from a plug or wireless connection to compatible processes and procedures for participating in distributed business transactions. In developing the conceptual model described in the next chapter, the high-level categorization approach developed by the GridWise Architecture Council (GWAC) was considered.[23]

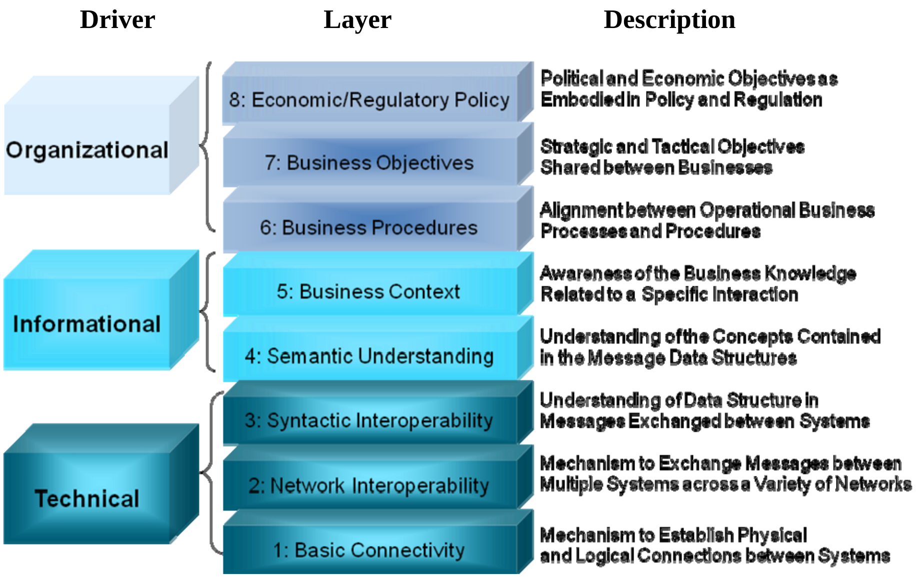

Driver
Layer
Description
Organizational
Informational
Technical
8: Economic/Regulatory Policy
7: Business Objectives
6: Business Procedures
5: Business Context
4: Semantic Understanding
3: Syntactic Interoperability
2: Network Interoperability
1: Basic Connectivity
Political and Economic Objectives as Embodied in Policy and Regulation
Strategic and Tactical Objectives Shared between Businesses
Alignment between Operational Business Processes and Procedures
Awareness of the Business Knowledge Related to a Specific Interaction
Understanding of the Concepts Contained in the Message Data Structures
Understanding of Data Structure in Messages Exchanged between Systems
Mechanism to Exchange Messages between Multiple Systems across a Variety of Networks
Mechanism to Establish Physical and Logical Connections between Systems

Figure 1. The GridWise Architecture Council's eight-layer stack provides a context for determining Smart Grid interoperability requirements and defining exchanges of information**.**

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

Referred to as the "GWAC stack," the eight layers comprise a vertical cross-section of the degrees of interoperation necessary to enable various interactions and transactions on the Smart Grid. Very simple functionality—such as the physical equipment layer and software for encoding and transmitting data—might be confined to the lowest layers. Communication protocols and applications reside on higher levels with the top levels reserved for business functionality. (This differs from the Open Systems Interconnect (OSI) model which stops at the application layer, or about layer 3 in the GWAC stack.)

As functions and capabilities increase in complexity and sophistication, more layers of the GWAC stack are required to interoperate to achieve the desired results. Each layer typically depends upon—and is enabled by—the layers below it.

The most important feature of the GWAC stack and the OSI model which preceded it is that layering defines well-known interfaces: establishing interoperability at one layer can enable flexibility at other layers. The most obvious example of this is seen in the Internet: with a common Network Interoperability layer, the Basic Connectivity Layer can vary from Ethernet to WiFi to optical and microwave links and devices can still communicate.

As shown in Figure 1and as described in the *GridWise Interoperability Context-Setting Framework*, the eight layers are divided among three "drivers," each requiring a different level of interoperability:

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

2.3.4 Standards and Conformance

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

The evidence of the essential role of standards is growing. A recent Congressional Research Service report, for example, cited the ongoing deployment of smart meters as an area in need of widely accepted standards. Ultimately, the U.S. investment in smart meters is predicted to total $40 billion to $50 billion.[24] Globally, 100 million new smart meters are predicted to be installed

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

over the next five years.[25]

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

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

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

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

3 Conceptual Reference Model

3.1 Overview

For the purpose of developing a conceptual model that supports planning and organization of what ultimately will be a collection of interconnected networks, NIST adopted the approach of dividing the Smart Grid into seven domains, as described in Table 1.

In turn, each domain—and its sub-domains—encompasses *actors* and *applications*. Actors are devices, systems, or programs that make decisions and exchange information necessary for performing applications. Examples of devices and systems include smart meters, solar panels, and control systems. Applications, on the other hand, are tasks performed by one or more actors within a domain. For example, corresponding applications may be home automation, solar energy generation and storage, and energy management. To enable Smart Grid functionality, the actors in a particular domain often interact with actors in other domains, as shown in Figure 2

Table 1. Actors in the Domains in the Smart Grid Conceptual Model

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

In general, actors in the same domain have similar objectives. However, communications within the same domain may not necessarily have similar characteristics and requirements. Actors in one domain also may interact with actors in other domains, and particular domains also may contain components of other domains. For instance, the 10 Independent System Operators (ISOs) and Regional Transmission Organizations (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.

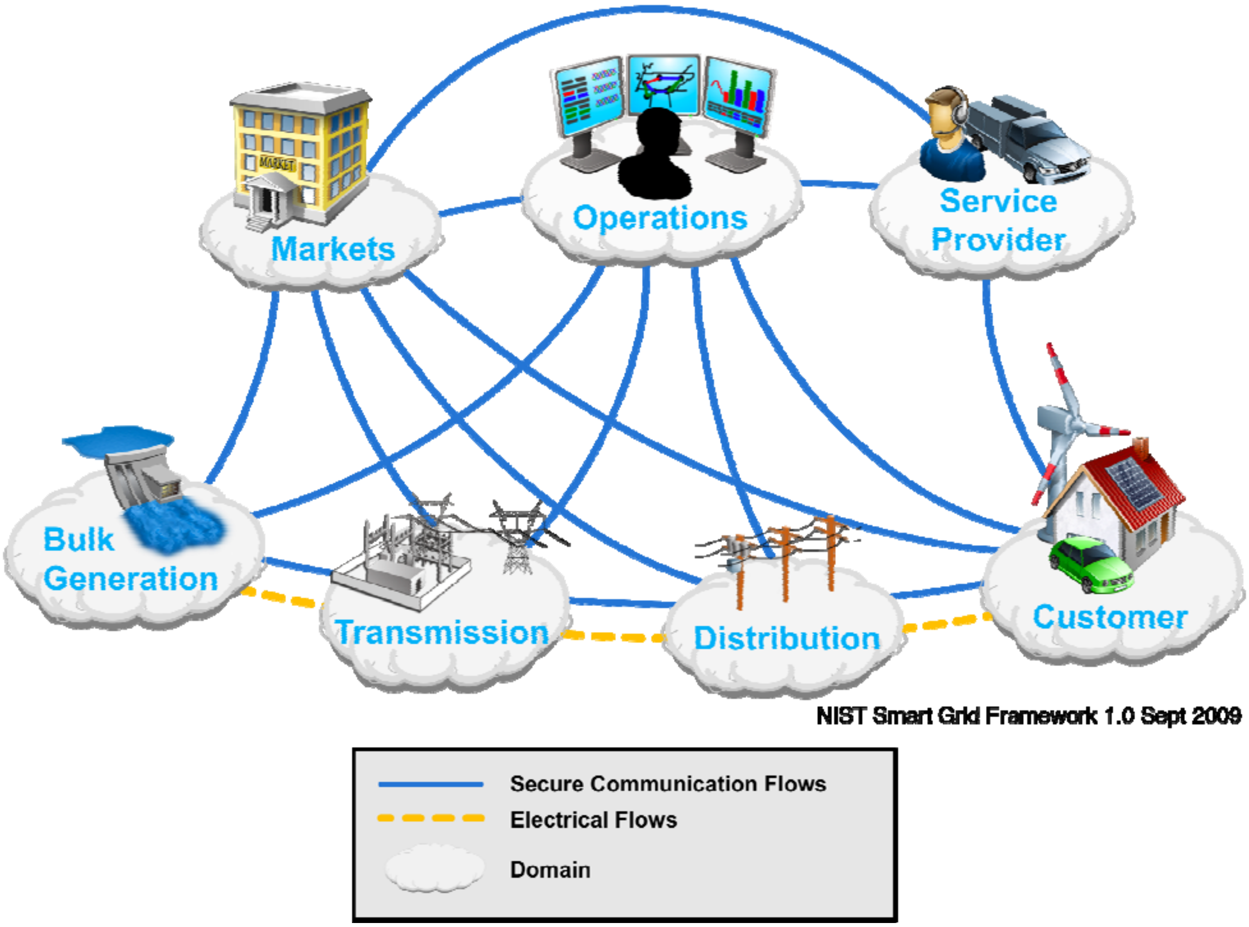
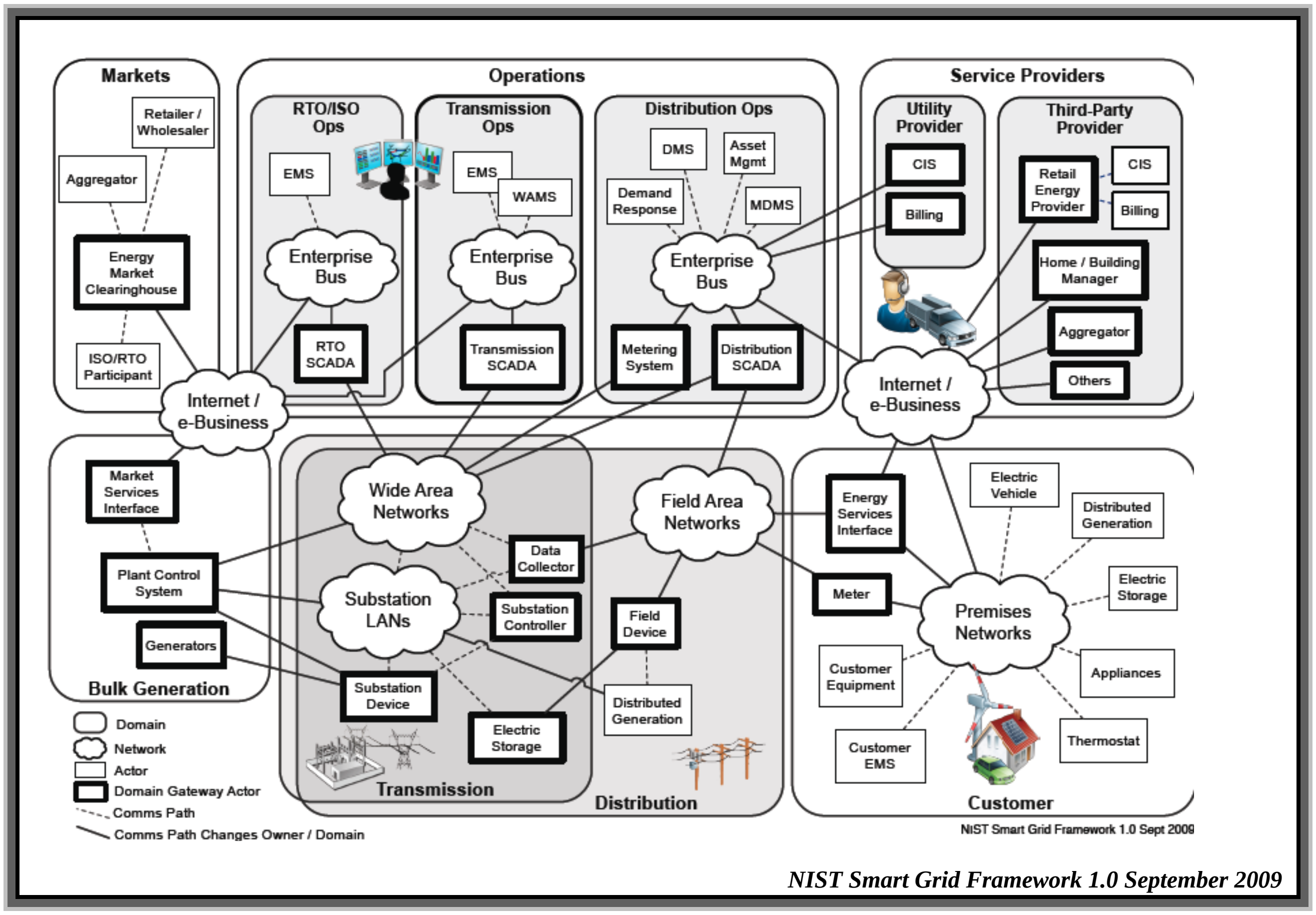


Figure 2. Smart Grid Domains

3.2 Description of Conceptual Model

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



NIST Smart Grid Framework 1.0 September 2009

Figure 3. Conceptual Reference Diagram

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

Actor: 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 the actors in the Smart Grid. Each of the actors may exist in several different varieties, and may contain many other actors within them.

