DISCLAIMER OF WARRANTIES AND LIMITATION OF LIABILITIES

THIS DOCUMENT WAS PREPARED BY THE ORGANIZATION(S) NAMED BELOW AS AN ACCOUNT OF WORK SPONSORED OR COSPONSORED BY THE ELECTRIC POWER RESEARCH INSTITUTE, INC. (EPRI). NEITHER EPRI, ANY MEMBER OF EPRI, ANY COSPONSOR, THE ORGANIZATION(S) BELOW, NOR ANY PERSON ACTING ON BEHALF OF ANY OF THEM:

(A) MAKES ANY WARRANTY OR REPRESENTATION WHATSOEVER, EXPRESS OR IMPLIED, (I) WITH RESPECT TO THE USE OF ANY INFORMATION, APPARATUS, METHOD, PROCESS, OR SIMILAR ITEM DISCLOSED IN THIS DOCUMENT, INCLUDING MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, OR (II) THAT SUCH USE DOES NOT INFRINGE ON OR INTERFERE WITH PRIVATELY OWNED RIGHTS, INCLUDING ANY PARTY'S INTELLECTUAL PROPERTY, OR (III) THAT THIS DOCUMENT IS SUITABLE TO ANY PARTICULAR USER'S CIRCUMSTANCE; OR

(B) ASSUMES RESPONSIBILITY FOR ANY DAMAGES OR OTHER LIABILITY WHATSOEVER (INCLUDING ANY CONSEQUENTIAL DAMAGES, EVEN IF EPRI OR ANY EPRI REPRESENTATIVE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES) RESULTING FROM YOUR SELECTION OR USE OF THIS DOCUMENT OR ANY INFORMATION, APPARATUS, METHOD, PROCESS, OR SIMILAR ITEM DISCLOSED IN THIS DOCUMENT.

ORGANIZATION(S) THAT PREPARED THIS DOCUMENT

Company Name

NOTE

For further information about EPRI, call the EPRI Customer Assistance Center at 800.313.3774 or e-mail askepri@epri.com.

Electric Power Research Institute, EPRI, and TOGETHER...SHAPING THE FUTURE OF ELECTRICITY are registered service marks of the Electric Power Research Institute, Inc.

Copyright © 2009 Electric Power Research Institute, Inc. All rights reserved.
CITATIONS

This report was prepared by
Electric Power Research Institute
3420 Hillview Avenue
Palo Alto, CA 94304

Principal Investigator
J. Hughes

This report describes research sponsored by the Electric Power Research Institute (EPRI) the National Institute of Standards and Technology.

This publication is a corporate document that should be cited in the literature in the following manner:

National Institute of Standards and Technology Interim Smart Grid Roadmap EPRI, Palo Alto, CA and the National Institute of Standards and Technology:2009 <Product ID Number>.
EXECUTIVE SUMMARY

TBD
# CONTENTS

1. PURPOSE AND SCOPE ....................................................................................................................... 1
2. SMART GRID VISION ....................................................................................................................... 2
3. SMART GRID HIGH-LEVEL ARCHITECTURE .................................................................................... 8
4. SMART GRID APPLICATIONS AND USER REQUIREMENTS ............................................................ 31
5. SMART GRID ARCHITECTURE AND INTERFACES ....................................................................... 34
6. SMART GRID STANDARDS GAP ASSESSMENT .............................................................................. 37
7. PRIORITIZED ACTIONS AND TIMELINES TO ADDRESS IDENTIFIED ISSUES ................. 39
8. DEFINITIONS ................................................................................................................................. 42
9. REFERENCES .................................................................................................................................. 45
LIST OF FIGURES

Figure 1: MGI's Principle Characteristics are part of their Smart Grid system vision for measuring success..........................................................5
Figure 2: Risk Management Cycle ..............................................................................11
Figure 3: Smart Grid Interface Cube ........................................................................16
Figure 4: Idealized Smart Grid Interface Cube ..........................................................17
Figure 5: An Environment Profile Selected from the Smart Grid Interface Cube.............19
Figure 6: Environments for the Smart Grid ..................................................................20
Figure 7: Relating Use Cases, Requirements, and Standards ........................................23
Figure 8: Sample Extract from Tree of Requirements Knowledge ....................................24
Figure 9: The Standards Evolution Path ......................................................................27
LIST OF TABLES

Table 1: Sample Environment Profile .........................................................................................18
Table 2: Environment Descriptions .............................................................................................20
Table 3: Cross Cutting Functions Descriptions .............................................................................21
Table 4: Architecture Principles ..................................................................................................25
Table 5: Examples of Adaptors ......................................................................................................26
Table 6: Description and Examples of Types of Standards ..........................................................26
Table 7: Sample Environment Profile for Distribution ..................................................................30
1 Purpose and Scope

1.1 Background

This document is the result of a focused project that is a part of an overall mandate laid out in the Energy Independence and Security Act (EISA) 2007 Federal Legislation. EISA States that NIST:

“…shall have 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…”

The goals of this project can be summarized as follows:

- Respond to the NIST Charter as Defined in EISA 2007
- Provide the Status of key elements of Smart Grid related Standards, Recommended Practices and Infrastructure Development
- Provide a proposed pathway to the development of a robust, open, well managed and secure infrastructure for smart grid development, deployment and life-cycle management

As an Interim Roadmap this document provides a starting point to bring the stakeholders together to work toward common goals and visions of what the smart grid needs to become. In addition this Interim Roadmap initiates some of the processes and work activities necessary to accelerate the adoption of an open infrastructure to enable the smart grid to become manifest. It should be noted that this work is intended to augment the Standards and Consortia work that is taking place across various stakeholder communities. The focus on architecture concepts also recognizes the need to see the big picture of how the smart grid infrastructure will need to become integrated not only within the power industry but across all the industries and markets that will have key roles in the development, implementation, and management of the smart grid. The smart grid will require cooperation on unprecedented levels to achieve the visions of interoperable systems that are not only supplied by hundreds of companies but can be effectively integrated, secured and managed in a way that inspires public trust and confidence.

1.2 Context of this Document

This document serves as an initial roadmap for the high-level architecture of the Smart Grid moving forward. In doing so, this document describes the principles and interface design, current status of the Smart Grid, issues and priorities for interoperability standards development and harmonization between stakeholders. This document is divided into the following major sections:

**Smart Grid Vision.** This section provides understanding as to what we consider to be the “Smart Grid”. It also gives insight into development planning and deployment of Smart Grid components including the associated organizational drivers, opportunities and challenges.
2 Smart Grid Vision

Smart Grid High-level Architecture. This section defines Smart Grid in terms of architecture from a high level including the scope, security, destinations and metrics, supporting principles and methods.

Architecture Requirements and Interfaces. This section delves into the requirements driven approach to architecting the Smart Grid and the integration between interfaces.

Smart Grid Standards and Recommended Practices Development. This section evaluates the current and emerging standards and best practices relevant to the Smart Grid, including the identification of gaps.

Prioritized Actions and Timelines to Address Identified Issues. This section discusses the NIST-focused Action Plan for resolving the gaps identified in the previous section.

1.3 NIST Role and Plans

NIST had developed a three-phase approach to expedite development of key standards for a Smart Grid, a nationwide network that uses information technology to deliver electricity efficiently, reliably, and securely. This approach will:

- Further engage utilities, equipment suppliers, consumers, standards developers and other stakeholders to achieve consensus on Smart Grid standards. This consensus-based process will deliver:
  - the Smart Grid architecture;
  - priorities for interoperability and cyber security standards, and an initial set of standards to support implementation; and
  - plans to meet remaining standards needs.
- Launch a formal partnership to facilitate development of additional standards to address remaining gaps and integrate new technologies.
- Develop a plan for testing and certification to ensure that Smart Grid equipment and systems conform to standards for security and interoperability.

Interoperability standards are needed to ensure that software and hardware components from different vendors will work together seamlessly, while cyber security standards will protect the multi-system network against natural or human-caused disruptions. By the end of 2009, NIST plans to submit these standards for review and approval by the Federal Energy Regulation Commission, which has jurisdiction over interstate distribution and sales of electric power.

2 Smart Grid Vision

This section summarizes the consensus from a variety of stakeholders on what a Smart Grid should be. It describes the destination for the technological and architectural paths that are described in this roadmap.
2 Smart Grid Vision

2.1 What is the Smart Grid

There are a great variety of definitions of a Smart Grid available. Most formal definitions tend to be based on the one found in the Energy Independence and Security Act of 2007. The example provided here is a merger of a few of those definitions.

2.1.1 A Definition

The term “Smart Grid” refers to a modernization of the electricity delivery system so it monitors, protects and automatically optimizes the operation of its interconnected elements – from the central and distributed generator through the high-voltage network and distribution system, to industrial users and building automation systems, to energy storage installations and to end-use consumers and their thermostats, electric vehicles, appliances and other household devices.

The Smart Grid will be characterized by a two-way flow of electricity and information to create an automated, widely distributed energy delivery network. It incorporates into the grid the benefits of distributed computing and communications to deliver real-time information and enable the near-instantaneous balance of supply and demand at the device level.

2.2 Smart Grid Characteristics: Drivers and Opportunities

The Smart Grid is, and will be, a dynamic system combining new ideas and functions with the many existing functions that have allowed the power system to provide electrical energy to customers for over 100 years. The known drivers for the Smart Grid, and the wide-ranging opportunities arising from the future possibilities of the Smart Grid, are all motivating the Smart Grid development to achieve the benefits envisioned.

Industry initiatives and workgroups like the Modern Grid Initiative (MGI), the IntelliGrid project, and the Gridwise Architecture Council (GWAC) have spent significant time in developing and articulating vision statements, architectural principles, barriers, benefits, technologies and applications, policies, and frameworks that help define what the Smart Grid is. This section describes some of the principle characteristics of the Smart Grid that have been widely accepted within the Smart Grid community as the underlying basis for the 21st Century grid we are striving to achieve.

2.2.1 Categories of Smart Grid Benefits

Smart Grid benefits can be categorized into 5 types:

- **Power reliability and power quality benefits**, including reduced number and length of outages, “cleaner” power, more reliable energy supply, and self-healing power systems, through using advances in digital information and control technology.
- **Safety and security benefits**, including increased visibility into unsafe or insecure situations, increased physical plant security, increased cyber security, privacy protection, and energy independence.
- **Energy efficiency benefits**, including reduced energy usage, reduced demand during peak times, reduced energy losses, and the potential to use “efficiency” as equivalent to “generation” in power system operations.
2 Smart Grid Vision

- **Energy environmental and conservation benefits**, including reducing greenhouse gases (GHG) and other pollutants, reducing generation from inefficient energy sources, increasing the use of renewable sources of energy, and replacing gasoline-powered vehicles with plug-in electric vehicles.

- **Direct financial benefits**, including lower costs, avoided costs, pricing choices for customers, and customer access to energy information.

2.2.2 Stakeholder Benefits

The benefits from the Smart Grid can be categorized by the three major stakeholders:

- **Consumer benefits**, in which consumers can better match their energy needs to the capabilities of the Smart Grid and the price of these Smart Grid services, while taking advantage of the Smart Grid information infrastructure for additional services.

- **Utility benefits**, in which utilities can provide more reliable energy particularly during challenging emergency conditions, while managing their costs more effectively through efficiency and information.

- **Societal benefits**, in which society benefits from more reliable power for governmental services, businesses, and consumers sensitive to power outage, while renewable energy, efficiency, and replacement of gasoline-powered vehicles with electrical energy minimizes the environmental impacts from carbon dioxide and other pollutants.

Often the same Smart Grid function provides benefits in all three categories, but in different ways and by different amounts. In some benefits, particularly those which directly reduce costs for utilities, customers also “benefit” from either lower tariffs or avoiding increased tariffs, although the connection may not be direct. Societal benefits are often harder to quantify, but can be equally critical in assessing the overall benefits of a particular Smart Grid function.

Other stakeholders also benefit from the Smart Grid. For instance, regulators can benefit from the transparency and audit ability of Smart Grid information, while vendors and integrators benefit from supplying the Smart Grid components and systems.

2.2.3 Modern Grid Initiative Smart Grid Characteristics

For the context of this section, characteristics are prominent attributes, behaviors, or features that help distinguish the grid as “smart”. The MGI developed a list of seven (7) principle characteristics that define the behavior of the Smart Grid. These characteristics have been widely socialized and have reached consensus agreement as recognizable features of the smart grid. The same characteristics are coincidental similar initiatives and workgroups.
The Smart Grid principle characteristics include:

- **Self-healing.** The Smart Grid independently identifies and reacts to system disturbances and performs mitigation efforts to correct them. It incorporates an engineering design that enables problems to be isolated, analyzed, and restored with little or no human interaction. It performs continuous predictive analysis to detect existing and future problems and initiate corrective actions. It will react quickly to electricity losses and optimize restoration exercises.

- **Active Customer Participation.** The Smart Grid motivates and includes customers, who are an integral part of the electric power system. The smart grid consumer is informed, modifying the way they use and purchase electricity. They have choices, incentives, and disincentives to modify their purchasing patterns and behavior. These choices help drive new technologies and markets.

- **Resilience to Man Caused and Natural Disasters and Cyber Attacks.** The Smart Grid resists attacks on both the physical infrastructure (substations, poles, transformers, etc.) and the cyber-structure (markets, systems, software, communications). Sensors, cameras, automated switches, and intelligence are built into the infrastructure to observe, react, and alert when threats are recognized within the system. The system is “hardened” and incorporates self-healing technologies to resist and react to natural disasters. Constant monitoring and self-testing are conducted against the system to mitigate malware and hackers.

- **Enhanced Power Quality and Reliability for 21st Century Loads.** The Smart Grid provides reliable power that is interruption-free. The power is “clean” and free of disturbances. Our global competitiveness demands fault-free operation of the digital devices that power the productivity of our 21st century economy.

- **Support of All Generation and Storage Options.** The Smart Grid accommodates all generation and storage options. It supports large, centralized power plants as well as...
Distributed Energy Resources (DER). DER may include system aggregators with an array of generation systems or a farmer with a windmill and some solar panels. The Smart Grid supports all generation options. The same is true of storage, and as storage technologies mature, they will be an integral part of the overall Smart Grid solution set.

- **Enable New Products, Services, and Markets.** The Smart Grid enables a market system that provides cost-benefit tradeoffs to consumers by creating opportunities to bid for competing services. As much as possible, regulators, aggregators and operators, and consumers can modify the rules of business to create opportunity against market conditions. A flexible, rugged market infrastructure exists to ensure continuous electric service and reliability, while also providing profit or cost reduction opportunities for market participants. Innovative products and services provide 3rd party vendors opportunities to create market penetration opportunities and consumers with choices and clever tools for managing their electricity costs and usage.

- **Asset Utilization and Operational Efficiency.** The Smart Grid optimizes assets and operates efficiently. It applies current technologies to ensure the best use of assets. Assets operate and integrate well with other assets to maximize operational efficiency and reduce costs. Routine maintenance and self-health regulating abilities allow assets to operate longer with less human interaction.

### 2.3 Smart Grid Challenges

The Smart Grid faces many procedural and technical challenges as it moves increasingly rapidly from the current grid with one-way power flows from central generation to dispersed loads, toward the implementation of the new, fully networked grid with two-way power flows, interacting with customers and distributed generation, and dependent upon its information infrastructure. These challenges cannot be taken lightly – the Smart Grid will fundamentally entail a different paradigm for energy generation, delivery, and use.

#### 2.3.1 Procedural Challenges

The procedural challenges are enormous, and all need to be taken into account as the Smart Grid evolves:

- **Broad Set of Stakeholders.** Unlike some other arenas, the Smart Grid will affect literally every person and every business in the United States. Although not every person will directly participate in developing the Smart Grid, the need to understand and address the requirements of these universal stakeholders will require significant efforts, from the grassroots to the White House.

- **Complexity of the Smart Grid.** The Smart Grid is a vastly complex machine, with some parts racing at the speed of light, while others moving glacially with the speed of regulation changes. Some aspects of the Smart Grid machine must be very sensitive to human conditions, while others need instantaneous, automated responses. Other portions of the Smart Grid must reflect financial pressures, while still others may conflict with corresponding environmental pressures.

- **Transition to Smart Grid.** The transition from the existing paradigm to the Smart Grid paradigm will be lengthy. It is impossible (and unwise) for all the existing “less smart” equipment and systems to be ripped out, to be replaced with “smart equipment and
systems. Therefore methods must be available to allow the “legacy” systems, equipment, and methods to be gradually and carefully transitioned to avoid unnecessary expenses or unwarranted decreases in reliability, safety, or security.

- **Ensuring Security of Systems.** Security needs to be built into the Smart Grid. Many security issues require policies, risk assessment, and training in addition to any security technologies. The development of these human-focused procedures takes time – and need to take time – to ensure that they are done correctly.

- **Consensus on Standards.** Consensus on standards across many stakeholders takes time, but the results are far better than if some technologies were just mandated – for both technical and political reasons.

- **Development and Support of Standards.** The open process of developing a standard is usually challenging and time consuming but yields a far better result and one that has benefited from the technical expertise and insights of a broad constituency. The process of supporting standards by user groups or other organizations is essential for the standards to evolve along with the needs of the stakeholders. Both of these processes serve to enable consensus.

- **Research and Development.** Not all answers are yet available on exactly what the Smart Grid is or can do. Significant effort will be needed on R&D efforts to fully understand the new requirements for fulfill the Smart Grid paradigm, and to assess the true benefits and costs as the Smart Grid evolves over time.

### 2.3.2 Technical Challenges to Achieving the Smart Grid

The technical challenges can be categorized as those associated with the following components:

- **Electronic equipment:** Electronic equipment covers all field equipment which is computer-based or microprocessor-based, including controllers, remote terminal units (RTUs), intelligent electronic devices (IEDs), and includes the actual power equipment, such as switches, capacitor banks, or breakers. It also includes equipment inside homes, buildings and industrial facilities. This embedded computing equipment must be specified robustly to handle future applications for many years without being changed out. The equipment specification must be robust from the start.

- **Communication systems:** Communication systems cover not only the media but also the different types of communication protocols. Many of these technologies are in various stages of maturity. The smart grid will need to be robust enough to accommodate new media as it emerges from the communications industries and yet still preserve interoperable, secured systems.

- **Data management:** Data management covers all aspects of collecting, analyzing, storing, and providing data to users and applications, including the issues of data identification, validation, accuracy, updating, time-tagging, consistency across databases, etc. Often data management methods which work well for small amounts of data can fail or become too burdensome for large amounts of data – a situation common in distribution automation and customer information. Data management is probably the most time-consuming and difficult in many of the functions and must be addressed in a way that can scale to immense levels.
3 Smart Grid High-Level Architecture

- **System integration & security**: System integration & security covers the networking and exchanges of information among multiple disparate systems. The key issues include interoperability of interconnected systems, cyber security, access control, data identity across systems, messaging protocols. Cyber security issues, including risk assessment are critical to address and must become appropriately integrated with real time operations of equipment. This makes security in control environments challenging.

- **Software applications**: Software applications cover the programs, algorithms, calculations, data analysis, that executes everything from control algorithms to massive transaction processing. These applications are becoming increasingly sophisticated in order to solve increasingly complex problems, while demanding vastly larger amounts of accurate and timely data – a very real challenge. Software is difficult to do correctly on large scales and software engineering is still emerging as a discipline. The amount of software needed by the smart grid is immense and will be challenging to apply the rigor necessary across multiple systems and components.

3 Smart Grid High-Level Architecture

This section describes the scope and key attributes of architecture for the Smart Grid and the processes necessary to achieve it. The attributes are described in terms of principles, metrics, environments and functions. Interoperability is an overarching principle that profoundly impacts the architecture. One key cross cutting function is security. The process of achieving the architecture is described in terms of governance, methodologies and tools.

A key purpose of the Smart Grid Interim Roadmap is to provide an initial path for developing the high-level architecture.

3.1 Architecture Definition

The following definition is from the Federal Enterprise Architecture Framework:

Architecture: the structure of components, their interrelationships, and the principles and guidelines governing their design and evolution over time.[8]

This definition appears to be robust enough to encompass the development of the Interim Smart Grid Roadmap.

3.2 Architecture Scope

The scope of the Smart Grid architecture encompasses the full range of computing and communications environments, components, interfaces and standards implemented for the following:

- Independent System Operator (ISO) / Regional Transmission Organization (RTO) interactions
- Reliability coordinator applications
- Markets and balancing authorities
3 Smart Grid High-Level Architecture

- Transmission and distribution management systems
- Transmission, distribution and feeder protection, monitoring and control
- Advanced applications and system models
- Wide area system visualization
- Enterprise systems integration
- Electric transportation support
- Distributed generation
- Asset management
- Energy storage
- Building automation integration
- Advanced metering and Demand Response
- Consumer and appliance interfacing devices and applications

The scope also includes cross cutting requirements such as: security, network management, data management, and application integration.