Gateway Actor: An actor that interface 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, or use multiple protocols simultaneously.

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

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

3.3 Models for Smart Grid Information Networks

The conceptual reference diagram in Figure 3 shows many comunication paths between and within domains. Currently, various functions are supported by independent and, often, dedicated networks. Examples are SCADA systems, enterprise data networks, and corporate voice and video services. However, to fully realize the Smart Grid goals of vastly improving the control and management of energy generation, distribution and consumption, the current state of grid interconnectivity must be improved so that information can flow securely between the various actors in the Smart Grid. The following sections discuss some of the key outstanding issues that need to be addressed in order to support this vision.

Given that the Smart Grid will not only be a system of systems, but also a network of information networks, a thorough analysis of network and communications requirements for each subnetwork is needed. This analysis should differentiate among the requirements needed by 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, and high) of a security compromise of confidentiality, integrity and availability. This information will be used in the selection and tailoring of security requirements.

3.3.1 Information Networks

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

Figure 4 is a high-level vision for the information network for the Smart Grid. The clouds represent the networks handling two-way communications between the network end points of different domains, as represented by rectangular boxes in the figure. The domains include Generation, Transmission, Distribution, Customer, Markets, Operations, and Service Provider. Each domain is a unique distributed computing environment, and may have its own sub-network to meet the special communication requirements for the domain. This is shown in the innermost clouds in Figure 4. Within each network, a hierarchical structure consisting of network technologies, such as Home Area Networks, Personal Area Networks, Wireless Access Networks, Local Area Networks, and Wide Area Networks, may be implemented. Based on Smart Grid functional requirements the network should provide the capability to enable an application in a particular domain to communicate with an application in any other domain over the information network, with proper management control as to who and where applications can be inter-connected. Within each network and as the networks are linked together, security including the confidentiality, integrity and availability, is required to ensure the Smart Grid information and related information systems are properly protected.

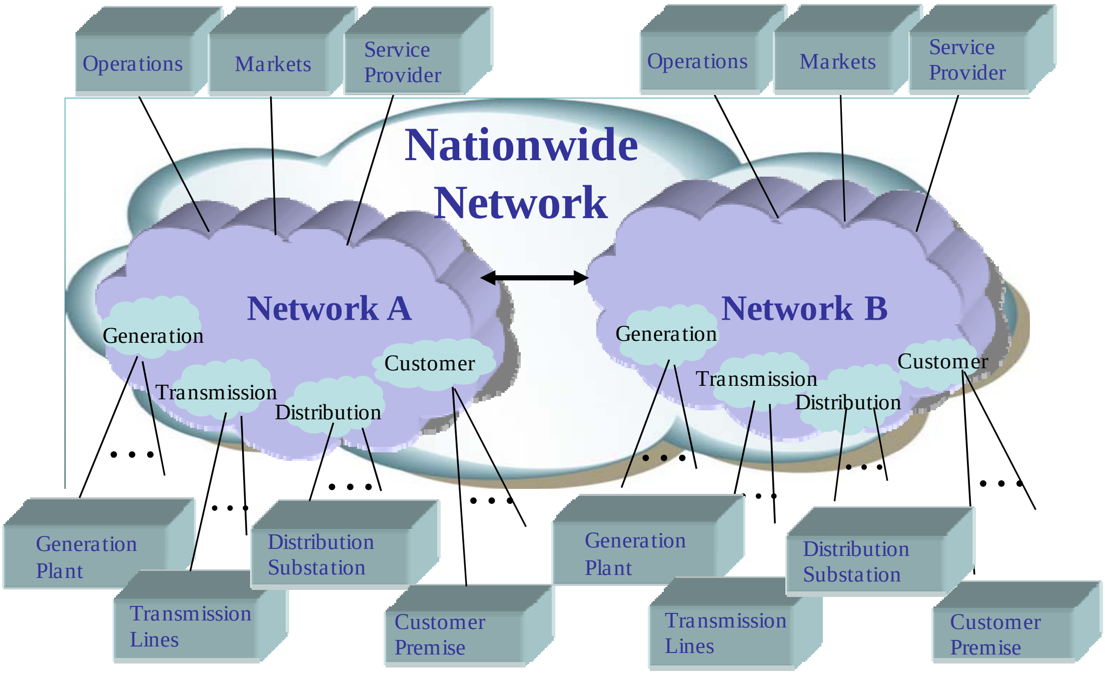


Figure 4. Smart Grid Networks for Information Exchange

Because the Smart Grid will include networks from the IT, telecommunications and electric sectors, security is required to ensure that information is protected and that a security compromise in a specific network does not result in a security compromise to other, interconnected systems. A security compromise could impact the availability and reliability of the electric sector. In addition, information within each specific system also needs to be protected. Security includes the confidentiality, integrity and availability of information. The NIST Smart Grid Cyber Security Coordination Task Group (CSCTG) is currently identifying and assessing the Smart Grid network interfaces to determine the impact of a loss of confidentiality, integrity and availability. The objective is to select countermeasures to mitigate the risk of cascading security breaches.

Devices and applications in each domain are the end points of the network. Examples of applications in the Customer domain could be a smart meter, appliance, thermostat, electric storage, electric vehicle, or distributed generation. Applications in the Transmission or Distribution domain could be a phasor measurement unit (PMU) in a transmission line substation, substation controller, electric storage, or field device. Applications in the Operations domain could be SCADA systems, computers or display systems at the operation center. The applications in the Operations, Market, and Service Provider domains are similar to typical web and business information processing. Thus, their networking function may not be distinguishable from normal information processing networks; therefore, no unique clouds are illustrated.

This information network may consist of multiple interconnected networks, represented by two backbone networks, A and B, in Figure 4. Each of these represents the network in the service region of a power utility or service. The physical or logical links within and between these networks, and the links to network end points could utilize any appropriate communication technology currently available or yet to be developed and standardized in the future. It is important to note that Figure 4 represents a vision for dedicated networks for Smart Grid control and information exchange.

Additional requirements for the information network include:

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

3.3.2 Security for Smart Grid information networks

Because Smart Grid information flows through so many different networks with different owners, it is of extreme importance to properly secure the information and the information networks. This means preventing intrusion, at the same time allowing access for the relevant stakeholders.

Security for the Smart Grid information network must include:

- security policies, procedures, protocols, and security controls to protect Smart Grid information in transit or residing in the network;
- authentication policies, procedures, mechanisms, protocols, and credentials for infrastructure components and network users;
- security policies, procedures, protocols, and security controls to protect infrastructure components and the interconnected networks;

An overview of the security strategy is included in Chapter 6 of this document.

3.3.3 IP-Based Networks

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

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

Note that the use of IP in this context refers to use of IP as a networking protocol within private networks used for communications in the Smart Grid, not use of the public Internet. Smart Grid security considerations and the public Internet are discussed further in Section 3.3.4.

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

3.3.4 Smart Grid and the Public Internet – Security Concerns

One of the advantages of the Smart Grid is the ability to better manage the consumption of energy within many domains. Many of the Smart Grid use cases describe how the utilities can work with customers to control and manage the energy consumption at home. To enable this functionality information must 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) introduces security concerns that must be addressed. With the customer having access to information at the utility, it is important to ensure that this access is separate from the utility access to the home to manage power grid operations. This can be generalized to cover any Smart Grid application that provides an interface between the Public Internet and the utility networks. These security risks are being addressed by the Cyber Security Coordination Task

Group (CSCTG). An overview of the security strategy is included in Chapter 6 of this document.

3.3.5 Technologies for Smart Grid Communication Infrastructure

There are a number of mature technologies that are available to support Smart Grid information networks. It is necessary to develop network requirements in support of Smart Grid applications in order to guide the choice of the communication technologies to be used. The following is a partial list of protocols for Smart Grid communication infrastructures that are defined by accredited standard developing organizations. In addition there may be applicable industry fora specifications, not listed here.

- Wired Networks - Wavelength Division Multiplexing (WDM) techniques, SONET /SDH fiber links, Passsive Optical Networks (PON), and Gigabit Ethernet (GbE, 10GbE), power line
- Wireless Networks – IEEE 802.15, IEEE 802.11, IEEE 802.16, 3/4G cellular

3.4 Use Case Overview

The conceptual reference models provide a useful tool in the construction of use cases. A use case describes the interaction between an actor and a system when the actor is using the system to accomplish a specified goal. Use cases can be classified as “black box” or “white box.” The black-box variety describes the user-system interaction and the functional requirements to achieve the goal, but it does not give details of the inner workings of the system. In contrast, white-box use cases also describe the internal details of the system, along with the interaction and associated requirements.

For this interoperability standards roadmap, black-box use cases were developed to describe how actors within Smart Grid systems will interact. The system requirements necessary to meet the needs of particular interactions were determined, but without specifying how the systems will implement a particular solution. These black-box use cases do not provide all details of the interactions. However, these use cases provide designers with information necessary to verify whether a particular implementation meets the needs of users, while providing designers with the flexibility to be innovative when crafting solutions.

Individually and collectively, use cases are helpful when scoping out interoperability needs in specific areas of functionality—such as on-premises energy management—and grid capability—such as predictive maintenance. 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.

Many Smart Grid intra- and inter-domain use cases already have been developed, and the number will grow substantially. The scope of the body of existing use cases also cover cross-cutting requirements, including cyber security, network management, data management, and application integration, as described in the *GridWise Architecture Council Interoperability Context-Setting Framework.*[26]

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

The detailed use cases can be found on the NIST Smart Grid wiki.[27]

[26] Document can be found at http://www.gridwiseac.org/pdfs/interopframework_v1_1.pdf

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

4 Standards Identified for Implementation

4.1 Overview of the Process

During the first phase of its three-phase plan for Smart Grid interoperability, NIST's approach to accelerating the availability of standards was to (1) identify existing standards that could be applied to meet Smart Grid needs; and (2) identify gaps and establish priorities and action plans to develop additional needed standards to fill the gaps.

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

The 16 specifications were submitted for public review and comment. In a notice published in the *Federal Register*, [28] NIST advised that the list was neither complete, nor exclusionary. Other existing standards, it said, "have not been eliminated from consideration, [and] standards that currently appear on the list ultimately may not be included." [29] In all, NIST received comments from 97 individuals and organizations on the 16 standards and specifications. The majority of the comments were positive, and several additional standards were recommended for inclusion on the initial list.

NIST reviewed all comments submitted in response to its notice in the Federal Register as well as other inputs received during its many interactions with stakeholders.

4.2 List of Standards After Initial Comments

Table 2 lists the standards identified by NIST at the conclusion of this process. The list includes the initial 16 specifications, plus 15 standards (which are shaded in Table 2) that NIST added after reviewing and evaluating the inputs it received.

Table 2. Standards Identified by NIST.

	Standard	Application
1	AMI-SEC System Security Requirements http://osgug.ucaiug.org/utilisec/amisec/Shared%20Documents/1.%20System%20Security%20Requirements/AMI%20System%20Security%20Requirements%20-%20v1_01%20-%20Final.doc	Advanced metering infrastructure (AMI) and SG end-to-end security

[28] 74 FR 27288, June 9, 2009.

.

[29] Ibid. p. 27288.

	Standard	Application
2	ANSI C12.19/MC1219 http://webstore.ansi.org/RecordDetail.aspx?sku=ANSI+C12.19-2008	Revenue metering information model
3	BACnet ANSI ASHRAE 135-2008/ISO 16484-5 http://resourcecenter.ashrae.org/store/ashrae/newstore.cgi?itemid=30853&view=item&page=1&loginid=39839941&priority=none&words=135-2008&method=and&	Building automation
4	DNP3 http://www.dnp.org/About/Default.aspx	Substation and feeder device automation
5	IEC 60870-6 / TASE.2 http://webstore.iec.ch/webstore/webstore.nsf/artnum/034806	Inter-control center communications
6	IEC 61850 http://webstore.iec.ch/webstore/webstore.nsf/artnum/033549!opendocument	Substation automation and protection
7	IEC 61968/61970 http://webstore.iec.ch/webstore/webstore.nsf/artnum/031109!opendocument http://webstore.iec.ch/webstore/webstore.nsf/artnum/035316!opendocument	Application level energy management system interfaces
8	IEC 62351 Parts 1-8 http://webstore.iec.ch/webstore/webstore.nsf/artnum/037996!opendocument	Information security for power system control operations
9	IEEE C37.118 https://sbwsweb.ieee.org/ecustomercme_enu/start.swe?SWECmd=GotoView&SWEView=Catalog+View+(eSales)_Standards_IEEE&mem_type=Customer&SWEHo=sbwsweb.ieee.org&SWETS=1192713657	Phasor measurement unit (PMU)communications
10	IEEE 1547 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	Physical and electrical interconnections between utility and distributed generation (DG)
11	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	Security for intelligent electronic devices (IEDs)
12	NERC CIP 002-009 http://www.nerc.com/page.php?cid=2|20	Cyber security standards for the bulk power system

	Standard	**Application**
13	NIST Special Publication (SP) 800-53, NIST SP 800-82 http://csrc.nist.gov/publications/drafts/800-82/draft_sp800-82-fpd.pdf	Cyber security standards and guidelines for federal information systems, including those for the bulk power system
14	Open Automated Demand Response (Open ADR) http://openadr.lbl.gov/pdf/cec-500-2009-063.pdf	Price responsive and direct load control
15	OpenHAN http://osgug.ucaiug.org/utilityami/openhan/HAN%20Requirements/Forms/AllItems.aspx	Home Area Network device communication, measurement, and control
16	ZigBee/HomePlug Smart Energy Profile http://www.zigbee.org/Products/TechnicalDocumentsDownload/tabid/237/Default.aspx	Home Area Network (HAN) Device Communications and Information Model
17	AEIC Guidelines v2.0	Utility-generated 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.
18	ANSI C12 Suite :	
	ANSI C12.1 ht-tp://webstore.ansi.org/RecordDetail.aspx?sku=ANSI+C12.1-2008	Performance and safety type tests for revenue meters
	ANSI C12.18/IEEE P1701/MC1218 http://webstore.ansi.org/FindStandards.aspx?SearchString=c12.18&SearchOption=0&PageNum=0&SearchTermsArray=null|c12.18|null	Protocol and optical interface for measurement devices
	ANSI C12.20 http://webstore.ansi.org/FindStandards.aspx?SearchString=c12.20&SearchOption=0&PageNum=0&SearchTermsArray=null|c12.20|null	Revenue metering accuracy specification and type tests
	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

	Standard	Application
	ANSI C12.22-2008/IEEE P1703/MC1222 http://webstore.ansi.org/FindStandards.aspx?SearchString=c12.22&SearchOption=0&PageNum=0&SearchTermsArray=null|c12.22|null	End Device Tables communications over any network
	ANSI C12.24 *Draft standard – not yet approved*	A calculation algorithm catalog Actors: Measurement devices, sensors, MDMS, enterprise applications
19	ANSI/CEA 709 and CEA 852.1 LON Protocol Suite	
	ANSI/CEA 709.1-B-2002 Control Network Protocol Specification http://www.ce.org/Standards/browseByCommittee_2543.asp	This is a general purpose networking protocol in use for various applications including electric meters, street lighting, home automation and building automation.
	ANSI/CEA 709.2-A R-2006 Control Network Power Line (PL) Chanel 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 http//www.ce.org/Standards/browseByCommittee_2759.asp	This is a specific physical layer protocol designed for use with ANSI/CEA 709.1-B-2002.
	CEA-852.1:2009 Enhanced Tunneling Device Area Network Protocols Over Internet Protocol Channels http://www.ce.org/Standards/browseByCommittee_6483.asp	This protocol provides a way to tunnel local operating network messages through an IP network using the User Datagram Protocol (UDP), thus providing a way to create larger internetworks.

	Standard	Application
20	CableLabs PacketCable Security Monitoring and Automation (SMA) http://www.cablelabs.com/specifications/PKT-TR-SMA-ARCH-V01-081121.pdf	Broad range of services, including energy management
21	FIXML Financial Information eXchange Markup Language http://www.fixprotocol.org/specifications/fix4.4fixml	Data exchange for markets
22	IEEE 1588 http://ieee1588.nist.gov/	Time Management and Clock Synchronization across the Smart Grid, equipment needing consistent time management
23	Internet Protocol Suite including, but not limited to :	
	IETF RFC 791 (IPv4) http://www.ietf.org/rfc/rfc791.txt	IETF RFC 791 : The internet protocol (IPv4) provides for transmitting blocks of data called datagrams from sources to destinations, where sources and destinations are hosts identified by fixed length addresses. The internet protocol also provides for fragmentation and reassembly of long datagrams, if necessary, for transmission through "small packet" networks.
	IETF RFC 768 (UDP) http://tools.ietf.org/html/rfc768	IETF RFC 768: User Datagram Protocol (UDP)-This protocol provides a procedure for application programs to send messages to other programs with a minimum of protocol mechanism.

	Standard	Application
	IETF RFC 2460 (IPv6) http://www.ietf.org/rfc/rfc2460.txt	IETF RFC 2460: Internet Protocol Version 6 (IPv6) Specification
24	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.
25	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.
26	ISO/IEC 18012, "Guidelines for Product Interoperability." http://www.iso.org/iso/catalogue_detail.htm?csnumber=30797 http://www.iso.org/iso/catalogue_detail.htm?csnumber=46317	Specifies requirements for product interoperability in the home and building automation systems,
27	ITU Recommendation G.9960 (G.hn) http://www.itu.int/ITU-T/aap/AAPRecDetails.aspx?AAPSeqNo=1853	In-home networking over power lines, phone lines, and coaxial cables.

	Standard	Application
28	Multispeak http://www.multispeak.org/About/specifications.htm	Application software integration within the operations domain; a candidate for use in an Enterprise Service Bus.
29	OPC-UA Industrial http://www.opcfoundation.org/Downloads.aspx?CM=1&CN=KEY&CI=283	A secure, high-speed data pipe from one system to another based on a tight publish/subscribe mechanism to provide a plug-n-play interface to another system with significant internal, high-speed data. Used in a variety of operations domain applications.
30	Open Geospatial Consortium Geography Markup Language (GML) http://www.opengeospatial.org/standards/gml	Exchange of location-based information addressing geographic data requirements for many Smart Grid applications.
31	US Department of Transportation's Federal Highway Administration's Intelligent Transportation System (ITS) Standard NTCIP 1213, "Electrical Lighting and Management Systems (ELMS) http://www.ntcip.org/library/documents/pdf/1213v0219d.pdf	Addresses open protocol remote monitoring and control of street, roadway and highway based electrical assets including lighting, revenue grade metering, power quality and safety equipment including remote communicating ground fault and arc fault interrupters.

While there is strong stakeholder consensus on the relevance of the standards listed in Table 2, many of the specifications require enhancements or other changes necessary to fully address Smart Grid requirements. Many of the needed modifications to these standards and related specifications will be driven by the Priority Actions Plans described in the next chapter. In addition, the Cyber Security Task Group, whose ongoing efforts are summarized in Chapter 6, also is addressing some of these needed modifications.

4.3 Standards for Further Consideration

Subsequently, NIST and its contractor, the Electric Power Research Institute (EPRI), convened a second workshop (May 19-20, 2009), where more than 600 people engaged in sessions focused on analyzing and enhancing use cases, locating key interfaces, determining Smart Grid interoperability requirements, and identifying additional standards for consideration. Many of the use cases discussed during this workshop referenced standards in addition to those in Table 2. Altogether, the use cases, which concentrated on the six priority areas, yielded more than 70 candidate standards and emerging specifications, which were compiled in EPRI's *Report to NIST on the Smart Grid Interoperability Standards Roadmap.*[30] The remainder of that list not covered by those in Table 2 is presented in Table 3.

EPRI used four "non-exclusive criteria" when identifying standards to include in the list:

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

EPRI's *Report to NIST on the Smart Grid* also was submitted for public review and comment. However, the standards listed were only a portion of a lengthy report. **NIST is using the public review process for this draft document as an opportunity to solicit further public comments and recommendations on existing standards or emerging specifications for inclusion in the list of standards that the Institute will publish in the final version of this document, the *NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0.*** A notice published in the *Federal Register* to announce the availability of this draft for public review will include a specific request for comments on standards listed in this chapter.

Table 3. Additional Standards for Further Review.

#	Standard	Application
1	ASN.1 (Abstract Syntax Notation)	Used to serialize data; used in (e.g.) X.400
2	Common pricing data and scheduling model (OASIS EMIX)	Exchange of price, characteristics, time, and related information for markets, including market makers, market participants, quote streams, premises automation, and devices

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

#	Standard	Application
3	DHS Cyber Security Procurement Language for Control Systems	The National Cyber Security Division of the Department of Homeland Security (DHS) developed this document to provide guidance to procuring cyber security technologies for control systems products and services - it is not intended as policy or standard. Because it speaks to control systems, its methodology can be used with those aspects of Smart Grid systems.
4	DLMS/COSEM (IEC 62056-X) Electricity metering - Data exchange for meter reading, tariff and load control	Device Language Message Specification/Companion Specification for Energy Metering.
5	FERC 888 Promoting Wholesale Competition Through Open Access Non-discriminatory Transmission Services by Public Utilities; Recovery of Stranded Costs by Public Utilities and Transmitting Utilities	Regulatory documentation for wholesale competition.
6	GPS	Global Positioning System for geospatial location and time
7	HomePlug AV	Entertainment networking content distribution for consumer electronic equipment
8	HomePlug C&C	Control and management of residential equipment for whole-house control products: energy management, lighting, appliances, climate control, security and other devices.
9	IEC 60929 AC-supplied electronic ballasts for tubular fluorescent lamps – performance requirements	Appendix E is known as DALI. Application: Information to and from lighting ballasts for Energy Management Systems
10	IEC PAS 62559	Requirements development method for all applications. This is a pre-standard with wide acceptance by early Smart Grid and AMI implementing organizations
11	IEEE C37.2	Protective circuit device modeling numbering scheme for various switchgear.

#	Standard	Application
12	IEEE C37.111-1999 (COMTRADE)	Applications using transient data from power system monitoring, including power system relays, power quality monitoring field and workstation equipment.
13	IEEE C37.232	Naming time sequence data files for substation equipment requiring time sequence data
14	IEEE 802 Family	This includes 802.1, 802.2, 802.3, 802.11 and subparts, 802.15.4, 802.15.4g, 802.16 and subparts, 802.20.
		802.1 Standard for Local and Metropolitan Area Networks (MAC/PHY layers)
		Station and Media Access Control Connectivity Discovery
		802.2 Logical Link Control
		802.3 Carrier Sense Multiple Access with Collision Detection Physical Layer
		802.11 Wireless LAN Medium Access Control and Physical Layer (MAC/PHY). Subparts are different network speeds and MAC/PHY characteristics.
		Commonly called WiFi. IEEE 802.11b data rate is 11Mbps, IEEE 802.11g data rate is 54Mbps, IEEE 802.11i specifies security
		802.15.1 Wireless Personal Area Networks (WPAN). Base for Bluetooth
		802.15.4 Wireless Personal Area Networks (WPANs). Base for ZigBee and others
		802.16 Fixed Broadband Wireless access systems. Base for WiMAX
		802.20 Mobile Broadband Wireless Access
15	IEEE 1159.3	Communications with Distributed Energy Resources
16	IEEE 1379-2000	Substation Automation - Intelligent Electronic Devices (IEDs) and remote terminal units (RTUs) in electric utility substations