3.3 Security Methodology and Framework

For the Smart Grid Roadmap, the methodology and framework for addressing security risk management will be through identifying vulnerabilities and assessing the impacts of security compromises. With this approach, the probability of security threats actually occurring, which would be nearly impossible to quantify, is not included in the risk assessment except as an assumption that indeed these threats are real and likely in some form or another. Based on these vulnerabilities and impacts, a set of security controls will be identified.

3.3.1 Risk Management

Risk management is the key to matching appropriate security measures to the level of threat that each information system and information exchange is vulnerable to. Over-application of security measures can be self-defeating particularly for control systems where performance and safety are critical. Therefore each information component (database, exchange, equipment) needs to be assessed as to the impact of security compromises and to the degree they are vulnerable to those compromises.

Although NIST SP800-39 and NIST SP800-53 address risk management, their risk management frameworks are not directly applicable to many aspects of the Smart Grid. NIST SP800-82 does address the risk management of Industrial Control Systems as follows: “Because every organization has a limited set of resources, organizations should perform a risk assessment for the ICS systems and use its results to prioritize the ICS systems based on the potential impact to each system. The organization should then perform a detailed vulnerability assessment for the highest-priority systems and assessments for lower-priority systems as deemed prudent/as resources allow. The vulnerability assessment will help identify any weaknesses that may be
present in the systems that could allow the confidentiality, integrity, or availability of systems and data to be adversely affected, along with the related cyber security risks and mitigation approaches to reduce the risks.” It also notes that using standard vulnerability assessment tools on ICS networks can be dangerous because ICS functions are real-time and these vulnerability tools can actually become inadvertent security compromises.

### 3.3.2 Security Vulnerabilities

The Smart Grid information infrastructure has many vulnerabilities – far more than the older, relatively isolated, mechanically-managed power system of the past. These vulnerabilities stem from the threats to the information infrastructure, as well as from the security measures themselves.

NIST SP800-82 identifies and categorizes certain Industrial Control Systems (ICS) vulnerabilities into:

- Policy and Procedure Vulnerabilities
- Platform Configuration Vulnerabilities
- Platform Hardware Vulnerabilities
- Platform Software Vulnerabilities
- Platform Malware Protection Vulnerabilities
- Network Configuration Vulnerabilities
- Network Hardware Vulnerabilities
- Network Perimeter Vulnerabilities
- Network Monitoring and Logging Vulnerabilities
- Communication Vulnerabilities
- Wireless Connection Vulnerabilities

Security measures that have been implemented to counter the threats can cause vulnerabilities of their own. These can include:

- Employees by-passing security measures for convenience (sharing passwords) or due to job requirements (such as breaking a lock to get into a substation)

- Security measures impacting the performance of the power system (such as requiring lengthy authorization steps to trip a breaker), thus acting as a threat that could be exploited.

- Security measures preventing critical, but unexpected information from reaching authorized users.

### 3.3.3 Security Impacts

The loss or compromise of Smart Grid equipment, systems, and communication networks can vary from having extremely severe consequences (wide scale power outages or large groups of customers having their privacy violated) to moderate and negligible consequences. Because of the complexity and interconnectedness of the Smart Grid information infrastructure, the actual impact of a specific loss or compromise may be difficult to determine (the loss of a horseshoe nail can cause the loss of a war). However, methods to understand the degree impact can be
3 Smart Grid High-Level Architecture

developed, using prior efforts by different security standards groups, including NIST, NERC, the IEC, etc.

3.3.4 Security Management and Security Controls

The security management procedure for the information infrastructure consists of a cycle of:

- Risk assessment of the information and development of the security requirements
- Security policy establishment and selection of security controls necessary to meet the security requirements
- Deployment of the selected security controls
- Training in the security policies and control
- Auditing of the security activities
- Re-assessment of the risks, vulnerabilities, and thus the revising of the security requirements and controls.

Security controls or security measures are the actual steps taken to implement security. NIST SP800-53 identifies 17 types of security controls, categorized into 3 areas:

- Security Management
  - Planning
  - Risk Assessment
  - System and Services Acquisition
  - Security Assessment and Authorization
- Operational Security
  - Awareness and Training
  - Contingency Planning
  - Configuration Management
  - Media Protection
  - Physical and Environmental Protection
  - System and Information Integrity
  - Personnel Security (and Safety)
  - Maintenance
  - Incidence Response
- Technical Security
  - Identification and Authentication
  - Access Control

Figure 2: Risk Management Cycle
After the security requirements have been determined, the next step in implementing security controls is to select which types of controls are necessary for each security domain. For the Smart Grid, this will entail more complex analysis than for the government systems addressed in NIST SP800-53.

### 3.4 Architecture Destinations and Metrics

Having a clear initial vision of where the roadmap should take the industry will help focus today’s efforts. The characteristics that represent the qualities of a smart grid in the future are not present today. The following discussion is to identify the destinations for the technologies, policies and architecture that if achieved will enable the visions of smart grid.

The Smart Grid technical foundations and open standards must be mature, well supported, integrated, scalable, and extensible and truly enabling or the Smart Grid will fail to meet its most fundamental charter—supporting the development of not only immediate needs but the future development of advanced applications by generations to come. In addition to the technical disciplines to specify, develop, design, procure, and manage systems, the Smart Grid components must be built on an infrastructure that is as correct and robust as possible.

The following items represent a vision for the “destinations” of where the “Roadmap” should take the industry:

**Requirements Are Mature and Valid**

Requirements that lay out the functions and applications of the smart grid are foundational to the smart grid. Requirements define what the smart grid is and does for all the stakeholder communities. Requirements must be complete as possible out the outset. The following are some of the key requirements destinations.

- Industry policies and rules of governance are well developed, mature, and can be consistently applied across the industry.
- Requirements are well-developed by domain experts and well documented following mature systems-engineering disciplines.
- Requirements not only include support for the applications but are also well developed for the management of systems as well as security.

**Well-Developed Standards Are in Place**

Standards are critical to enabling interoperable systems and components. Mature standards are the foundation of mature markets for the millions of components that will have a role in the future smart grid. Standards enable components to be constructed by thousands of companies as well as enabling consistency in systems management and maintenance over the life-cycles of components. Metrics can be further developed around the following destinations for standards:

- Open stable and mature industry-level standards from recognized standards development organizations (SDOs) are available.
3 Smart Grid High-Level Architecture

- Standards are 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.
- The standards were thoroughly evaluated both from focused technical review as well as through the development of reference designs and implementations that were subsequently tested rigorously.
- Standards are robust and can be extended as necessary to meet future requirements and applications as needs arise.
- There is a mechanism in place such as a user group to support and evolve the definition of the standard as the requirements of the stakeholders evolve.
- Standards conformance testing suites are thorough and are complemented with interoperability and performance testing suites.

Architecture and Infrastructure Have Been Validated by Users and the Larger Domain

Architecture provides the overall technical and management infrastructure for smart grid technologies. Architecture(s) must be well defined, documented and robust to assist in technical and management governance in addition to directing ongoing development work. Architecture concepts in particular are necessary to integrate technical and non technical oversight and governance of the smart grid infrastructure. The following are a few of the destinations for architecture concepts:

- Architecture artifacts include well-defined interfaces across industries external to the utility industry. The architecture also uses up-to-date system-modeling tools to manage the documentation and complexity of the system.
- Active consortia known as standards “user groups” assist in defining how to apply the standard for utility applications, as well as supporting standards conformance testing and quality assurance processes.
- The research and development results have been focused on the right topics and the results are in now and have solved some of the long time lingering infrastructure issues in critical areas.
- The architecture is robust for supporting power engineering and mission-critical systems through massively scaled, well-managed and secure networks for at least 30 years.
- The infrastructure is mature enough to support hundreds of companies building products that not only interoperate but appropriately integrate into the management and security infrastructures.
- Workforces are educated and developed and can support all aspects of the lifecycle of Smart Grid systems. University curricula cover specializations in “Complex Systems Architecture.”
- Equipment and components of the Smart Grid can be procured from well-defined specifications that make use of mature architecture and requirements documents as well as systems models and associated graphics.

3.5 Smart Grid Development Governance

The Smart Grid is recognized as a key strategic infrastructure need for consumers, utilities, regional transmission offices, and the country. Whether Smart Grid deployments are being
driven by legislative and regulatory policies, realizing operational efficiencies, or creating customer value, the motivation and pressure to produce has caused the industry to perform Smart Grid implementations in fragmented efforts with limited or no industry coordination or agreed-upon standards. The concern is that as the technology and interoperability standards mature and gain consensus, some early adopters may be faced with “sunk costs” or, at the very least, some serious integration and interoperability issues going forward.

According to a recent article in SmartGridNews.com[5] authored by the Open Smart Grid Subcommittee and the Utility Smart Grid Executive Working Group, there are three challenges facing broad Smart Grid standards adoption. (Open Smart Grid Subcommittee of the Utility Communication Architecture International Users Group and The Utility Smart Grid Executive Working Group, 2009)

1. The large number of stakeholders, different considerations, number and complexity of standards available (and missing) requires a more formal nationally-driven governance structure.
2. Since Smart Grid efforts are underway, and in some cases complete, standards adoption must consider work already completed and underway.
3. Interoperability discussions and definitions should be expanded to focus on standards across systems (inter-system) rather than just within systems (intra-system).

The industry can clearly benefit from developing governance rules for ensuring a secure, intelligent, interoperable, and fully-connected smart grid. In particular, agreement on a set of Smart Grid standards will enable Smart Grid vendors and implementer’s common rules and specifications for developing systems and devices that ensure interoperability beyond a single project or deployment. In fact, many of the baseline standards for Smart Grid already exist. The challenge is in getting industry “buy-in” from stakeholders and prioritizing key grid interoperability standards quickly. Industry-funded organizations and workgroups such as the GridWise Architecture Council, Open Smart Grid (OpenSG) Subcommittee of the Utility Communications Architecture International Users Group (UCAIug) have performed much of the “heavy lifting” in creating awareness, engaging a large cross section of stakeholders, and identifying and refining some of the Smart Grid interoperability standards.

NIST has the opportunity to dramatically accelerate consensus for adoption of key Smart Grid interoperability standards. NIST, along with DOE joint participation, will develop a formalized governance process to identify and select Smart Grid standards adoption for the U.S. The governance model for Smart Grid standards adoption should include key stakeholder representatives, including:

- Utilities
- RTOs/ISOs
- Smart Grid vendors
- Legislators
- Consumer Advocacy Groups
- Standards organizations
- Industry organizations and technical advisory workgroups
Feedback from industry stakeholders suggests that a successful NIST governance process will include the following characteristics:

- In general, the governance model must promote participation, openness, industry consensus, accountability, and transparency. It must prioritize and address standards adoption based on existing industry consensus and need.
- The Domain Expert Working Groups (DEWGs) must be inclusive, and embrace open participation, providing transparency to the efforts they are working on, and encouraging collaboration from the stakeholders.
- Standards candidate identification and selection criteria processes must be open, unbiased, formally documented, and published in a public, free of charge web site.
- Standards selection workshops and summits must be planned in advance with general announcements to stakeholders and other interested parties. Workshop and summit decisions and results will be documented and published in a free, public location.

### 3.6 Smart Grid Interfaces

This section provides an overview of the communications interfaces that will be described in this roadmap, and how they are organized. There are many ways to look at interfaces. For example, communications protocol experts often refer to the interfaces between layers in the Open Systems Interconnection -- Basic Reference Model (OSI) \[4\]. Of course there are interfaces between people, organizations, devices and other machines. Within organizations, there are interfaces between applications and business processes. Less obvious, but vital, are the hidden interfaces between security domains, ownership boundaries, and network segments.

In the Smart Grid, what will actually be built are the devices, networks, and software applications which make use of these interfaces. Networks are built from hardware and software that can provide a set of services i.e. that can fulfill specific requirements, with specific qualities of service. Networks are not deployed based on devices. Instead, devices are built and selected to reside on networks. For the Smart Grid, we want devices to expose and enforce interfaces. Therefore, we must define the interfaces first.

Given the various definitions of interfaces that are possible, this roadmap uses those that are helpful in selecting standards. We use interfaces as a valuable organizing principle around which to construct the lists of standards that will define portions of the Smart Grid. Specifically, we recognize that interfaces in the Smart Grid have three unique dimensions:

- They connect and are located in different distributed computing environments, termed Environments.
- They fulfill a set of common requirements for a robust infrastructure, termed Cross-Cutting Functions.
- They must address a variety of uses and applications of the Smart Grid

And so, we have devised the Smart Grid Interface Cube to illustrate this dimensionality of the problem, as shown in Figure 3.
As stated, the Cube is arranged to expose three relatively orthogonal dimensions of interfaces that can be used to describe Smart Grid Standards:

- Environments. (Horizontal Axis) This term and the list of environments are based on the list of environments defined in the IntelliGrid Architecture project [1], and the NIST Domain Expert Working Groups (DEWGs). [ reference ]

- Cross-Cutting Functions (Vertical Axis). This term and the list of functions are derived from the layers of the GWAC model [3], and the

- Applications (Depth Axis). There are a variety of different uses and applications of the Smart Grid, the most critical ones are listed in Chapter 4 are just a few examples, starting with those that have been identified as priorities by FERC [7].

Each intersection in the cube represents an interface at which a standard may be applied. As one moves through the cube, one crosses various interfaces, and can expect to come across appropriate standards for use in implementing information flows across these interface boundaries.

When moving through the cube, one encounters different standards for performing similar functions. Sometimes the use of a different standard is justified, when the requirements satisfied by the different standards are also different. However, using different standards creates an incompatibility gap that must be resolved.
The typical solution for closing such gaps is to deploy an “adaptor” that fills in the mismatch between requirements. There are a variety of different kinds of adaptors, from bridges and routers to convertors and gateways, depending on which interface is being adapted. The fewer the mismatches between communications requirements, and the more agreement on standards, the less frequent and complex the adaptors will have to be.

Ideally, a very successful Smart Grid Roadmap would require the barest minimum of such adaptors. Where needed, they would preferably be fairly simple devices that would not require much configuration or maintenance. One would hope to achieve the version of the “cube” identified in Figure 4: Idealized Smart Grid Interface Cube.

Figure 4: Idealized Smart Grid Interface Cube

Referring to this figure, you can see that no transition between standards is necessary when moving information within the solid planes. Only the Connectivity and Information models have a diversity of boundaries – and hence standards. This is as one might expect. It should be possible to have information flow across physical boundaries – like wireless to Ethernet with only simple adaptors. This implied homogeneity of capabilities allows for gateway-less communications from device to device and application to application.

We now discuss these dimensions in greater detail.

3.6.1 Environment Profiles

In the end, the Smart Grid Interim Roadmap seeks to identify candidate standards for the Smart Grid. Since no single standard is all encompassing of the needed capabilities, sets of standards
are needed. Additionally, it makes sense that the standards that are pervasive in the customer premises may be significantly different from those in an electrical substation where sub-millisecond performance is demanded. The Smart Grid Interface Cube suggests that using a variety of standards makes most sense when organized along the horizontal (x) axis – that is, Environments.

Therefore, this document contains Environment Profiles of standards (sets of Standards for each communications layer)\(^1\). Analyze the fit of the suite to the requirements of the applications via Use Cases and you have defined the Smart Grid.

Table 1: Sample Environment Profile illustrates what an Environment Profile looks like. It represents a “slice” through the Smart Grid Interface Cube for one particular environment, as illustrated in Figure 5: An Environment Profile Selected from the Smart Grid Interface Cube.

It is the goal of the Interim Roadmap project to paint a picture of what these Environments will look like and how they can optimally meet the requirements of the Smart Grid. It is the goal of the analysis techniques described in section 3.9 Analysis Process Methodology to provide a concrete justification for these selections.

Table 1: Sample Environment Profile

<table>
<thead>
<tr>
<th>Environment:</th>
<th>&lt;Name&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interfaces:</td>
<td>Standards</td>
</tr>
<tr>
<td>· Domain-specific Interfaces</td>
<td></td>
</tr>
<tr>
<td>– Object models</td>
<td>&lt;Standard&gt;</td>
</tr>
<tr>
<td>– Application models</td>
<td>&lt;Standard&gt;</td>
</tr>
<tr>
<td>– Application models</td>
<td>&lt;Standard&gt;</td>
</tr>
<tr>
<td>– Application models</td>
<td>...</td>
</tr>
<tr>
<td>· Cross-cutting</td>
<td></td>
</tr>
<tr>
<td>– Information Model</td>
<td>&lt;Standard&gt;</td>
</tr>
<tr>
<td>– Application Services</td>
<td>&lt;Standard&gt;</td>
</tr>
<tr>
<td>– Security</td>
<td>&lt;Standard&gt;</td>
</tr>
<tr>
<td>– Network Management</td>
<td>&lt;Standard&gt;</td>
</tr>
<tr>
<td>– Configuration management</td>
<td>&lt;Standard&gt;</td>
</tr>
<tr>
<td>– Time Synchronization</td>
<td>&lt;Standard&gt;</td>
</tr>
<tr>
<td>– Networking</td>
<td>&lt;Standard&gt;</td>
</tr>
<tr>
<td>– Connectivity</td>
<td>&lt;Standard&gt;</td>
</tr>
</tbody>
</table>

\(^1\) Note: Another organization might be by cross-cutting interface. The reason this would be problematic is that a particular Standard may address more than one Interface. Additionally, several Standards may naturally combine to address a single Cross-Cutting Interface.
3.6.2 Environments

The scope of smart grid development encompasses a variety of different distributed computing and communications environments. These environments range from real-time environments with utility protection equipment to e-commerce and business environments. Many of the standards today are targeted to one or more of these environments.

Environments, a term having many meanings in different contexts, were defined in the IntelliGrid [1] project to identify sets of requirements, and hence, standards with capabilities that could satisfy a set of Use Cases.
3 Smart Grid High-Level Architecture

Figure 6: Environments for the Smart Grid

The term Environments, defined this way, is particularly useful because once defined, it makes the specification of its portion of the infrastructure clear. In essence, Environments are an updating of the concept of “profiles” used in earlier similar activities historically to describe communications stacks. For the purposes of the Smart Grid Roadmap, we focus on a smaller list the Environments as shown in Table 2, this mapping is approximate.

Table 2: Environment Descriptions

<table>
<thead>
<tr>
<th>Smart Grid Interface Cube</th>
<th>NIST Domain Expert Working Groups</th>
<th>IntelliGrid Environments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transmission</td>
<td>TnD</td>
<td>1 High-speed Intra-substation</td>
</tr>
<tr>
<td>Transmission</td>
<td>TnD</td>
<td>2 High-speed Inter-substation</td>
</tr>
<tr>
<td>Transmission</td>
<td>TnD</td>
<td>3 High Security Intra-substation</td>
</tr>
<tr>
<td>Distribution</td>
<td>TnD</td>
<td>4 Inter-Field Equipment</td>
</tr>
<tr>
<td>Transmission</td>
<td>TnD</td>
<td>5 Critical Data Acquisition and Control</td>
</tr>
<tr>
<td>Distribution</td>
<td>TnD</td>
<td>6 Non-Critical Data Acquisition and Control</td>
</tr>
</tbody>
</table>

Note that the others are also relevant and can be represented by differences to the main ones.
3 Smart Grid High-Level Architecture

<table>
<thead>
<tr>
<th>Smart Grid Interface Cube</th>
<th>NIST Domain Expert Working Groups</th>
<th>IntelliGrid Environments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enterprise</td>
<td>TnD</td>
<td>7</td>
</tr>
<tr>
<td>Enterprise</td>
<td>TnD</td>
<td>8</td>
</tr>
<tr>
<td>E-Commerce</td>
<td>BnP</td>
<td>9</td>
</tr>
<tr>
<td>E-Commerce</td>
<td>BnP</td>
<td>10</td>
</tr>
<tr>
<td>E-Commerce</td>
<td>C2U</td>
<td>11</td>
</tr>
<tr>
<td>E-Commerce</td>
<td>I2G, BnP</td>
<td>12</td>
</tr>
<tr>
<td>Enterprise</td>
<td>I2G, BnP</td>
<td>13</td>
</tr>
<tr>
<td>E-Commerce</td>
<td>I2G</td>
<td>14</td>
</tr>
<tr>
<td>Transmission</td>
<td>TnD</td>
<td>19</td>
</tr>
<tr>
<td>Distribution</td>
<td>TnD</td>
<td>20</td>
</tr>
</tbody>
</table>

3.6.3 Cross-Cutting Functions

In the presentation the Gridwise Architecture Council (GWAC) Context Setting Framework [3], a series of Cross-Cutting Issues are presented which are essentially those “Interfaces” which in order to be useful and properly applied, need to be pervasive within the implementation space of an application. If they are not, adaptors or gateways will be required to make up the differences in the required capabilities as stated earlier.