#	Standard	Application
17	IEEE 1686-2007	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.
18	IEEE P1901	Smart Grid Physical Communications Broadband over Powerline (MAC/PHY)
19	IEEE P2030	Smart Grid Infrastructure
20	Internet-Based Management Standards (DMTF, CIM, WBEM, ANSI INCITS 438-2008	Data Communications Networking, Routing, Addressing, Multihoming, Faults, Configuration, Accounting, Performance, Security and other management
21	Internet-Based Management Standards (SNMP vX)	Data Communications Networking, Routing, Addressing, Multihoming, Fault, Configuration, Accounting, Performance, Security and other management
22	ISA SP99	Cyber security mitigation for industrial and bulk power generation stations. International Society of Automation (ISA) Special Publication (SP) 99 is a standard that explains the process for establishing an industrial automation and control systems security program through risk analysis, establishing awareness and countermeasures, and monitoring and improving an organization’s cyber security management system. Smart Grid contains many control systems that require cyber security management.
23	ISA SP100	Wireless communication standard intended to provide reliable and secure operation for non-critical monitoring, alerting, and control applications specifically focused to meet the needs of industrial users.
24	ISO27000	Security Management Infrastructure across various IT environments, which could be applied to field systems

#	Standard	Application
25	ISO/IEC 24752 user interface – universal remote control	Facilitates operation of information and electronic products through remote and alternative interfaces and intelligent agents. The series of standards, ISO/IEC 24752: 1-5, defines a framework of components that combine to enable remote user interfaces and remote control of network-accessible electronic devices and services through a universal remote console (URC)
26	NAESB OASIS (Open Access Same-Time Information Systems)	Utility business practices
27	NAESB WEQ 015 Business Practices for Wholesale Electricity Demand Response Programs	Utility business practices for Demand Response
28	NEMA Smart Grid Standards Publication SG-AMI 1-2009 – Requirements for Smart Meter Upgradeability www.nema.org	This standard will be used by smart meter suppliers, utility customers, and key constituents, such as regulators, to guide both development and decision making as related to smart meter upgradeability.
29	Networking Profiles Standards and Protocols	Recent workshops and prior work by the power industry has needed to adopt open standards for networking profiles. The Internet Protocols and standards in widespread use are supported by a significant number of documents. There is no single document that defines a networking profile for the use of the Internet Protocol. In addition the power industry will need a variety of different profiles to meet different requirements. NIST Special Publication 500-267 provides an example of profiles that several Internet Protocols and their capabilities satisfying the requirements of Smart Grid applications.
30	NIST FIPS 140-2	U.S. government computer security standard used to accredit cryptographic modules.
31	NIST FIPS 197 AES	Cryptographic standard: Advanced Encryption Standard (AES)
32	oBIX	Building automation, access control

#	Standard	Application
33	OSI (Open Systems Interconnect) Networking Profiles	Data Communications Networking, Routing, Addressing, Multihoming, Mobility and other networking services supporting functions
34	OSI-Based Management Standards (CMIP/CMIS)	Data Communications Networking, Routing, Addressing, Multihoming, Fault, Configuration, Accounting, Performance, Security and other management
35	RFC 3261 SIP: Session Initiation Protocol	Session Initiation Protocol (SIP) is an application-layer control (signaling) protocol for creating, modifying, and terminating sessions with one or more participants.
36	SAE J1772 Electrical Connector between PEV and EVSE	Electrical connector between Plug-in Electric Vehicles (PEVs) and Electric Vehicle Supply Equipment (EVSE)
37	SAE J2293 Communications between PEVs and EVSE for DC Energy	Communications between PEVs and EVSE for DC energy flow
38	SAE J2836/1-3 Use Cases for PEV Interactions	J2836/1: Use Cases for Communication between Plug-in Vehicles and the Utility Grid. J2836/2: Use Cases for Communication between Plug-in Vehicles and the Supply Equipment (EVSE). J2836/3: Use Cases for Communication between Plug-in Vehicles and the Utility Grid for Reverse Power Flow
39	SAE J2847/1-3 Communications for PEV Interactions	J2847/1 Communication between Plug-in Vehicles and the Utility Grid. J2847/2 Communication between Plug-in Vehicles and the Supply Equipment (EVSE). J2847/3 Communication between Plug-in Vehicles and the Utility Grid for Reverse Power Flow
40	Telecommunication Network Standards for Cellular and Broadcast	This list represents the collections of cellular and broadcast communications networking standards: 1xRTT, 3GPPP/LTE, CDMA, DLS, EDGE, EvDO, GPRS, GSM, HSDPA, RDS, SMS.
41	W3C Simple Object Access Protocol (SOAP)	XML protocol for information exchange
42	W3C WSDL Web Service Definition Language	Definition for Web services interactions

#	Standard	Application
43	W3C XML eXtensible Markup Language	Self-describing language for expressing and exchanging information
44	W3C XSD (XML Schema Definition)	Description of XML artifacts, used in WSDL (q.v.) and Web Services as well as other XML applications.
45	WS-Calendar (OASIS)	XML serialization of IETF iCalendar for use in calendars, buildings, pricing, markets, and other environments
46	WS-Security	Toolkit for building secure, distributed applications. Broadly used in eCommerce and eBusiness applications. Fine-grained security. Part of extended suite using SAML, XACML, and other fine-grained security standards.

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

NIST has developed a core set of criteria to provide initial guidance when evaluating prospective Smart Grid standards. This guidance is presented in the text box below. NIST seeks public comments on the usefulness of the criteria as well as suggestions for improving the guidance for future evaluations of standards.

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

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

Reviewing these criteria and the comments received on them will be one of the first tasks of the Smart Grid Interoperability Panel that will be created to continue development of action plans for the Smart Grid.

Guidance for Identifying Standards for Implementation

NIST proposes that the criteria listed below be used to evaluate standards and emerging specifications for inclusion in the *NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0,* and subsequent versions. The full set of criteria does not apply to every standard or specification listed in Tables 2 and 3. Judgments on whether a standard merits inclusion should be made on the basis of combinations of relevant criteria.

For *Release 1.0,* NIST proposes that a standard or emerging specification should be evaluated on whether it:

- Is well-established and widely acknowledged as important to the Smart Grid.
- Is an open, stable and mature industry-level standards developed in consensus processes from a standards development organization (SDO).
- Enables the transition of the legacy power grid to the Smart Grid.
- Has, or is expected to have, significant implementations, adoption, and use.
- Is supported by an SDO or Users Group to ensure that it is regularly revised and improved to meet changing requirements and that there is strategy for continued relevance.
- Is developed and adopted internationally, wherever practical.
- Is integrated and harmonized 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, or
    - Distribution Grid Management.

[†] 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.

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

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

5 Priority Action Plans

5.1 Overview

NIST has identified an initial set of priorities for developing standards necessary to build an interoperable Smart Grid. Among the criteria for inclusion on this initial list were (1) immediacy of need, (2) relevance to high-priority Smart Grid functionalities,[31] (3) availability of existing standards to respond to the need, and (4) the extent and stage of the deployment of affected technologies. In assembling this list, NIST considered stakeholder input received at three public workshops and other public interactions, as well as reviews of research reports and other relevant literature.

The most recent of these workshops (August 3-4, 2009) engaged more than 20 standards development organizations (SDOs) as well as user groups in addressing these priorities. At the workshop, SDOs and other Smart Grid stakeholders agreed on many individual and collaborative responsibilities for addressing standards issues and gaps. They also defined tasks and set aggressive timelines for accomplishing many of them.

In addition to parallel efforts on cyber security (described in the next chapter), the priority actions plans (PAPs) summarized below are proceeding rapidly but are also works in progress. They are undergoing continuing improvement and refinement, and are updated to incorporate new developments and to reflect the current status of plan implementation. Complete versions of the PAPs, which are summarized below, can be found on-line on the NIST Smart Grid wiki.[32]

The initial PAPs are just the beginning of accelerated development and sustained standardization effort that will span a number of years. New PAPs will be developed over time as existing PAPs are completed to encompass the larger scope of standardization efforts that will be required as the nation pursues the vision of a fully interoperable Smart Grid.

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

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

Meter Upgradeability Standard—A Completed Priority Action Plan

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

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

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

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

5.2 Develop Common Specification for Price and Product Definition

A common specification for price is critical for applications used across the Smart Grid. The price and product specification is being developed on a rapid time-scale. A draft specification will be ready in April 2010. This effort is drawing on input from a wide group of stakeholders as well as existing work. It focuses on meeting the immediate needs of utilities and demand response program mandates while building an extensible foundation for a market-based Smart Grid.

Abstract

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

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

Why

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

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

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

Major Objectives

- Develop a summary of power reliability and quality characteristics that affect price and availability (supply side) and desirability (demand side).
- Survey existing price communications and develop harmonized specification (review by October 2009, draft specification by April 2010).
- Engage the broad group of stakeholders into the effort.
- Build on existing work in financial energy markets and existing demand response programs.
- Integrate with schedule and interval specifications under development (see section 5.3).

Project Team

NIST Lead: Dave Holmberg

Collaborators:

AHAM

ASHRAE

BAE Systems

Cazalet Group

FIX

FIX Protocol

GWAC

IEC

ISO

LONMark International

Multispeak

NAESB

New England ISO

No Magic, Inc.,

OASIS

OpenADR

PNL

UCAIug

ZigBee

The full plan can be found at this referenced link[33]

5.3 Develop Common Scheduling Mechanism for Energy Transactions

The coordination of supply and demand is already of critical importance on the grid; tomorrow, with the increase of distributed energy resources, this coordination becomes more critical. A draft specification for facilitating common scheduling operations across different domains will be completed by December 2009.

Abstract

Already important, coordination of supply and demand in the grid will be even more critical as distributed energy resources increase and as renewables account for a growing share of electric power. Beyond electromechanical devices and equipment, necessary levels of coordination extends to enterprise activities, home operations and family schedules, and market operations. A common schedule specification is required for the Smart Grid and the many sectors that interact with the grid.

Under this plan, NIST and its collaborators are surveying existing calendaring specifications. They will develop a standard for how schedule and event information is passed between and within services. The output will be a micro-specification that can then be incorporated into price, demand-response, and other specifications. Easy integration of the specification will facilitate a common scheduling operation across different domains and diverse contracts. A draft is scheduled to be completed by the end of 2009 so that it can be included in the Common Specification for Price and Product Definition that will be developed under another PAP.

Why

Services operate—and are negotiated—on the basis of schedules. Some services may stem from almost instantaneous transactions while others may require significant lead times and

[33] http://collaborate.nist.gov/twiki-sggrid/bin/view/_SmartGridInterimRoadmap/PAP03PriceProduct

coordination with other services, processes, or actors. Central coordination of such services actually reduces interoperability, as it requires the coordinating agent to know the lead time of each service. The Smart Grid relies on coordinating processes in homes, offices, and industry with projected and actual power availability, including different prices at different times. In addition, regularly updated weather reports are becoming increasingly important to projecting energy availability. Energy use in buildings can be reduced if building-system operations are coordinated with the schedules of the occupants. A common standard for transmitting calendaring information will enable the coordination necessary to improve energy efficiency and overall performance.

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

Major Objectives

- The Calendar Consortium will complete its current work of XML serialization of ICalendar into a Web-service component (WS-Calendar) by the end of 2009.
- ISO20022 will comment on and coordinate with the Calendar Consortium on schedule semantics across enterprise, energy, and financial information.
- Ongoing work in price and product definition standards development and in grid end node interactions (OASIS Energy Interoperability) will incorporate a schedule component pending completion of this work.

Project Team

NIST Lead: Dave Holmberg

Collaborators:

CALCONNECT	NAESB	SIIA
FIX Protocol	OASIS	UCAIug
ISO	OSCRE	
ISO20022	PNL	

The full plan can be found at this referenced link.[34]

5.4 Develop Common Information Model (CIM) for Distribution Grid Management

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 and create a more reliable and efficient grid. The accelerated timeline calls for creation of an interoperability test team in 2009; development of integrated models for

[34] http://collaborate.nist.gov/twiki-sggrid/bin/view/_SmartGridInterimRoadmap/PAP04Schedules

Multispeak, a standard that is widely used by rural cooperative electric utilities; and development of requirements and common models for data and information used in distribution systems and back-office equipment by the end of 2010.

Abstract

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

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

Why

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

Major Objectives

- Develop strategies to integrate and expand IEC 61970-301, IEC 61968, Multispeak and IEC 61850 for Smart Grid applications.
- Create a scalable strategy to integrate other identified standards.
- Evaluate the contents of each standard for a “best fit” to meet the requirements of key applications that span the environments of these standards. Agree on an approach to integrate domain knowledge represented in each standard.