Table 3: Cross Cutting Functions Descriptions

<table>
<thead>
<tr>
<th>Smart Grid Interface Cube</th>
<th>GWAC Interoperability Framework</th>
<th>Open Systems Interconnect Model</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information Model</td>
<td>Layer Business Procedures</td>
<td>7 Application Layer</td>
</tr>
<tr>
<td></td>
<td>Business Context</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Issue Shared Meaning of Content Resource Identification</td>
<td>6 Presentation Layer</td>
</tr>
<tr>
<td>Application Services</td>
<td>Layer Semantic Understanding</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Issue Transaction &amp; State Mgmt</td>
<td>5 Session Layer</td>
</tr>
<tr>
<td>Security</td>
<td>Issue Security and Privacy</td>
<td>Varies</td>
</tr>
<tr>
<td></td>
<td>Logging and Auditing</td>
<td></td>
</tr>
<tr>
<td>Network Management</td>
<td>Issue System Preservation</td>
<td>Varies</td>
</tr>
<tr>
<td></td>
<td>Discovery and Configuration</td>
<td></td>
</tr>
<tr>
<td></td>
<td>System Evolution &amp; Scalability</td>
<td></td>
</tr>
<tr>
<td>Time Synchronization</td>
<td>Issue Time Synch &amp; Sequencing</td>
<td>Varies</td>
</tr>
</tbody>
</table>
3.6.4 Applications

Application specific functions consist of models of information and message content that express the essence of Smart Grid applications as implemented. Note that this dimension of the cube extends indefinitely and only a few examples are shown in the diagram. The complete list is discussed in chapter 4.

3.7 Smart Grid Infrastructure Methods and Tools

The process described herein seeks to meet the following requirements of the NIST Interim Roadmap:

- Select a set of standards targeted for the Smart Grid.
- Identify gaps in those standards to allow the definition of needed enhancements.
- Identify boundaries between standards to allow harmonization efforts to be defined and pursued.
- While perfect objectivity is a goal, never an achievement, devise an objective process around which consensus can be gathered.

The analysis process recognizes that the appropriate elements of a selection process such as this are to:

1) Identify Use Cases that impact the interfaces where standards are needed, and that illustrate how the results will be utilized
2) Derive Requirements that satisfy the Use Cases
3) Select Standards that afford the capabilities to satisfy the Requirements

This classic waterfall approach to system’s engineering is appropriate to our goals. However, in the Smart Grid Standards selection process there are on the order of 1000 existing Use Cases; with thousands of identified Requirements and hundreds of potentially appropriate Standards for selection. So to great extent, we focus on harvesting the existing knowledge and coordinating its analysis to achieve our results.

This process, therefore, begins with a collection activity to organize the most relevant materials in each category. It further correlates the Use Cases with Requirements and the Requirements with the Standards. This way, the set of Requirements can be considered building blocks with reflect the Use Cases and drive the Standards. Finally, these sets are correlated in an assessment function which identifies “goodness of fit” of the Standards to the Use Cases via the Requirements, resulting in the Environment Profiles presented in section 3.6.1.
The following figure illustrates this arrangement:

![Diagram](image)

**Figure 7: Relating Use Cases, Requirements, and Standards**

The Hierarchy of “Standardized” Requirements is used to collate Requirements from a variety of relevant sources and organize them according to type of Requirement. This effort is proposed to develop a master list of requirements from the stakeholders.

The requirements in this hierarchy include those from recommended practices, systems, software and communications engineering as well as from utility Use Cases and Requirements documents. This master collection of requirements once completed can be used as a set of metrics against which to evaluate either standards or the use cases.

Note that some Requirements are very high level. And some are very detailed.

A standards based definition of a requirement is from IEEE STD 610.12:

*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.*

Note that to be a good requirement, it must address one and only one thing, and the statement that the Requirements makes must be testable in a straightforward manner.
3 Smart Grid High-Level Architecture

In order to accommodate Requirements from varied sources, an organizational means is required. Each organization that has produced documents containing explicit Requirements has chosen a specific level of abstraction at which to relate its needs. For example, one organization may say that “it is a requirement to use open source implementations”. Another relevant requirement might be “the meter must be able to store 1 minute load profile”. Both kinds (and many more for that matter) of Requirements are relevant to the Smart Grid. How then to arrange these sets of somewhat orthogonal, and, somewhat overlapping Requirements? There is a need to recognize both the differing nature of the Requirements, as well as, their level of specificity.

The resulting organization is a tree structure. The branches are the outline heading levels, for example 1.1.2.1.1 Pricing Requirements. The Requirements, themselves, represent the leaves of the tree. The Branches and the leaves represent either recommended practices or the Requirements or should have attribution to the origin of the standard.

To analyze a given Standard to characterize what Requirements it meets:

1. Determine a list of branches that the standard addresses
2. Assess the leaves under the branches to determine whether the standard meets each requirement.
3. The list of branches and the pass/fail criteria of the nested leaves become a quantitative metric by which a standard can be analyzed.

<table>
<thead>
<tr>
<th>Branch</th>
<th>Leaves</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Applications</td>
<td></td>
</tr>
<tr>
<td>1.1 E-Commerce</td>
<td></td>
</tr>
<tr>
<td>1.2 Enterprise</td>
<td></td>
</tr>
<tr>
<td>1.3 Transmission</td>
<td></td>
</tr>
<tr>
<td>1.4 Distribution</td>
<td></td>
</tr>
<tr>
<td>1.4.1 DOMA</td>
<td></td>
</tr>
<tr>
<td>1.4.2 FLIR</td>
<td></td>
</tr>
<tr>
<td>1.5 Customer</td>
<td></td>
</tr>
<tr>
<td>1.5.0.1 AMI Requirements</td>
<td></td>
</tr>
<tr>
<td>1.5.1 H2G</td>
<td></td>
</tr>
<tr>
<td>1.5.2 B2G</td>
<td></td>
</tr>
<tr>
<td>1.5.3 V2G</td>
<td></td>
</tr>
<tr>
<td>2 Cross-Cutting Functions</td>
<td></td>
</tr>
<tr>
<td>2.1 Information Model</td>
<td></td>
</tr>
<tr>
<td>2.1.1 Device Identity</td>
<td></td>
</tr>
<tr>
<td>2.2 Application Services</td>
<td></td>
</tr>
<tr>
<td>2.3 Security</td>
<td></td>
</tr>
<tr>
<td>2.4 Network Management</td>
<td></td>
</tr>
<tr>
<td>2.4.1 Fault Management</td>
<td></td>
</tr>
<tr>
<td>2.4.2 Configuration</td>
<td></td>
</tr>
<tr>
<td>2.4.3 Accounting</td>
<td></td>
</tr>
<tr>
<td>2.4.4 Performance</td>
<td></td>
</tr>
<tr>
<td>2.5 Configuration management</td>
<td></td>
</tr>
<tr>
<td>2.6 Time Synchronization</td>
<td></td>
</tr>
<tr>
<td>2.7 Networking</td>
<td></td>
</tr>
<tr>
<td>2.8 Connectivity</td>
<td></td>
</tr>
<tr>
<td>3 General</td>
<td></td>
</tr>
<tr>
<td>3.1 Standardization</td>
<td></td>
</tr>
<tr>
<td>3.2 User Group Support</td>
<td></td>
</tr>
<tr>
<td>3.3 Demonstrations and availability</td>
<td></td>
</tr>
</tbody>
</table>

Figure 8: Sample Extract from Tree of Requirements Knowledge (prototype)
3 Smart Grid High-Level Architecture

Similar spreadsheets are constructed for Use Case analysis and Standards analysis.

3.8 Architectural Principles

This section describes the principles used to develop this roadmap and the information system architecture it is intended to produce. Architectural principles can be distinguished from characteristics of the Smart Grid by the fact that they do not describe what makes the grid “smart”, but on how it can continue to be so in the years to come.

The architectural principles listed here are summarized from those identified by the GridWise Architecture Council, IntelliGrid and UtilityAMI among other stakeholders.

Table 4: Architecture Principles

<table>
<thead>
<tr>
<th>Principle</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standardization</td>
<td>The elements of the infrastructure and the ways in which they interrelate are clearly defined, published, useful, open and stable over time.</td>
</tr>
<tr>
<td>Openness</td>
<td>The infrastructure is based on technology that is available to all qualified stakeholders on a nondiscriminatory basis. Providers of the technology have an evolution plan toward openness and standardization.</td>
</tr>
</tbody>
</table>
| Interoperability | The standardization of interfaces within the infrastructure is organized such that:  
|               |   - The system can be easily customized for particular geographical, application-specific, or business circumstances, but  
|               |   - Customization does not prevent necessary communications between elements of the infrastructure. |
| Security   | The infrastructure is protected against unauthorized access and interference with normal operation. It consistently implements information privacy and other security policies. |
| Extensibility | The infrastructure is not designed with built-in constraints to extending its capabilities as new applications are discovered and developed. Toward this goal,  
|               |   - Its data is defined and structured according to a common information model  
|               |   - It separates the definition of data from the methods used to deliver it  
|               |   - Its components can announce and describe themselves to other components |
| Scalability | The infrastructure can be expanded throughout the power system with no inherent limitations on its size. |
| Manageability | The components of the infrastructure can have their configuration assessed and managed, faults can be identified and isolated, and the components are otherwise remotely manageable. |
| Upgradeability | The configuration, software, algorithms and security credentials of the infrastructure can be upgraded safely and securely with minimal remote site visits. This is a particular aspect of manageability. |
| Shareability | The infrastructure uses shared resources which offer economies of scale, minimize duplicative efforts, and if appropriately organized, encourage the introduction of competing innovative solutions. |
| Ubiquity   | Authorized users can readily take advantage of the infrastructure and what it provides regardless of geographic or other types of barriers. |
3 Smart Grid High-Level Architecture

<table>
<thead>
<tr>
<th>Principle</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Integrity</td>
<td>The infrastructure operates at a high level of availability, performance and reliability. It re-routes communications automatically, operates during power outages, and stores data for intervals sufficient to recover from failure events</td>
</tr>
<tr>
<td>Ease of Use</td>
<td>There are logical, consistent and preferably intuitive rules and procedures for the use and management of the infrastructure. The system maximizes the information and choices available to users while minimizing the actions they must take to participate if they choose to do so.</td>
</tr>
</tbody>
</table>

3.8.1 Eliminating Adaptors

As discussed briefly in earlier sections, it is a goal of this roadmap to create a communications architecture that reduces the number of “adaptors” necessary between interfaces and standards. Adaptors come in a variety of forms, as shown in Table 5.