Project Team

NIST Lead: Jerry FitzPatrick

SDO Leads: IEC TC57 WG14, IEC TC57 WG17, MultiSpeak

Collaborators:

IEC TC57 WG10

IEC TC57 WG13

IEC TC57 WG15

IEC TC57 WG19

IEEE Power Systems Relay Communications Committee

IEEE Power and Energy Society Distribution Automation Working Group
NAESB

OpenGeospatial Consortium

Transmission & Distribution Domain Expert Working Group

UGAIug

Utility Communication Architecture International users' group (UCAIug)

Utilities Standards Board (USB)

The full plan can be found at this referenced link.[35]

5.5 Standard Demand Response Signals

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

Abstract

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

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

[35] http://collaborate.nist.gov/twiki-sggrid/bin/view/_SmartGridInterimRoadmap/PAP08DistrObjMultispeak

Why

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

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

Major Objectives

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

Project Team

NIST Lead: Dave Holmberg

Collaborators:

ASHRAE
AHAM
CAISO
EPRI (appliances)
GWAC/Industrial
Home Automation
HomePlug SEP2
IEC TC57 WG14
ISO/IEC JTC 1 WG15
ISO/RTU+GWAC
LBNL OpenADR
LONMark
NAESB
OASIS
UCAIug
UCAIug AMI-ENT TF
UCAIug Smart Grid SC
ZigBee

The full plan can be found at this referenced link.[36]

[36] http://collaborate.nist.gov/twiki-sggrid/bin/view/_SmartGridInterimRoadmap/PAP09DRDER

5.6 Standards for Energy Usage Information

Customers will benefit from energy usage information that enables them to make better decisions about energy use and take other actions consistent with the goals of Section 1301 of EISA. In particular, consumers could make better decisions about emerging energy conservation/efficiency applications, including whether to change DR plans, or to take specific actions now in anticipation of future DR events. Given that some states have mandated customer access to this information, an initial specification is expected in January 2010.

Abstract

This action plan will define data standards to enable customers and customer-authorized third-party service or software providers to access energy usage information from the Smart Grid, enabling customers to make better decisions about energy use and conservation. The data standards will enable immediate and widespread benefit. They will support access to monthly usage information, which is already available, as well as near-real-time information that will be available as smart meters are deployed. The standards will promote innovation by third-party service and software providers in providing novel ways to help consumers manage their energy usage. In the absence of these standards, software developers and utilities would have to negotiate pair-wise interfaces, an impractical situation.

These standards must be developed on an aggressive timetable. States such as California and Texas have mandated that consumers have electronic access to such data in 2010. This action plan will result in a requirements definition for the standards by October 2009 and an initial specification by January 2010.

Why

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

Information about energy consumption can be provided by the on-premises meter. It also can be made available through energy delivery systems (such as those operated by utilities or aggregating service providers) and through consumer devices. Anticipated initial users of this information model will be utilities and other service providers, which will provide energy usage information to customers via the World Wide Web, or public Internet. The model also will support development of on-premises devices that can access meters and provide usage information directly to the occupant.

A robust information model should be invariant, scalable, and extensible, as well as interoperable with the communications standards in place in the home, business, distribution system, or enterprise. This effort will overlap with and support information standards for load curtailment, load shaping, and energy market operations. The primary focus, however, will be on more immediate actionable steps to define and standardize energy usage information and to make it more readily available.

Major Objectives

- Develop a summary of information needs for various means of customer access to metering and billing information. The goal is to develop requirements by the end of October 2009.
- Vet these requirements among standards organizations (including IEC, NEMA, OASIS, and ZigBee) and identify potential harmonization opportunities. (UCAIug – OpenSG has committed to developing a statement of support for extending their process to include additional stakeholders.).
- Carry out an initial effort that delivers on meeting upcoming state public utility commission mandates (including California) to provide customer electronic access to energy-usage data (from both smart meters and legacy meters). This effort must encompass scalability for the larger effort, such that applications designed to use the initial release will function properly in the presence of data from later, more extensive releases. The goal is to have useable definitions in place by January 2010 to meet PUC mandates.
- Develop a composite information model that can be easily transformed without loss and transported via standards in OASIS, IEC61970/61968, IEC61850, ANSI C12.19/22, ASHRAE 135, and ZigBee SEP.
- Develop and implement a plan to expedite harmonized standards development and adoption within the associated standards bodies.

Project Team:

NIST lead: David Wollman

Lead organization: UCAIug – OpenSG

Coordinating organizations:

IEC (61850; 61970/61968)

NEMA (ANSI C12 Secretariat)

OASIS

ZigBee

The full plan can be found at this referenced link. [37]

5.7 IEC 61850 Objects/DNP3 Mapping

DNP3 (the Distributed Network Protocol) is the de facto communication protocol used at the distribution and transmission level in the North American power grid. However, DNP3 is not fully capable of enabling Smart Grid functions. The Smart Grid must accommodate and build upon the legacy systems of today’s power grid, and DNP3 is an essential element of it.

[37] http://collaborate.nist.gov/twiki-sggrid/bin/view/_SmartGridInterimRoadmap/PAP10EnergyUsagetoEMS

Guidelines for achieving interoperable integration of DNP3 with Smart Grid standards will be completed in 2010.

Abstract

This action plan focuses on developing the means to enable transport of Smart Grid functions over the legacy DNP3 networks. This will be accomplished by carrying out the first step in integrating DNP3 data to conform with the newer IEC 61850 standard for Communication Networks and Systems in Substations, which is better suited to support Smart Grid functions. IEC 61850 is a standard for substation automation, and supports monitoring and control of grid equipment (relays, circuit breakers, transformers) as well as renewable energy resources. This step is called mapping, which enables the translation of data between different systems. There is an urgent need for communication networks in legacy, DNP3-based distribution systems to support exchanges of large volumes of data (with low latency, i.e., time delays) that are necessary to achieve new Smart Grid capabilities. Many of the new deployments, including those funded under Department of Energy Smart Grid grants programs, will require rapid, high-bandwidth communications that are better supported by IEC 61850. For 2009, the tasks of this action plan include performing a gap analysis to identify the extent to which DNP3 meets Smart Grid requirements. Guidelines for achieving interoperable integration of DNP3 with IEC 61850 and other Smart Grid standards will be produced in 2010.

Why

DNP3 was designed for low-bandwidth Supervisory Control and Data Acquisition (SCADA) operations that control grid equipment. Data acquisition consists of three types of data: binary (digital) inputs, analog inputs, and counters. Supervisory control consists of commands for both digital and analog equipment. Although this protocol allows any DNP data to be transported between any two points, the semantic content of the messages depends upon lists of tables, which are not machine readable.

The desire is to ensure that data is seamlessly transported between devices and readily used by them, even when there are communication constraints imposed by the DNP3 protocol.

Mapping of objects in each direction presents difficult challenges.

Major Objectives

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

Project Team

NIST Leads: Jerry FitzPatrick, Tom Nelson

SDO Leads:

DNP Technical Committee

IEC TC57 WG10

UCAIug Technical Committee

Collaborators:

DNP User Group

IEC TC57 WG03

UCAIug Testing Committee

Utility Representatives

The full plan can be found at this referenced link.[38]

5.8 Time Synchronization

Common time synchronization is the key to many Smart Grid applications that will result in the real-time operation necessary to make the Smart Grid highly robust and resilient to disturbances (“self-healing”), either from natural events such as earthquakes or large variations in wind or solar power availability, or from terrorist actions. Precision time protocols and synchrophasor rapid prototyping and testing are planned for mid-2010.

Abstract

This action plan focuses on ensuring that Smart Grid deployments use a common format and have common meaning for time data so that the applications are readily interoperable. The approach includes determining detailed requirements for Smart Grid applications and in particular, for synchrophasor measurements used to monitor conditions in the transmission grid. Additionally, the tasks cover harmonizing the differences in time data formats used by Smart Grid standards, promoting rapid prototype development and interoperability testing, and developing guidelines on how to achieve uniform time-stamping throughout the Smart Grid. The DOE Smart Grid Investment Grant Program will fund implementations of phasor measurement units (PMUs) that measure synchrophasors, which makes rapid resolution of time synchronization issues imperative. The tasks for this action plan to be completed in 2009 include determining synchrophasor data transport requirements, performing device interoperability demonstrations for time standards such as IEEE 1588, a key element to achieving synchronization, resolving timestamp differences between PMU and substation communication standards, and performing interoperability demonstrations for time data. A precision time protocol is to be completed in early 2010, and the synchrophasor rapid prototyping and interoperability testing is planned for mid-2010.

Why

Two standards are related to communications of phasor measurement unit (PMU) data and information. IEEE C37.118 was published in 2005 for PMUs. IEC 61850 has been substantially

[38] http://collaborate.nist.gov/twiki-sggrid/bin/view/_SmartGridInterimRoadmap/PAP12DNP361850

developed for substations but is seen as a key standard for all 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 is only a small step to use it as well for transmission of PMU data. The models for PMU data need to be defined in IEC 61850. This work item seeks to assist and accelerate the integration of standards that can impact phasor measurement and applications depending on PMU-based data and information. Integrating IEEE C37.118 with IEC 61850 will help to remove overlaps between the standards, which may impede development of interoperable equipment and systems. IEEE C37.118 is intended to support applications such as protection. IEC 61850 is suitable for system-wide applications that require higher publishing rates.

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

Major Objectives

- Develop contributing technical work to integrate IEEE C37.118 and IEC 61850 under a Dual IEEE/IEC Logo Standard January 2010.
- Participate with SDO working groups to work out technical issues related to the standard integration (ongoing).
- Support prototyping activities (ongoing).
- Facilitate interoperability demonstrations of prototypes (plugfest) (September 2009).
- Validate detailed requirements from Smart Grid applications using common time synchronization and time management (October 2009).
- Develop, in cooperation with SDO working groups, guidelines for application and role-based time synchronization.
- Develop contributing technical work to prepare standard profiles for IEEE 1588 (January 2010).
- Ensure NASPI-NET and NERC timing requirements are encompassed by work of this group (September 2009).
- Resolve differences between time stamp format and time semantic of C37.118 and 61850 (perhaps add a second timestamp to message) (November 2009).

Project Team

NIST Lead: Jerry FitzPatrick

Lead SDO: IEC TC 57 WG 10 6185090

Collaborators:

EPRI

IEC TC57 WG19

IEC TC57 WG15

IEC TC38 WG37

IEEE Power Systems Relaying Committee (PSRC) H11

IEEE PSRC H7

IEEE PSRC H3

IEEE PSRC, Communications Subcommittee

IEEE PSRC H4 C37.111 COMTRADE

NASPI

NASPI, Performance and Standards Committee

NERC CSSWG

PJM

Utillity Communication Architecture International users' group (UCAIug)

The full plan can be found at this referenced link.[39]

5.9 Transmission and Distribution Power Systems Model Mapping

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

Abstract

This plan will define strategies for integrating standards across different utility environments to support different real-time grid operations (relay, circuit breaker, transformer operations) and back-office applications for customer services, meter data and billing, and other business operations. The work must meet an aggressive schedule to enable ready interoperability of ongoing Smart Grid deployments funded by federal and industry investments. Modeling of the electric power system, multifunctional intelligent electronic devices (IEDs), and definition of standard methods for reporting events and exchanging relay settings will enable improving the efficiency of many protection, control, engineering, commissioning, and analysis tasks. Tasks for

[39] http://collaborate.nist.gov/twiki-sggrid/bin/view/_SmartGridInterimRoadmap/PAP1361850C27118HarmSynch

2009 include identifying issues that stand in the way of harmonizing potentially conflicting standards and identifying information requirements for relay settings in the Smart Grid. Some of the tasks identified for this action plan overlapped with those in the PAP described in 5.4, Develop Common Information Model (CIM) for Distribution Grid Management, and are covered by it as noted in the objectives given below.

Why

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

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

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

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

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

Major Objectives

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

- Develop a summary of information required from the power system for various Smart Grid applications (December 2009). (Covered by the PAP tasks described in section 5.4.)

- Map that information with the already defined models from MultiSpeak, IEC 61970, IEC 61968-11, and IEC 61850 (June 2010). (Covered by the PAP tasks described in section 5.4.)
- Coordinate with the SDO to extend the existing models. (Covered by the PAP tasks described in section 5.4.)
- Identify power equipment setting information that is required for performing an automatic verification of the power system configuration to prevent failures due to misconfigurations. This information shall include both settings in the devices as well as parameters of the power network that need to be available for verification.
- Coordinate with SDOs to extend the existing standards to include the necessary setting information (year-end 2010).

Project Team

NIST Lead: Jerry FitzPatrick

Lead SDO: IEC TC57, WG10

Collaborators:

EPRI

IEEE PSRC H7

IEEE PSRC H5

IEEE PSRC H16

IEEE PSRC, Communications Subcommittee

IEC TC57 WG13

IEC TC 57 WG14

UCAIug

The full plan can be found at this referenced link.[40]

5.10 Guidelines for the Use of IP Protocol Suite in the Smart Grid

Abstract

Internet technologies have important roles to play in the Smart Grid information networks. Defining the roles and identifying the appropriate Internet standards or Internet Engineering Task Force “requests for comments” (RFCs) are important jobs that must begin immediately and must receive sustained effort. This action plan presents steps for developing guidelines for the use of the IP protocol suite by working with key SDO committees to determine the characteristics of Smart Grid application areas and types and the applicable protocols. The networking profiles identified under this action plan will define a significant portion of the interfaces to Smart Grid equipment and systems in any intra-domain and inter-domain applications.

[40] http://collaborate.nist.gov/twiki-sggrid/bin/view/_SmartGridInterimRoadmap/PAP14TDModels

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

Why

The Smart Grid will require a comprehensive mapping of application requirements to the capabilities of protocols and technologies in a well-defined set of Internet Protocol Suite(s) or Profiles. This set should be defined by experts well-versed in the applications and protocols, including management and security. Most notably, the interfaces that integrate systems over wide-area networks and large geographical areas must be defined, in part, by these profiles. The profiles will specify networking functions, such as addressing, and the integration of concepts, such as multihoming and other key functions necessary for the Smart Grid. Therefore, a set of well-defined networking profiles needs to be tested for the consistency and interoperability necessary to achieve appropriate levels of integration across the Smart Grid. Consistent, testable protocol profiles also are necessary to ensure that conforming technologies will meet today's requirements and that the profiles can be extend to accommodate future Smart Grid application as well.

Major Objectives

- Review the communications networks and domains identified in the Smart Grid conceptual model and determine whether they are described in sufficient detail for evaluations of the application of Internet Protocol suites.
- Determine an approach to fully defining the network and systems management requirements for Smart Grid networking infrastructures.
- Define a set of standards profiles required for Smart Grid networks.
- Identify key networking profiles issues, including issues surrounding IPv4 vs. IPv6.
- Determine the key remaining issues surrounding adoption of standardized networking profiles.
- Determine appropriate Smart Grid network architectures and technologies appropriate for basic transport and security requirements (e.g., shared IP networks, virtual private networks, MPLS switching, traffic engineering, and resource control mechanisms).
- Determine which transport layer security protocol(s) (e.g., TLS, DTLS, SCTP, and IPsec) are most appropriate for securing Smart Grid applications.
- Identify higher layer security mechanisms (e.g., XML, S/MIME) to secure transactions.
- Develop an action plan for development of necessary usage guides, profiles, and remaining work.

Project Team

NIST Lead: David Su

Lead SDO: IETF

Collaborators:

ATIS

IEEE

NEMA

TIA

UCAIug

The full plan can be found at this referenced link.[41]

5.11 Guidelines for the Use of Wireless Communications

Abstract

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

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

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

Why

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

Specific tasks include:

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

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

[41] http://collaborate.nist.gov/twiki-sggrid/bin/view/_SmartGridInterimRoadmap/PAP01InternetProfile

3) Compiling and communicating Smart Grid requirements and use cases in a standardized format mapped into categories identified in task 1.
4) Creating an attribute list and performance metrics for wireless standards.
5) Creating an inventory of wireless technologies and standards that are identified by each SDO in accordance with the metrics developed in task 4.
6) Performing the mapping and conducting an evaluation of the wireless technologies based on the criteria and metrics developed in task 4 and identify gaps where appropriate.

Major Objectives

- Identify key issues to be addressed in wireless assessments and development for the Smart Grid.
- Identify requirements for use of wireless technologies for different Smart Grid applications.
- Identify approaches to define the strengths and weaknesses of candidate wireless technologies to assist Smart Grid design decisions.
- Analyze both intentional and unintentional interference issues and develop coexistence guidelines for deployment and operation.
- Identify guidelines for effectively, safely, and securely employing wireless technologies for different Smart Grid applications.

Project Team

NIST Lead: David Su

Collaborators:

ATIS

IEEE 802

IEEE P2030

IETF

ISA SP100

TIA

WiFi Alliance

UCAIug

Utility Telecom Council (UTC)

Zigbee Alliance

The full plan can be found at this referenced link.[42]

5.12 Energy Storage Interconnection Guidelines

Although still in their infancy, energy storage technologies will play an increasingly important role in the evolution of the power grid, particularly in providing a solution that will enable large penetration of intermittent renewables while also enhancing the stability of the grid. Indeed, the

[42] http://collaborate.nist.gov/twiki-sggrid/bin/view/_SmartGridInterimRoadmap/PAP02Wireless

Federal Energy Regulatory Commission has identified energy storage as a key Smart Grid functionality. Specifications, standards and guidelines are planned to be completed by the middle of 2010.

Abstract

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

The initial step of defining interconnection requirements across a broad range of anticipated ES-DER scenarios (including islanding[43]) is scheduled to be completed by October 2009, and the use case analyses for these scenarios is scheduled to be completed by December 2009. This will greatly expedite the formation of new standards projects for Smart Grid dispatchable storage extensions of the IEEE 1547 series of standards, which define the physical and electrical interconnection of DERs with the grid. A similar fast-tracking effort will focus on defining ES-DER object models in the IEC 61850-7-420 standards to accommodate Smart Grid requirements. Collaborations with UL, SAE, NEC-NFPA70, and CSA also have been initiated to focus on specifications for safe and reliable implementation.

Why

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

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

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

ES-DER systems based on photovoltaic, wind, and other intermittent renewables are exploring the use of storage to help smooth their intermittency and augment their ability to respond to distribution power grid management requirements. Appropriate interconnection standards, Smart Grid devices, and storage are all key elements of the solution that will enable large penetration of renewables while also enhancing rather than diminishing the stability of the Grid.

An assortment of ES-DER systems are emerging. They vary in abilities to respond to power grid management requests, and they use different system parameters and technologies for forecasting their availability. Furthermore, the storage needs (power, energy, duty cycle, and functionality) will also depend on the grid domain where the storage is used (e.g., transmission, distribution, consumer). These considerations need to be included in the storage and hybrid generation-storage interconnection and information model standards.

Major Objectives

- Convene a broad set of stakeholders, including utilities from different regions, the international community, groups addressing similar issues (such as wind turbine interconnection), vendors and researchers, to address ES-DER electric interconnection issues.
- Develop a scoping document to identify the ES-DER interconnection and operational interface requirements for the full spectrum of application issues: high penetration of ES-DER, ride-through of power system anomalies, plug-in electric vehicles, and all sizes of ES-DER systems, including those at customer sites, within distribution systems, and at transmission level; to be completed by October 31, 2009.
- Develop within IEEE P2030 use cases to identify and prioritize interconnection and object modeling requirements for ES-DER before electrical connectivity standards are developed; to be completed by December 31, 2009.
- Update or augment the IEEE 1547 distribution level standards series, as appropriate, to accommodate the wide range of ES-DER system requirements; including new IEEE SCC21 projects to be initiated in Spring 2010.
- Augment the IEC 61850-7-420 object models for ES-DER.
- Initiate development of transmission level standards for ES-DER. These should build on the FERC wind plant interconnect (LGIP) guidelines and European practice (e.g., e-on, ESB).
- Harmonize the distribution and transmission level standards, where possible.

Project Team

NIST Lead: Al Hefner

SDO Leads:

IEEE SCC21

IEC TC57 WG17

Collaborators:

A123Systems

ABB

AEP

Altairnano

BuildingSmart

CSA-Standards

DTE Energy

EPRI

FSEC

GMATC

IEEE

NEC-NFPA

NEMA

Novus Energy

NREL

ORNL

OSCRE

SAE

Satcon

Sandia

S&C

UL

The full plan can be found at this referenced link.[44]

5.13 *Interoperability Standards to Support Plug-in Electric Vehicles*

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

Abstract

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

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

Why

Hybrid and electric vehicle owners will need to charge their vehicles, both at home and at sites along their local and extended travels. These travels might take them to work, to the grocery store, or on a cross-country trip. PEVs have the potential to significantly burden utilities. They also have the ability to be used as strategically important energy storage assets that can smooth

[44] http://collaborate.nist.gov/twiki-sggrid/bin/view/_SmartGridInterimRoadmap/PAP07Storage

out power demand. By providing intelligent charging capabilities and giving customers the control and the price incentives to charge during off-peak hours and to return stored power during periods of high demand, the nation can better leverage existing resources to support this new source of load and distributed storage.

Objectives

- Gather and normalize all the existing use cases and derive requirements so that each element of prospective standards meetsa particular stakeholder need; to be completed by December 2009.
- Draft common high-level information models in UML to be used as a basis for specific models needed for different SDO projects; to be completed by February 2010.
- Facilitate productive collaboration among the many different SDOs involved in the PEV infrastructure. These SDOs represent a variety of domains and, traditionally, most have not worked together. Currently, there are few—or no—mechanisms for the different standards groups to work together; to be completed by September 2009.
- Once the common high-level model is developed in task (2), specific implementation models must be developed for each standard. The common UML model will be used to create this standards-specific view of the model for IEC 61968/61850. These standards-specific implementation models will form the basis for the standards documents; to be completed by December 2010.
- Identify regulatory impediments to achieving the goals defined in the PEV use cases. Review the current regulatory/use case conflicts to determine areas where changes are needed; advise regulatory bodies of the identified obstacles and develop options for solutions; to be completed by January 2010.
- Ensure that other standards involving safety, interconnection, and certification support the PEV use cases; to be completed by January 2010.

Project Team

NIST lead: Eric Simmon

Lead organization: SAE

Collaborators:

ANSI

IEC 61850; 61970/61968)

IEEE

NEMA

ZigBee

The full plan can be found at this referenced link.[45]

[45] http://collaborate.nist.gov/twiki-sggrid/bin/view/_SmartGridInterimRoadmap/PAP11PEV

5.14 Standard Meter Data Profiles

Abstract

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

Tasks include mapping utility requirements expressed via AEIC Guidelines v2.0 to device classes by January 2010, expressing AEIC Guidelines v2.0 in terms of one or more additional device classes by May 2010, and completing AEIC Guidelines v2.0 by December 2009. Other tasks include socializing the existence of additional tables within ANSI C12.21-2006 and C12.22-2008 and socializing the existence and application of existing default sets, and the definition of new default sets, device classes, and profiles via Web conferences, all by fourth quarter 2010.

Why

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

Meter information that can be made available in common data tables will greatly reduce the time for utilities and others requiring meter data to implement Smart Grid functions, such as demand response and real-time usage information.

Major Objectives

- Define common meter Device Classes by building upon the work performed by the AEIC for defining the common meter data tables that are required to enable Smart Grid applications.
- Deliver these meter Device Classes to ANSI C12 SC17 for inclusion in ANSI C12.192008.
- Revise ANSI C12.19 and publish by March 2010.
- Publish these meter Device Classes in ANSI C12.19 and make these meter Device Classes readily available for use by all vendors and software implementers.

Project Team

NIST lead: Tom Nelson

Collaborators:

AEIC

ANSI C12 SC12.1

ANSI C12 SC17

ANSI C12 SC17 WG1

ANSI C12 SC17 WG2

ANSI C12 SC17 WG3

ANSI C12 SC17 WG4

IEC TC13

IEC TC57 Smart Grid TF

IEEE SCC31

IEEE SCC31 End Devices SC

MultiSpeak

NEMA:

UCAIug AMI-NET TF

Measurement Canada

The full plan can be found at this referenced link.[46]

[46] http://collaborate.nist.gov/twiki-sggrid/bin/view/_SmartGridInterimRoadmap/PAP05MeterProfiles

6 Cyber Security Risk Management Framework and Strategy

6.1 Overview

With the Smart Grid's transformation of the electric system to a two-way flow of electricity and information, the information technology (IT) and telecommunications infrastructures have become critical to the energy sector infrastructure. Therefore, the management and protection of systems and components of all three of these infrastructures must also be addressed in concert by an increasingly diverse energy sector. To achieve this requires that security be designed in at the architectural level.