Table 5: Examples of Adaptors

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bridge</td>
<td>Physical layer adaptor. Operates automatically</td>
<td>Ethernet switch converting wireless network to a wired network</td>
</tr>
<tr>
<td>Router</td>
<td>Network layer adaptor. Operates automatically</td>
<td>Internet router or firewall converting a local area network to a wide area network</td>
</tr>
<tr>
<td>Algorithmic Gateway</td>
<td>Automatic application layer adaptor. Converts one complete protocol to another. Does not require configuration.</td>
<td>Front-end processor in a control center converting message bus to a SCADA protocol.</td>
</tr>
<tr>
<td>Full Gateway</td>
<td>Requires extensive configuration to map individual pieces of data to one another.</td>
<td>Data concentrator in a substation stores data from one device in a pre-configured database before sending it to a master using a different protocol</td>
</tr>
</tbody>
</table>

It is a goal of this roadmap to eliminate all adaptors as much as possible, and to select standards that facilitate simpler and more automatic adaptors rather than more complex adaptors requiring greater configuration.

3.8.2 Encouraging Standards Evolution

This roadmap recognizes that different types of standards exist on a continuum as shown in Figure 9 and that all of them may be useful. Standards from official or “de jure” organizations are preferable over other types of standards, but standards and best practices from unofficial or “de facto” may be developed more quickly. These can lead to more formally specified practices later through the process of developing contributions to SDO based standards. A preferable path is to do supportive work under user groups associated with the formal SDO’s so that there is a relationship already established. These contributions need to be made in concert with SDO rules of governance.

Table 6: Description and Examples of Types of Standards
Figure 9: The Standards Evolution Path

3.9 Analysis Process Methodology

Once the concept of Environments and Interfaces is established, the collections of Use Cases, Requirements, and Standards can be guided by their relevance to them.

Remember, we use the term Standards to represent the body of standards, technologies, and best practices for simplicity.
Here is the step by step cookbook process to achieve the goal:

1) Collection
   a. Use Cases
   b. Requirements
   c. Standards

Collect Use Cases that will be the basis of analysis. Produce a list of Use Cases and their associated documents. Use the Environments and Interfaces to guide the selection process, specifically to identify those Use Cases that “exercise” the Interfaces in different ways. Additional or non-conforming Use Cases can be collected and potentially constructed by the stakeholders/DEWGs/etc…

Assemble an initial collection of Requirements from IntelliGrid, GridWise, SCE, EnerNex, CEC, USB, EPRI, DEWGs, NIST, etc. Note we would rely on our experts and the document reviews to obtain an initial concrete list of Requirements documents. We are not looking at Use Cases here. Many organizations and projects have created concrete lists of Requirements that can be directly used. Those that have Use Cases associated with them will be used in a later step.

Categorize Requirements according to a hierarchy including general to more specific. This is the “Tree of Requirements” described in section 3.7 Smart Grid Infrastructure Methods and Tools. We would assemble the tree from the prototype by “hanging” the Requirements collected in step 1). As we populate the tree with the Requirements, we will simultaneously refine the branching so that there is a reasonable organization. Note that the branching does not have to be perfect – just logical enough to facilitate analyzing against them. In constructing the branches, recognition should be given to well-established organizing principles such as IntelliGrid, GridWise, FCAPS, etc.…

Identify all of the Standards that are pertinent to each of the Environments and Interfaces. The communication layers (physical media, network, application, security, abstract object model, etc.) to which they are applicable should be identified.

2) Preliminary analysis (What is missing)
   a. Analyze Use Cases against Requirements
   b. Analyze Standards against Requirements

At this point, some obvious gaps may be observed by inspection and these can be filled in the next activity.

3) Complete initial collection (Fill gaps discovered)
   a. Use Cases
   b. Requirements
   c. Standards
3 Smart Grid High-Level Architecture

Additional Use Cases, Requirements, and Standards can be added to the list to arrive at useful set against which to analyze.

4) Complete analysis
   a. Use Cases to Requirements
   b. Standards to Requirements

At this point, the analyses produce vectors containing Use Cases and their identified Requirements, and, Standards and their identified Requirements.

This is done in two steps – first identify the appropriate branches that pertain to a given standard. Then for each relevant branch, assess each leaf requirement against the standard. This analysis is done in a spreadsheet that has the requirements tree complemented by columns representing each Standard and check marks made relative to each branch and Requirement.

For each Use Case we analyze against the Requirements tree in similar fashion. There are expected sections of the Use Case that will correspond to the major branches of the Requirements Tree.

5) Construct Environments

Arrange “suites” of standards into environments. This should conclude several sets per environment. There is judgment at this step, but more is better since each “suite” will be analyzed and scored.

6) Construct a correlation algorithm

This will allow a numeric metric to be computed algorithmically by determining the goodness of fit of the set of Standards in the Environment profile to the Use Cases. Depending on how this is developed there might be weighting factors applied to some branches – for example a legally required branch might hold more weight then another requirement. Because this is difficult to do objectively it should be kept to a minimum and discussed so consensus can be reached on this critical algorithm.

Note that the correlation algorithm will produce numeric scores. However, interpreting those scores will have to recognize the potentially large standard deviation to be expected from the methodology. That is, relatively close scores may not clearly detect a substantive difference worthy of a conclusion. Therefore a coarse comparison of these scores is all that can be expected.

7) Compute correlation scores

Apply algorithm 6) to results of 5); the winners have the highest scores correlating the standards to the Use Cases.

8) Refine Environments to optimize contents
3 Smart Grid High-Level Architecture

This selects winning “suites” for each environment. If you then look at the correlation scores, you can determine gaps. If you study the standards in the suites you can identify where the rough spots are that need harmonization.

9) Assess remaining Requirements mismatches

Once an optimal set of Environment definitions are made, their scores can be inspected to identify which requirements were not satisfied by the capabilities of the enclosed profiles of Standards. This will identify where the Standards should be enhanced.

Reviewing the transitions between the Standards in the Environment, such as communications protocols to application protocols, etc…, as well as, the potential transitions between Environments, reveals where harmonization needs to be pursued to minimize the complexity of the transitions.

10) Describe the gaps in the Standards

Once the assessment is complete, describe the gaps in the Standards or set of Standards within different profiles in an Environment, identify the SDOs that would need to be involved to address the gaps, and discuss the relative difficulty of undertaking those efforts.

3.9.1 Sample Environment Profile

The table below illustrates what a final result can look like. It is a populated Environment Please note: The project is not asserting a conclusion here, just showing what one might look like.

Table 7: Sample Environment Profile for Distribution

<table>
<thead>
<tr>
<th>Interfaces:</th>
<th>Distribution</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Domain-specific Interfaces</strong></td>
<td><strong>Standards/Use Cases</strong></td>
</tr>
<tr>
<td>-- Applications (Supporting Use Cases)</td>
<td>D1, D2, D3, D5, C7</td>
</tr>
<tr>
<td>-- Object models</td>
<td>IEC 61850 Part 7.3, 7.4</td>
</tr>
<tr>
<td><strong>Cross cutting</strong></td>
<td></td>
</tr>
<tr>
<td>-- Information Model</td>
<td>IEC 61850 Part 7.2</td>
</tr>
<tr>
<td>-- Application Services</td>
<td>IEC 9506 (MMS) Over ACSE</td>
</tr>
<tr>
<td>-- Security</td>
<td>IEC 62351 Part 4</td>
</tr>
<tr>
<td>-- Network Management</td>
<td>IEC62351 Part 7</td>
</tr>
<tr>
<td>-- Configuration management</td>
<td>IEC 61850 Part 6</td>
</tr>
<tr>
<td>-- Time Synchronization</td>
<td>IEC 62351 Part Z</td>
</tr>
<tr>
<td>-- Networking</td>
<td>RFC 2460 IPV6 (may list some others here too)</td>
</tr>
<tr>
<td>-- Connectivity</td>
<td>IEEE 802.xxx 1G Ethernet over copper or fibre</td>
</tr>
</tbody>
</table>
4 Smart Grid Applications and User Requirements

4.1 Introduction to Smart Grid Applications and User Requirements

Acknowledge the wide range of Use Cases, but quickly narrow them down to those the help define the characteristics of the key interfaces (which will be identified as Environments in the next section).

- Each section will cover:
  - Range of user applications
  - Selection of key user applications and data exchange requirements that “challenge” the interfaces
  - Identification of key user requirements that can be used to define the interface requirements

4.2 Markets Applications and User Requirements

Markets include the operations of ecommerce and market operations extending across stakeholders.

4.3 Industry to Grid Operations Applications and User Requirements

Industry to grid operations will integrate with the DEWG work and examine the requirements developed to date for large customers in industrial classes.

4.4 Building to Grid Integration Applications and User Requirements

Building to Grid operations will cover the issues in the NIST DEWG with commercial building operations. This domain will evaluate the present situation with commercial sector requirements development and identify missing requirements.

4.5 Home to Grid Integration Applications and User Requirements

Home to grid has seen some significant requirements development from progressive utilities, however this group will examine the completeness of the growing collection of use cases and define those that are still needed.

4.6 Electric Vehicle to Grid Applications and User Requirements

Emerging vehicle to grid is an important area to address upfront. Vehicles are like mobile customers with both demand response as well as power injection capabilities now being planned. This requires both revenue cycle services as well as DER integration capabilities.

4.7 Transmission Operations Applications and User Requirements

Transmission operations includes ISO/RTO operations, central generation integration, substation operations, wide area protection and control as example areas.
Coordination of transmission operations with distribution operations is imperative, especially when the distribution system is significantly penetrated by DER and DR.

4.8 Distributed Energy Resources Integration Applications and User Requirements

Distributed Energy Resources may be deployed anywhere on the power system and includes storage technologies. This domain will include discussion of the need for the paradigm of widely dispersed and distributed generation to be managed in concert with central station generation and storage technology.

DER applications should be coordinated with distribution and transmission operations under normal and emergency conditions.

4.9 Distribution Operations Applications and User Requirements

Distribution operations will examine requirements within its domain but also investigate how distribution operations will be impacted by customer dynamic integration including electric vehicle integration. Distribution requirements must also consider how the topologies of distribution system designs could be altered in the future to make use of advanced automation capabilities. Distribution systems will play key roles in emerging paradigms such as customer dynamics and DER deployments.

Coordination of distribution operations with transmission operations is needed and it will be more effective in the Smart Grid environment due to the significant active components in the distribution (DER, DR, Electric storage, Electric transportation).

4.10 Security User Requirements

This section covers the security requirements and the corresponding countermeasures necessary to secure the Smart Grid information infrastructure, including communications media, communications networks, connected equipment, and software applications and systems. These areas are critical to ensuring that the Smart Grid information infrastructure can be effectively secured over its life cycle. Interface designs must be able to support security in a way that is commensurate with applications and the potential threats. This section will discuss the security requirements of security functions that can provide a framework for evaluating the completeness of these requirements for the smart grid.

4.11 Information Infrastructure Management User Requirements

Information infrastructure management topics are both cross cutting as well as embedded with domains. Management must be implemented and managed at multiple levels across the enterprise and smart grid. This section covers the more federated architecture related requirements development.

- Information Infrastructure Policies
- Rules of Governance
4 Smart Grid Applications and User Requirements

- Network and System Management
5 Smart Grid Architecture and Interfaces

Defines Smart Grid Principles introduced in proposal and Defines what is meant by “Interfaces”. The design of interfaces must be approached through the steps identified below that define "functional" requirements as well as "non-functional" requirements.

5.1 Architecture and Interface Requirements Methodology (Marty)

Requirements Driven process is a must for the smart grid. The functions that the smart grid needs to support need to be defined independent of the underlying standards and technology. The requirements for the smart grid originate in both power engineering as well as distributed computing, communications and information technology. It should be noted that requirements are embedded in standards development so they remain foundational from both the stakeholder as well as the standards developer. For interface designs requirements are also the starting point. Each of these areas are discussed below.

Discusses the Existing Coverage of Requirements Development for the "Smart Grid" including the development of a "Taxonomy" of Applications that can be used to assess the state of requirements coverage. This section will be developed with the DEWGS to identify what requirements are needed to effectively define a "smart grid". The project will catalog what use cases are needed to define the smart grid. This will be followed by assessing the existing libraries of requirements that have been developed by industry to date. This task will also identify those under development in various organizations and projects. In effect this section catalogs what has been done to date.

Each of the key technical domains needs to provide a status of the development of requirements for the “smart grid” for their areas of operation. This project will not be able to develop requirements in the short time frame but will address the status of requirements development for the smart grid with the following three defined activities by domain.

For each domain the following will be identified:

1. Discussions of visions trends and observations driving the domain and its relation to other domains. This section by domain is intended to identify the higher level requirements and perspectives driving the need for smart grid infrastructure. (The following two categories of discuss are more specific to what is already done and where the gaps and overlaps are)

   The traditional domains of central generation, transmission, distribution, customer integration are evolving to become more integrated. It is important to recognize how each of the domains are evolving and needs to evolve as well as how the domains are changing relative to each other. A few key areas as examples are the development of more customer dynamics in the energy markets and with real time grid operations. These operations are coming from demand response and power injection from buildings and homes as well as the emergence of electric vehicles. Also the visioning exercises and whitepapers from DEWGs can also be sources of high level requirements. This section will describe the state of emerging and needed smart grid requirements development by domain.
2. Identification of existing sources of smart grid requirements:

In some domains several sets of requirements for smart grid and next generation automation have been developed. These are developing within utilities seeking to deploy advanced customer communications and metering systems as well as for Transmission and Distribution operations. Identify and catalog existing sources of requirements for the domain.

3. Identify where requirements development are needed by domain:

Requirements for the smart grid are not complete each of the domains will provide an assessment of where the requirements are complete and where they need to be developed. This discussion may also include where requirements overlaps are occurring i.e. where separate developments are taking place that need to be integrated through either technical work and/or getting rules of technical governance in place. Each domain should propose a taxonomy of applications development specific to the domain. This is a consensus building pathway to obtain a level of agreement on what needs to be defined for smart grid applications and function. The draft domains are listed below subject to the processes of this project. It should be noted that these assessments are to understand the state of the industry at this point and identify missing requirements for future development.

5.2 Markets Architecture and Interface Requirements

Markets include the operations of ecommerce and market operations extending across stakeholders.

5.3 Industry to Grid Operations Architecture and Interface Requirements

Industry to grid operations will integrate with the DEWG work and examine the requirements developed to date for large customers in industrial classes.

5.4 Building to Grid Architecture and Interface Requirements

Building to Grid operations will cover the issues in the NIST DEWG with commercial building operations. This domain will evaluate the present situation with commercial sector requirements development and identify missing requirements.

5.5 Home to Grid Architecture and Interface Requirements

Home to grid has seen some significant requirements development from progressive utilities, however this group will examine the completeness of the growing collection of use cases and define those that are still needed.

5.6 Electric Vehicle to Grid Architecture and Interface Requirements

Emerging vehicle to grid is an important area to address upfront. Vehicles are like mobile customers with both demand response as well as power injection capabilities now being planned. This requires both revenue cycle services as well as DER integration capabilities.
5.7 Transmission Operations Architecture and Interface Requirements

Transmission operations includes ISO/RTO operations, central generation integration, substation operations, wide area protection and control as example areas.

5.8 Distributed Energy Resources Architecture and Interface Requirements

Distributed Energy Resources may be deployed anywhere on the power system and includes storage technologies. This domain will include discussion of the need for the paradigm of widely dispersed and distributed generation to be managed in concert with central station generation and storage technology.

5.9 Distribution Operations Architecture and Interface Requirements

Distribution operations will examine requirements within its domain but also investigate how distribution operations will be impacted by customer dynamic integration including electric vehicle integration. Distribution requirements must also consider how the topologies of distribution system designs could be altered in the future to make use of advanced automation capabilities. Distribution systems will play key roles in emerging paradigms such as customer dynamics and DER deployments.

5.10 Security Architecture and Interface Requirements

This section covers the security requirements and the corresponding countermeasures necessary to secure the Smart Grid information infrastructure, including communications media, communications networks, connected equipment, and software applications and systems. These areas are critical to ensuring that the Smart Grid information infrastructure can be effectively secured over its life cycle. Interface designs must be able to support security in a way that is commensurate with applications and the potential threats. This section will discuss the security requirements of security functions that can provide a framework for evaluating the completeness of these requirements for the smart grid.

- SP800-53

5.11 Information Infrastructure Management Architecture and Interface Requirements

Information infrastructure management topics are both cross cutting as well as embedded with domains. Information infrastructure management must be implemented and managed at multiple levels across the enterprise and smart grid. This section covers the more federated architecture related requirements development.

- Information Infrastructure Policies
- Rules of Governance
- Network and System Management
6 Smart Grid Standards Gap Assessment

6.1 Overview of Standards Gap Assessment
Describe the Smart Grid standards, assess any gaps for meeting Smart Grid requirements, and identify actions to address these gaps. Anticipated characteristics -- Define the status of Existing and emerging standards for the smart grid. This can build from earlier industry architecture documentation, adding as appropriate and defining status of leading standards. Review of most likely standards and DEWG contributions.

6.2 Markets Standards Gap Assessment
Markets include the operations of ecommerce and market operations extending across stakeholders.

6.3 Industry to Grid Operations Standards Gap Assessment
Industry to grid operations will integrate with the DEWG work and examine the requirements developed to date for large customers in industrial classes.

6.4 Building to Grid Integration Standards Gap Assessment
Building to Grid operations will cover the issues in the NIST DEWG with commercial building operations. This domain will evaluate the present situation with commercial sector Standards Assessment and identify missing requirements.

6.5 Home to Grid Integration Standards Gap Assessment
Home to grid has seen some significant Standards Assessment from progressive utilities, however this group will examine the completeness of the growing collection of use cases and define those that are still needed.

6.6 Electric Vehicle to Grid Standards Gap Assessment
Emerging vehicle to grid is an important area to address upfront. Vehicles are like mobile customers with both demand response as well as power injection capabilities now being planned. This requires both revenue cycle services as well as DER integration capabilities.

6.7 Transmission Operations Standards Gap Assessment
Transmission operations includes ISO/RTO operations, central generation integration, substation operations, wide area protection and control as example areas.

6.8 Distributed Energy Resources Standards Gap Assessment
Distributed Energy Resources may be deployed anywhere on the power system and includes storage technologies. This domain will include discussion of the need for the paradigm of widely dispersed and distributed generation to be managed in concert with central station generation and storage technology.
6.9 Distribution Operations Standards Gap Assessment

Distribution operations will examine requirements within its domain but also investigate how distribution operations will be impacted by customer dynamic integration including electric vehicle integration. Distribution requirements must also consider how the topologies of distribution system designs could be altered in the future to make use of advanced automation capabilities. Distribution systems will play key roles in emerging paradigms such as customer dynamics and DER deployments.

6.10 Security Standards Assessment

6.11 Information Infrastructure Management Standards Assessment
7 Prioritized Actions and Timelines to Address Identified Issues

7.1 Overview of Actions and Timelines

NIST-focused Action Plan for resolving the gaps identified in the previous section. Prioritized actions and time lines will be defined as the project progresses.

This section describes the strategy that NIST can use to achieve a set of clear specifications within which manufacturers of goods and services can build interoperability, manageability, and security into products for the Smart Grid.

Interoperability Framework/Architecture. An initial version of the interoperability framework will be developed— one that will have the flexibility to evolve as the Smart Grid develops. Consensus on this Smart Grid Interoperability Framework and Architecture should be achieved by all stakeholders as the first step.

Recommendations and Justifications. Specific standards and technologies should be recommended in the Smart Grid Roadmap, but usually should not be mandated to all stakeholders. However, stakeholders should be required to justify why they are not implementing the standards. Some of these justifications could include:

- Some standards may not yet be finalized or available from vendors as mature products.
- Many near-term system implementations may need to be integrated with existing systems, so that it would be impractical to require new technologies.
- Stakeholders may have developed a plan for moving toward standards over time.
- Immediate implementation of certain standards may not be cost-justified until pilot projects assessing the technologies and standards have been analyzed.

On-going Consensus-Building Workshops. NIST should sponsor on-going workshops and other venues to assess the progress of different standards and technologies identified in the Roadmap.

Publicly Accessible Interoperability Knowledge Base. NIST plans to create a publicly-accessible interoperability knowledge base that will be the repository of the information necessary to perform standards assessments.

Accelerate Standards Development. With the clear picture of the standards landscape and roadmap established, NIST will work effectively with standards development organizations (SDOs), contractors, and industry experts and other stakeholders to accelerate the development of scalable, compatible and interoperable standards."