NIST has established a Smart Grid Cyber Security Coordination Task Group (CSCTG), which now has more than 200 volunteer members from the public and private sectors, academia, regulatory organizations, and federal agencies. Cyber security is being addressed in a complementary and integral process that will result in a comprehensive set of cyber security requirements. As explained more fully later in this chapter, these requirements are being developed using a high-level risk assessment process that is defined in the cyber security strategy for the Smart Grid.

Although still a work in progress, NIST soon will be publishing a preliminary report, NISTIR 7628 Smart Grid Cyber Security Strategy and Requirements, which describes the CSCTG's overall cyber security strategy for the Smart Grid. The preliminary report distills use cases collected to date, requirements and vulnerability classes identified in other relevant cyber security assessments and scoping documents, and other information necessary for specifying and tailoring security requirements to provide adequate protection for the Smart Grid. Anticipated to be published by the end of 2009, a subsequent draft will include the overall Smart Grid security architecture and security requirements.

The first installment of this in-process document, Smart Grid Cyber Security Strategy and Requirements,[47], also will be submitted for public review and comment in conjunction with this interoperability standards framework and roadmap. This roughly 200-page document is summarized below.

6.2 Cyber Security and Critical Infrastructure

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

[47] The document will be available at: http://csrc.nist.gov/publications/PubsDrafts.html#NIST-IR-7628 Comments may be submitted to: csctgdraftcomments@nist.gov.

The Energy Independence and Security Act of 2007 states that, “It is the policy of the United States to support the modernization of the Nation's electricity transmission and distribution system to maintain a reliable and secure electricity infrastructure that can meet future demand growth and to achieve each of the following, which together characterize a Smart Grid: …

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

DOE’s *Energy Sector-Specific Plan*[48] “envisions a robust, resilient energy infrastructure in which continuity of business and services is maintained through secure and reliable information sharing, effective risk management programs, coordinated response capabilities, and trusted relationships between public and private security partners at all levels of industry and government.”

6.3 Scope, Risks, and Definitions

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

Additional risks to the grid include:

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

With the transition to the Smart Grid, the IT and telecommunication sectors will be more directly involved. These sectors have existing cyber security standards to address vulnerabilities and assessment programs to identify known vulnerabilities in these systems. These same

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

vulnerabilities need to be assessed in the context of the Smart Grid. In addition, the Smart Grid has additional vulnerabilities due to its complexity, large number of stakeholders, and highly time-sensitive operational requirements.

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

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

For this document cyber security is defined as follows:

- **Cyber Security**: The protection required to ensure confidentiality, integrity and availability of the electronic information communication systems.

6.4 Smart Grid Cyber Security Strategy

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

Implementation of a cyber security strategy requires the development of an overall cyber security risk management framework for the Smart Grid. This framework is based on existing risk management approaches developed by both the private and public sectors. This risk management framework establishes the processes for combining impact, vulnerability, and threat information to produce an assessment of risk to the Smart Grid and to its domains and sub-domains, such as homes and businesses. Risk is the potential for an unwanted outcome resulting from an incident, event, or occurrence, as determined by its likelihood and the associated impacts. Because the Smart Grid includes systems and components from the IT, telecommunications, and energy sectors, the risk management framework is applied on an asset, system, and network basis, as applicable. The goal is to ensure that a comprehensive assessment of the systems and components of the Smart Grid is completed. Following the risk assessment, the next step is to select and tailor (as necessary) the security requirements.

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

- National Institute of Standards and Technology (NIST) Special Publication (SP) 800-39, *DRAFT Managing Risk from Information Systems: An Organizational Perspective*, April 2008.

- Federal Information Processing Standard (FIPS) 200, *Minimum Security Requirements for Federal Information and Information Systems*, March 2006.

- FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004.

- North American Electric Reliability Corporation (NERC), *Security Guidelines for the Electricity Sector: Vulnerability and Risk Assessment*, 2002.

- *The National Infrastructure Protection Plan*, 2009.

- The IT, telecommunications, and energy sectors sector specific plans (SSPs), initially published in 2007 and updated annually.

- ANSI/ISA-99, *Manufacturing and Control Systems Security, Part 1: Concepts, Models and Terminology*, 2007 and *Part 2: Establishing a Manufacturing and Control Systems Security Program*, 2009.

- The *Advanced Metering Infrastructure (AMI) System Security Requirements*, 2008.

In a typical risk management process, assets, systems and networks are identified; risks are assessed (including vulnerabilities, impacts and threats); security requirements are specified; and security controls are selected, implemented, assessed for effectiveness, authorized, and then monitored over the lifecycle of the system. The risk assessment process for the Smart Grid will be completed when the security requirements are specified. These requirements will be selected on the basis of a risk assessment and will apply to the Smart Grid as a whole. The requirements will not be allocated to specific systems, components, or functions of the Smart Grid. In specifying the security requirements, all gaps will be identified. The implementation, assessment and monitoring of security controls are applicable when a system is implemented in an operational environment. The output from the Smart Grid risk management process should be used in these steps. In addition, the full risk management process should be applied to legacy systems and when Smart Grid owners and operators implement new systems or augment/modify existing systems.

The tasks within the cyber security strategy for the Smart Grid are being performed by participants in the NIST-led Cyber Security Coordination Task Group (CSCTG). Representatives from the private and public sectors, regulatory bodies, and federal agencies participate in the CSCTG. The CSCTG is developing a NIST Interagency Report (NISTIR): Smart Grid Cyber Security Strategy and Requirements. In addition, the CSCTG is coordinating activities with the Advanced Security Acceleration Project – Smart Grid. The ASAP-SG is a collaborative effort between EnerNex Corporation, multiple major North American utilities, the National Institute of Standards and Technology (NIST), and the U.S. Department of Energy (DOE), including resources from Oak Ridge National Laboratory and the Software Engineering Institute of Carnegie Mellon University.

Following are the tasks that are being performed by the CSCTG in the implementation of the cyber security strategy. Also included are the deliverables for each task. Because of the time frame for developing the document, the tasks listed below will be performed in parallel, with significant interactions among the groups addressing the tasks. (These tasks are not listed in priority order—task 1 is near completion, and tasks 2 and 3 are being worked on in parallel)

1. Selection of use cases with cyber security considerations.[49]

The use cases were selected from several existing sources, e.g., IntelliGrid, Electric Power Research Institute (EPRI), and Southern California Edison (SCE). The set of use cases provides a common framework for performing the risk assessment, developing the security architecture, and selecting and tailoring the security requirements. Because of the compressed time frame to complete the work, many of the tasks are being performed in parallel.

2. Performance of a risk assessment of the Smart Grid, including assessing vulnerabilities, threats and impacts.

The risk assessment, including identifying vulnerabilities, impacts and threats will be done from both a high-level overall functional perspective and a focus on the six functional priority areas that are the focus of this framework and roadmap report. The output will be used in the selection of security requirements and the identification of security requirements gaps. The initial draft list of vulnerability classes[50] was developed using information from several existing documents and Web sites, e.g., NIST SP 800-82 and the Open Web Application Security Project (OWASP) vulnerabilities list. These vulnerability classes will be used in ensuring that the security controls address the identified vulnerabilities. The vulnerability classes may also be used by Smart Grid implementers, e.g., vendors and utilities in assessing their systems.

Both top-down and bottom-up approaches are being used in implementing the risk assessment. The top-down approach focuses on the use cases and the overall Smart Grid functionality. The bottom-up approach focuses on well-understood problems that need to be addressed, such as authenticating and authorizing users to substation IEDs, key management for meters, and intrusion detection for power equipment. Also, interdependencies among Smart Grid domains/systems will be considered when evaluating the impacts of a cyber or physical security incident. An incident in one infrastructure can cascade to failures in other domains/systems.

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

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

3. Development of a security architecture linked to the Smart Grid conceptual reference model.

The first phase in this task is to assess and revise the six functional priority areas with logical interfaces. The information that is communicated across each interface is specified. Also, implementation constraints and issues are specified for each interface and the confidentiality, integrity, and availability impact levels are defined. After all the logical interfaces across all the priority areas have been identified, each interface will be allocated to one of the logical interface categories based on similarity of networks, constraints, and types of information. Some examples are: control systems with high data accuracy and high availability, as well as media and compute constraints; B2B connections, interfaces between sensor networks and controls systems; and interface to the customer site. For each logical interface category, constraints, issues, and impacts will be selected using the information provided for each individual interface. This information will be used in the selection and tailoring of security requirements— task 4 below.

This Smart Grid conceptual reference model, described in Chapter 3, provides a common view that is being used to develop the Smart Grid security architecture. The Smart Grid security architecture will overlay this conceptual architecture and security requirements will be allocated to specific domains, mission/business functions and/or interfaces included in the Smart Grid conceptual reference model. Alternatively, some security requirements, such as the policy requirements, will be allocated to the entire Smart Grid. (Note: this task has not been initiated; therefore, how the security requirements will be allocated has not been finalized.) The objective is to ensure that cyber security is addressed as a critical cross-cutting requirement of the Smart Grid.

4. Specification and tailoring of security requirements to provide adequate protection.

There are many requirements documents that may be applicable to the Smart Grid. Currently, only the North American Electric Reliability Corporation (NERC) Critical Infrastructure Protections (CIPs) are mandatory for a specific domain of the Smart Grid. The following documents have been identified by members of the CSCTG as having security requirements relevant to one or more aspects of the Smart Grid:

The following standards are directly relevant to Smart Grid

- NERC CIP 002, 003-009
- IEEE 1686-2007, *IEEE Standard for Substation Intelligent Electronic Devices (IEDs) Cyber Security Capabilities*
- AMI System Security Requirements, 2008
- *UtilityAMI Home Area Network System Requirements Specification,* 2008
- IEC 62351 1-8, Power System Control and Associated Communications—Data and Communication Security

The following documents are applicable to control systems:

- ANSI/ISA-99, *Manufacturing and Control Systems Security, Part 1: Concepts, Models and Terminology* and *Part 2: Establishing a Manufacturing and Control Systems Security Program*
- NIST Special Publication (SP) 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems*, August 2009
- NIST SP 800-82, *DRAFT Guide to Industrial Control Systems (ICS) Security*, September 2008
- DHS Procurement Language for Control Systems
- ISA SP100, *Wireless Standards*

Because the impact of a security compromise may vary across the domains and interfaces of the Smart Grid, security requirements from different baselines in NIST SP 800-53 will be considered. For example, in the federal government, FIPS 199 identifies three impact levels; low, moderate and high. The impact is based on the potential impact of the security breach of confidentiality, integrity, and availability. FIPS 200 establishes the minimum security requirements for federal information and information systems. These minimum requirements are further defined by a set of baseline security controls in SP 800-53 that are based on the impact levels in FIPS 199.

The cyber security requirements in the documents listed above are not unique across the documents. To assist in assessing and selecting the requirements, a cross-reference matrix was developed. This matrix maps the requirements from the various documents listed above to the controls included in the *Catalog of Control Systems Security: Recommendations for Standards Developers*, published by the Department of Homeland Security in 2008. The security requirements included in the catalog document are the base for the development of the specific cyber security controls for the Smart Grid. The requirements in the catalog are at a high level and will need to be tailored for the specific needs of the Smart Grid. Included in the NISTIR are the AMI security requirements that were developed by the ASAP-SG project.

6.5 Time Line and Deliverables

The first installment of *Smart Grid Cyber Security Strategy and Requirements* (NISTIR 7628) is a companion document to this NIST framework document. The first draft includes the initial risk assessment documents (vulnerability classes and bottom-up analysis), the security-relevant use cases, the base set of security requirements and cross-reference of security standards, the six functional priority areas diagrams and interfaces, and the interface categories with constraints, issues and impacts. This document is being posted for public comment.

The draft of the initial sections of the report will be revised on the basis of comments received on the first draft. In addition, the second draft will include the overall Smart Grid security architecture and the security requirements. This draft also will be posted for public comment. This draft is scheduled to be published in December 2009.

The final version of the NISTIR is scheduled to be published in March 2010 and will address all comments received to date. The document will have the final set of security controls and the final security architecture.

7 Next Steps

7.1 Phase 2 – Smart Grid Interoperability Panel

The Release 1.0 Framework described by this document represents an important first step in establishing the standards needed to realize a secure and interoperable Smart Grid. However it is only the beginning of an ongoing process. Phase 2 of the NIST Plan will establish the Smart Grid Interoperability Standards Panel to provide a more permanent process with stakeholder representation to support the ongoing evolution of the Smart Grid Interoperability Framework to identify and address additional gaps, reflect changes in technology and requirements in the standards, and provide ongoing coordination of SDO efforts to support timely availability of new or revised Smart Grid standards.

The Panel will be established by the end of 2009.

7.2 Smart Grid Conformity Testing

NIST recognizes the importance of ensuring the development of a conformity assessment program for Smart Grid (SG) standards. In order to support true interoperability of Smart Grid systems and products, it is important that Smart Grid products developed to conform to standards go through a rigorous conformity testing process. NIST has laid out a program to develop a Smart Grid Conformity Testing Framework which will be developed and maintained as part of the planned Smart Grid Panel. NIST has a three-phase plan to expedite the acceleration of interoperable Smart Grid standards, and Smart Grid Conformity Testing is part of Phase III of this plan. However, in recognition of the importance of Smart Grid Conformity Testing, NIST has now moved up Smart Grid Conformity Testing to be addressed within a contract established to initiate the Smart Grid Interoperability Panel (Phase II).

In today’s standards environment, NIST understands the importance of eliminating duplication of work activities related to Smart Grid standards as well as conformity testing. It is recognized that some efforts exist today, and others are under way, to test certain SG standards. Our intention is to identify the existing programs wherever possible. Hence our first step in developing a SG Conformity Testing Framework is to perform an analysis of existing SG standards conformity testing programs. As part of the NIST contract to establish a Smart Grid Interoperability Panel, the contractor will conduct an in-depth study to identify and describe existing conformity assessment programs for existing SG products/services based on standards and specifications identified in the most recent NIST Framework Document and other NIST-identified standards. This study will consist of a survey of conformity assessment programs and shall address, in particular, conformity assessment programs for assuring interoperability and cyber security and other relevant characteristics. Descriptions of these programs shall include, but not be limited to, a survey of 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 will also identify present gaps and deficiencies in these existing conformity assessment programs.

In addition, the contractor, based on its technical expertise, will develop a report outlining the conformity assessment requirements of federal and state governments, and other relevant SG stakeholders.

The output of this scoping study will then be used to develop a framework for SG conformity testing to be used by the Smart Grid Interoperability Panel as a baseline for an ongoing conformity testing program. As mentioned above, the framework will consider maximizing use of existing conformity assessment entities and systems in use today as appropriate. It is envisioned that the Smart Grid Conformity Testing Framework will result in an organization (via the SGIP) overseeing the current Smart Grid conformity testing which exists in the industry today, recommending changes for improvements and to fill gaps, and working with current standards bodies and user groups to develop new test programs to fill voids where they exist. This Smart Grid Conformity Testing Framework will serve as an oversight group and coordination advisor of all the current individual testing programs within the Smart Grid ecosystem.

Another important aspect of the Smart Grid Conformity Testing Framework will be to work with SDOs and other relevant bodies to provide a feedback mechanism to these groups. Throughout the normal conformity testing process, errors, clarifications and enhancements are typically identified to existing standards. It is critical that an overall process is incorporated to ensure changes and enhancements are made continuously in order to improve interoperability.

NIST intends that the first Conformity Assessment Framework Organizational Coordination Meeting be held within the SGIP by February 15, 2010. Invited attendees will include the Smart Grid stakeholders but the meeting will be open and advertised to the general public.

7.3 Other Issues that Must be Addressed

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

7.3.1 Affordability and Availability of Standards and Design Information

Interoperability in the Smart Grid requires the ability for vendors of products and services to independently implement designs that will result in the ability to interwork with equipment developed by others. This requires that their equipment be based on open standards from SDOs and user interoperability agreement specifications from user groups.

In this regard, ready access to standards and design material is essential. The Smart Grid is anticipated to be based on many standards. Access to the latest standards and user agreements by system developers including during development, is of key importance to the development of interoperable equipment.

During the 1980s there was significant competition between standards developed in the international standards community (OSI standards) and those of the Internet (IETF standards). Free and ubiquitous access to IETF Request For Comments (RFCs) and working source code enabled a highly accelerated degree of interoperation in the absence of a formal certification regime. Although the international standards are more capable, extensible, and well-developed, the difficulty of obtaining this kind of support is a factor weighing against its success in the marketplace.

This is especially true for small business, where entrepreneurs, and, in larger businesses intrapeneurs, aggressively pursue rapid development opportunities. In order to capitalize on the opportunity for rapid development of innovative products, while leveraging the substantial depth and consensus work of the SDOs, it is desirable to facilitate access to standards and related user agreements in a way comparable to the Internet model.

Initial conversations with SDOs are exploring approaches that seek to make draft standards available at affordable cost to collaborators on the Smart Grid.

Additionally, the following concepts might be pursued:

> In conjunction with the Conformity Assessment Framework part of NIST's Phase III plan, test vectors and reference test implementations and tools can be made available as open source for developers' usage . (Note this allows for rapid development but there might be certification requirements that are not without cost.)
>
> User's guides can be contracted that paraphrase standards to provide condensed materials for implementers to use. This approach has been used in several of the Smart Grid standards to date, such as ANSI C12.19.
>
> SDOs can arrange for critical Smart Grid standards to be freely publicly available, such as with many of the IEEE 802 standards.
>
> User groups such as UCA International can arrange for standards under development to be made available to its user communities that are working on implementations of the standard and/or resolving technical issues and developing implementation agreements.
>
> Organizations or governments may procure and make available critical standards through bulk purchases or, sometimes, through agreements as a result of developing contributions to the SDO.

7.3.2 Electromagnetic Disturbances

When we consider electromagnetic disturbances, we are including severe solar (geomagnetic) storm risk and Intentional Electromagnetic Interference (IEMI), threats including High-Altitude Electromagnetic Pulse (HEMP).

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

7.3.3 Electromagnetic Interference

Another example of a standards issue requiring study is the plethora of communications technologies being employed by the smart meter manufacturers, both wired and wireless. There are also proposals for new approaches, such as the Utility Telecom Council's proposal for the allocation of dedicated spectrum for utility communications. It is appropriate that multiple standards be supported to meet different real-world requirements and is in keeping with Congress's requirement that the NIST Interoperability Framework be technology neutral to encourage innovation. However, some communications technologies perform better in some environments than others, and little guidance is available to utilities to inform their technology choices. NIST identified the potential for wireless interference with some wireless meters operating in the unlicensed frequencies as an important issue to be addressed and is working closely with the FCC and DOE to study these issues and develop recommendations. These issues will require study in order to develop recommendations and guidance on appropriate standards and technologies for wireless smart meter communications. The goals in studying this issue will be to clearly define potential interference problems, to offer the best technical guidance to mitigate interference, and to fill any standards gaps identified.

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

In addition to the wireless transmitters discussed above, electromagnetic interference sources include electrostatic discharge, fast transients, and surges, which can lead to interruptions of service. The ability to withstand this interference with sufficient immunity without causing interference to other devices or systems is generally termed electromagnetic compatibility (EMC). There are significant benefits, including minimizing overall costs, to incorporating EMC up front in system development through modeling, simulation and testing to appropriate standards, including those standards discussed in section 7.3.2.. EMC standards and testing issues relating to the Smart Grid are anticipated to be addressed within the Smart Grid Interoperability Panel.

7.3.4 Privacy Issues in the Smart Grid

The vision of the Smart Grid includes dramatic increases in energy efficiency and cost savings to both utilities and consumers, with the resultant environmental benefits that come from smart energy use. Since the privacy implications of the Smart Grid are not yet fully understood, the Privacy Sub-group of the Cyber Security Coordination Task Group (CSCTG) conducted an initial Privacy Impact Assessment (PIA), as well as a broad look at the laws and regulations relevant to the privacy of information on consumers' use of electricity. The results of this analysis and the proposed next steps are included in a NIST Interagency Report (NISTIR 7628), *Smart Grid Cyber Security Strategy and Requirements* posted on the Web at the referenced link.[51]

The PIA analysis was performed in accordance with the Generally Accepted Privacy Principles (GAPP) on which most international, national and local data protection laws are based. Under GAPP, privacy is defined as "the rights and obligations of individuals and organizations with respect to the collection, use, retention, and disclosure of personal information."[52] The privacy principles reviewed were: management and accountability; notice and purpose; choice and consent; collection and scope; use and retention; individual access; disclosure and limiting use; security and safeguards; accuracy and quality; and openness, monitoring and challenging compliance.

The major benefit provided by the Smart Grid, i.e. the ability to get richer data to and from customer meters and other electric devices, is also its Achilles' heel from a privacy viewpoint. Privacy advocates have raised serious concerns[53] about the type and amount of billing and usage information flowing through the various entities of the Smart Grid, the dangers posed by data aggregation of what was considered to be "anonymized" data,[54] and the privacy implications of frequent meter readings that could provide a detailed time-line of activities occurring inside the home.

The PIA findings are that there is a "lack of consistent and comprehensive privacy policies, standards and supporting procedures throughout the states, government agencies, utility companies, and supporting entities that will be involved with Smart Grid management and information collection and use creates a very significant privacy risk that must be addressed." While NARUC has adopted[55] the "Resolution Urging the Adoption of General Privacy Principles for State Commission Use in Considering the Privacy Implications of the Use of Utility Customer Information," the CSCTG Privacy Group's research shows that few state utility commissions have begun to consider the privacy implications of the SmartGrid.

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

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

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

[53] http://www.philly.com/inquirer/business/20090906_Utilities__smart_meters_save_money__but_erode_privacy.html

[54] http://arstechnica.com/tech-policy/news/2009/09/your-secrets-live-online-in-databases-of-ruin.ars

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

7.3.5 Safety

An additional cross-cutting issue that must be addressed within the Smart Grid Interoperability Panel is role of safety in the Smart Grid, with respect to interoperability standards and conformity testing. Within standards such as those needed to support distributed energy resources including renewables, without proper attention to safety there could be situations in which utility crews or first responders are potentially exposed to live wires connected to energy storage units or local generation such as photovoltaic solar panels. These types of overall safety operating issues must be addressed in a comprehensive manner across the Smart Grid. In addition, the safety of operation of Smart Grid devices and systems, including consumer products in the home, will need to demonstrated, such as through testing by entities, including Underwriters Laboratory, Met Laboratories, and other similar organizations.

8 List of Acronyms

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

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

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

MMS	Manufacturing Messaging Specification
NAESB	North American Energy Standards Board
NARUC	National Association of Regulatory Utility Commissioners
NEMA	National Electrical Manufacturers Association
NERC	North American Electric Reliability Corporation
NIAP	National Information Assurance Partnership
NIPP	National Infrastructure Protection Plan
NIST	National Institute of Standards and Technology
NOAA	National Oceanic and Atmospheric Administration
NSA	National Security Agency
NSM	Network and System Management
OASIS	Organization for the Advancement of Structured Information Standards
OGC	Open Geospatial Consortium
OID	Object Identifier
OMG	Object Management Group
OMS	Outage Management System
OpenSG	Open Smart Grid
OSI	Open Systems Interconnection
OWASP	Open Web Application Security Project
PEV	Plug-in Electric Vehicles
PMU	Phasor Measurement Unit
QOS	Quality Of Service
RAS	Remedial Automation Schemes
RBAC	Role Based Access Control
RFC	Request For Comments, Remote Feedback Controller
RSA	Rivest, Shamir, Adelman
RTO	Regional Transmission Operator
RTP	Real-Time Pricing

RTU	Remote Terminal Unit
SCADA	Supervisory Control and Data Acquisition
SCL	Substation Configuration Language
SCP	Secure Copy Protocol
SDO	Standards Development Organization
SOA	Services Oriented Architecture
SHA	Secure Hash Algorithm
SNMP	Simple Network Management Protocol
SNTP	Simple Network Time Protocol
SP	Special Publication
SOA	Service-Oriented Architecture
SSH	Secure Shell
SSP	Sector Specific Plan
TCP	Transport Control Protocol
TFTP	Trivial File Transfer Protocol
TOGAF	The Open Group Architecture Framework
TOU	Time-of-Use
UCA	Utility Communications Architecture
UCAIug	UCA International Users Group
UID	Universal Identifier
UML	Unified Modeling Language
VAR	Volt Amps Reactive
VVWC	Voltage, Var, and Watt Control
WAMS	Wide-Area Measurement System
WAN	Wide Area Network
WASA	Wide Area Situational Awareness
XML	Extensible Markup Language