7.2 Markets Prioritized Actions

Markets include the operations of ecommerce and market operations extending across stakeholders.
7.3 Industry to Grid Operations Prioritized Actions

Industry to grid operations will integrate with the DEWG work and examine the requirements developed to date for large customers in industrial classes.

7.4 Building to Grid Integration Prioritized Actions

Building to Grid operations will cover the issues in the NIST DEWG with commercial building operations. This domain will evaluate the present situation with commercial sector Prioritized Actions and identify missing requirements.

7.5 Home to Grid Integration Prioritized Actions

Home to grid has seen some significant Prioritized Actions from progressive utilities, however this group will examine the completeness of the growing collection of use cases and define those that are still needed.

7.6 Electric Vehicle to Grid Prioritized Actions

Emerging vehicle to grid is an important area to address upfront. Vehicles are like mobile customers with both demand response as well as power injection capabilities now being planned. This requires both revenue cycle services as well as DER integration capabilities.

7.7 Transmission Operations Prioritized Actions

Transmission operations includes ISO/RTO operations, central generation integration, substation operations, wide area protection and control as example areas.

7.8 Distributed Energy Resources Integration Prioritized Actions

Distributed Energy Resources may be deployed anywhere on the power system and includes storage technologies. This domain will include discussion of the need for the paradigm of widely dispersed and distributed generation to be managed in concert with central station generation and storage technology.

7.9 Distribution Operations Prioritized Actions

Distribution operations will examine requirements within its domain but also investigate how distribution operations will be impacted by customer dynamic integration including electric vehicle integration. Distribution requirements must also consider how the topologies of distribution system designs could be altered in the future to make use of advanced automation capabilities. Distribution systems will play key roles in emerging paradigms such as customer dynamics and DER deployments.

7.10 Security Prioritized Actions

7.11 Information Infrastructure Management Prioritized Actions
7 Prioritized Actions and Timelines to Address Identified Issues

7.12 Consolidated Action Plan and Time Schedule
Consolidated Action Plan across all Domains, plus the time schedule for each of the actions.

7.13 Recommendations to NIST on Action Plan
Additional work defining both the Smart Grid power system requirements and the necessary information system capabilities to meet future or newly identified requirements. The results of that work can be included the Roadmap as they are identified. This section also includes a discussion on specific research and development issues. These are areas for which there is no clear solution now but are necessary for the vision of smart grid to be manifest.
8 Definitions

8.1 Terms

Note that it is impossible to write a document of broad scope such as this without encroaching on definitions understood to have accepted but different meanings in more than one constituent audience. Therefore, for the purposes of considered understanding, the definitions in this section represent the intended meanings of the authors when used within this document.

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Capability</td>
<td>The ability of a standard to satisfy a Requirement</td>
</tr>
<tr>
<td>Environment</td>
<td>The definition of a profile of standards organized by Interface and Requirements.</td>
</tr>
<tr>
<td>Interface</td>
<td>The place at which two systems meet and act on or communicate with each other.</td>
</tr>
<tr>
<td>Requirement</td>
<td>(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.</td>
</tr>
<tr>
<td>Standards</td>
<td>A technical specification, usually produced by an Standards Development Organization (SDO).</td>
</tr>
<tr>
<td>Use Case</td>
<td></td>
</tr>
<tr>
<td>Confidentiality</td>
<td>“Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information…” [44 U.S.C., Sec. 3542] A loss of confidentiality is the unauthorized disclosure of information.</td>
</tr>
<tr>
<td>Integrity</td>
<td>“Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity…” [44 U.S.C., Sec. 3542] A loss of integrity is the unauthorized modification or destruction of information.</td>
</tr>
<tr>
<td>Availability</td>
<td>“Ensuring timely and reliable access to and use of information…” [44 U.S.C., SEC. 3542] A loss of availability is the disruption of access to or use of information or an information system.</td>
</tr>
</tbody>
</table>
# 8.2 ACRONYMS

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACSE</td>
<td>Association Control Service Element</td>
</tr>
<tr>
<td>AES</td>
<td>Advanced Encryption Standard</td>
</tr>
<tr>
<td>AMI</td>
<td>Advanced Metering Infrastructure</td>
</tr>
<tr>
<td>AMR</td>
<td>Automated Meter Reading</td>
</tr>
<tr>
<td>ANSI</td>
<td>American National Standards Institute</td>
</tr>
<tr>
<td>API</td>
<td>Application Program Interface</td>
</tr>
<tr>
<td>ASD</td>
<td>NII DoD CIO - Assistant Secretary of Defense - Networks &amp; Information Integration - CIO Office</td>
</tr>
<tr>
<td>ASHRAE</td>
<td>American Society of Heating, Refrigerating and Air Conditioning Engineers</td>
</tr>
<tr>
<td>CM</td>
<td>Configuration Management</td>
</tr>
<tr>
<td>CIM</td>
<td>Common Information Model</td>
</tr>
<tr>
<td>CIGRE</td>
<td>International Council On Large Electric Systems</td>
</tr>
<tr>
<td>CSRC</td>
<td>Computer Security Resource Center</td>
</tr>
<tr>
<td>DA</td>
<td>Distribution Automation</td>
</tr>
<tr>
<td>DDNS</td>
<td>Dynamic Domain Name System</td>
</tr>
<tr>
<td>DER</td>
<td>Distributed Energy Resources</td>
</tr>
<tr>
<td>DES</td>
<td>Data Encryption Standard</td>
</tr>
<tr>
<td>DHCP</td>
<td>Dynamic Host Configuration Protocol</td>
</tr>
<tr>
<td>DHS</td>
<td>Department of Homeland Security</td>
</tr>
<tr>
<td>DLC</td>
<td>Direct Load Control</td>
</tr>
<tr>
<td>DNS</td>
<td>Domain Name System</td>
</tr>
<tr>
<td>DOD</td>
<td>Department of Defense</td>
</tr>
<tr>
<td>DOE</td>
<td>Department of Energy</td>
</tr>
<tr>
<td>DR</td>
<td>Demand Response</td>
</tr>
<tr>
<td>ECWG</td>
<td>Electronic Commerce Working Group</td>
</tr>
<tr>
<td>EMCS</td>
<td>Utility/Energy Management and Control Systems</td>
</tr>
<tr>
<td>EPRI</td>
<td>Electric Power Research Institute</td>
</tr>
</tbody>
</table>
### Definitions

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Full Form</th>
</tr>
</thead>
<tbody>
<tr>
<td>ESP</td>
<td>Energy Service Provider</td>
</tr>
<tr>
<td>FBI</td>
<td>Federal Bureau of Investigation</td>
</tr>
<tr>
<td>FCC</td>
<td>Federal Communications Commission</td>
</tr>
<tr>
<td>FTP</td>
<td>File Transfer Protocol</td>
</tr>
<tr>
<td>GID</td>
<td>Generic Interface Definition</td>
</tr>
<tr>
<td>GOOSE</td>
<td>Generic Object-Oriented Substation Event</td>
</tr>
<tr>
<td>GSA</td>
<td>General Services Administration</td>
</tr>
<tr>
<td>GWAC</td>
<td>Gridwise Architecture Council</td>
</tr>
<tr>
<td>HTTP</td>
<td>Hyper Text Transfer Protocol</td>
</tr>
<tr>
<td>HVAC</td>
<td>Heating Ventilating and Air Conditioning</td>
</tr>
<tr>
<td>IATFF</td>
<td>Information Assurance Technical Framework Forum</td>
</tr>
<tr>
<td>IEC</td>
<td>International Electrotechnical Commission</td>
</tr>
<tr>
<td>IED</td>
<td>Intelligent Electronic Device</td>
</tr>
<tr>
<td>IEEE</td>
<td>Institute of Electrical and Electronic Engineers</td>
</tr>
<tr>
<td>IOSS</td>
<td>Interagency OPSEC Support Staff</td>
</tr>
<tr>
<td>IP</td>
<td>Internet Protocol</td>
</tr>
<tr>
<td>ISO</td>
<td>International Organization for Standardization</td>
</tr>
<tr>
<td>KPI</td>
<td>Key Point of Interoperability</td>
</tr>
<tr>
<td>LAN</td>
<td>Local Area Network</td>
</tr>
<tr>
<td>MIB</td>
<td>Management Information Base</td>
</tr>
<tr>
<td>MIME</td>
<td>Multipurpose Internet Mail Extensions</td>
</tr>
<tr>
<td>MMS</td>
<td>Manufacturing Messaging Specification</td>
</tr>
<tr>
<td>NARUC</td>
<td>National Association of Regulatory Utility Commissioners</td>
</tr>
<tr>
<td>NIAP</td>
<td>National Information Assurance Partnership</td>
</tr>
<tr>
<td>NIETP</td>
<td>National IA Education and Training Program</td>
</tr>
<tr>
<td>NIST</td>
<td>National Institute of Standards and Technology</td>
</tr>
<tr>
<td>NSA</td>
<td>National Security Agency</td>
</tr>
<tr>
<td>NSM</td>
<td>Network and System Management</td>
</tr>
</tbody>
</table>
9 References

OID Object Identifier
OSI Open Systems Interconnection
QOS Quality Of Service
RBAC Role Based Access Control
RFC Request For Comments
RSA Rivest, Shamir, Adelman
RTP Real-Time Pricing
SCL Substation Configuration Language
SCP Secure Copy Protocol
SDO Standards Development Organization
SHA Secure Hash Algorithm
SNMP Simple Network Management Protocol
SNTP Simple Network Time Protocol
SOA Service-Oriented Architecture
SSH Secure Shell
TCP Transport Control Protocol
TFTP Trivial File Transfer Protocol
UCA Utility Communications Architecture
UCAIug UCA International Users Group
UID Universal Identifier
UML Unified Modeling Language
WAN Wide Area Network
XML Extensible Markup Language

9 References

[1] Integrated Energy and Communications System Architecture (IECSA), Volume I-IV, Electricity Innovation Institute Consortium for Electric Infrastructure to Support a Digital Society (CEIDS). (Note: the term IECSA is being phased out; the new name for this effort is “IntelliGrid Architecture” and it continues to be sponsored by CEIDS).
References


[7] SMART GRID POLICY, 126 FERC ¶ 61,253, UNITED STATES OF AMERICA, FEDERAL ENERGY REGULATORY COMMISSION, 18 CFR Part Chapter I, [Docket No. PL09-4-000], (Issued March 19, 2009)