I. Preamble/Context

This document provides a preliminary overview of Smart Grid interoperability standards to meet functional requirements that may impact reliability in the bulk electric power system. The scope includes standards relevant to grid monitoring and control, integration of renewable energy sources, and demand response programs. Not included, however, are standards covering communication behind the customer interface, i.e., within a home or facility, market transactions, utility business systems, and compliance testing and user guidelines. At this preliminary stage of a longer-term process to coordinate the development of an interoperability roadmap for the Smart Grid, NIST does not here formally endorse or recommend specific standards because the necessary roadmapping input and standards gap analyses have not been completed. Based on preliminary analysis and input from stakeholders, however, candidate standards are identified as having potential to meet interoperability requirements for the Smart Grid. These standards are in various stages of maturity and parts of them may be incomplete or under development. These interim identifications are preliminary and are not intended to be comprehensive, and must be expanded, revisited and updated as the more complete interoperability framework is developed.

A. Smart Grid Architecture.

As shown in Figure 1, the electric power system can be conceptually divided into different domains:

- utility transmission and distribution grid
- customer premises’ networks and devices, including residential, commercial, and industrial
- utility enterprise systems

Among these domains, NIST and the DOE GridWise Architecture Council (GWAC) have established Domain Expert Working Groups (DEWGs): Home-to-Grid (H2G), Building-to-Grid (B2G), Industrial-to-Grid (I2G), and Transmission and Distribution (T&D). In addition, a Business and Policy (B&P) DEWG has been created to identify and address business and regulatory policy issues that affect the technical issues. The broad domains in Fig. 1 may be more finely divided into environments, as shown in Figure 2. Between and within the environments are the interfaces at which interoperability issues must be addressed. Most importantly, the core information communicated must be made consistent across multiple interfaces to ensure a common understanding of the meaning of the information among different applications. For instance, a single standard for communicating an electric price signal across the Smart Grid, or a single standard for demand response signaling to multiple customer interfaces would be used.

Another consideration in prioritizing interface identification is to focus on the “inter-system” rather than “intra-system” interfaces, shown in Fig. 3. This approach identifies the key interfaces as those between multiple stakeholders, rather than those within a given utility system. This could be an interface between a utility system and the many unique customer systems, services provider systems, resources supplier systems, and an overall macro-system such as a wide area control system and Regional Transmission Organizations (RTO)/Independent System Operators (ISO) systems.

Development is underway to create a Smart Grid roadmap that identifies and prioritizes the key interfaces and required standards. The issues and priorities identified in this document focus on ensuring reliability in the bulk power system, and will represent one part of the complete roadmap.

B. Principles and Goals

Achieving interoperability can be supported by adhering to the principles outlined in the GWAC Decision-makers Checklist. These principles, which apply to Smart Grid devices, systems, and “systems of systems,” are as follows:
• Architecture and Design
  o Specifies points of interface clearly
  o Uses open architecture and open standards\(^1\)
  o Specifies results, not a specific technology
  o Promotes interchangeability – encourages vendor competition

• Interconnectivity and Security
  o Has physical and electronic interconnection capability
  o Uses standard communication protocols
  o Makes information available to all authorized devices and users
  o Can manage multiple devices using a common command
  o Meets at least basic NERC cyber-security requirements
  o Has adequate redundancy to ensure reliability and safety

• Evolutionary Capability and Service Life
  o Device is upgradeable via software upload
  o Device/project is backwards compatible

• Collaborator Independence
  o Device/project is transactive rather than command/control

As described in section 1305, Title XIII in the Energy Independence and Security Act, the following principles shall be used for the interoperability framework:

• Flexible, uniform and technology neutral
• Designed to accommodate centralized generation and transmission resources and consumer distributed resources (including distributed generation, renewable generation, energy storage, energy efficiency, and demand response and enabling devices and systems)
• Designed to be flexible to incorporate regional and organization differences and technology innovations
• Considers the use of voluntary uniform standards for demand-response ready equipment (including load reduction, provision of ancillary services, and short term load shedding); and
• Provides appropriate manufacturer lead time.

In addition, there are several goals that should be central to any effort to develop the Smart Grid information infrastructure. These goals include:

• Functional requirements are met
• Low cost of implementation
• Low cost of maintenance
• Adaptable
• Interoperable
• Protocol independent
• Scalable
• Broad industry support

To achieve these goals the following items are desirable:

• A common library of definitions that is used across all Smart Grid systems and use cases.

\(^{1}\) NIST views "open standards" as those standards that are openly available and are developed in an open manner, meaning that all interested parties are able to participate. NIST also believes that standards for Smart Grid technologies should be interoperable, scalable and should avoid vendor lock-in or proprietary technologies that will limit user choice, regardless of the process under which the standards are developed.
A model driven approach that improves human understanding of Smart Grid domains and links human readable models with implementations.

A robust, accepted conformity testing framework to allow stakeholders to test products for compliance with a particular standard.

A reference implementation to test the standard as it is being developed.

II. SG Standards Development Priorities and Issues

NIST has received input identifying issues and priorities both individually from the many stakeholders, and collectively through DEWG teleconferences, meetings, and workshops, with representation of all the major industry stakeholders. Based on this preliminary input, the following are priority areas in transmission and distribution for the development of the Smart Grid: 1) integration of distributed energy resources (DER), and demand response (DR), including renewable energy sources, energy storage, and electric vehicles; and 2) Grid reliability and management. The status, issues, and standards for these Smart Grid Areas are given below.

A. Priority areas

I. Integration of DER and DR

a. Integration of DER

DER includes both distributed generation and storage. DER communications are covered by the IEC 61850 series, discussed in greater detail in Section II.B.2. Dispatchable storage provides backup in the event of voltage sags and short interruptions and therefore requires extremely rapid communication. It is also used to provide intermediate backup power while backup generators are brought on-line. It can provide for load leveling and peak shaving, and support non-dispatchable generators. Currently, commercial storage technology is not realistically capable of supporting the full Smart Grid dispatchable storage vision, which makes it difficult to predict what information needs will be required. At present it is anticipated that DER standards will support the basic information required for communication with storage devices.

b. Demand Response

Demand response is as a priority area because of its important role in maintaining grid stability as the grid is operated closer to capacity, and as more renewables are brought online with their less stable generation characteristics. DR is key, at least in the short term, to changing load shape and replacing peaking generation plants.

Demand response is an area where utilities and ISOs nationwide have a large variety of programs that implement different DR goals. There is not yet a standard that covers all the variations of information elements across the spectrum of DR programs, or a standard for communicating that information. Two standards are addressing both in different sectors.

OpenHAN, developed under the Open Smart Grid (OpenSG) Subcommittee of the Utility Communication Architecture (UCA®) International Users Group (UCAIUG), is a specification that covers the energy services interface which provides security and coordination functions that enable secure interactions between relevant home area network (HAN) devices and the utility. It permits applications such as remote load control, monitoring and control of distributed generation, in-home display of customer usage, reading of non-energy meters, and integration with building management systems. It also provides auditing/logging functions that record transactions to and from HAN Devices.

Open Automated Demand Response (OpenADR) moved from research project phase to formal standards development within OASIS Energy Interoperation TC with utility input organized via UCAIug. OpenADR is a web-services based communications data model designed to facilitate sending and receiving of DR signals from a Utility or independent system operator (ISO) to electric customers. The intention of the data model is to interact with building and industrial control systems that are pre-
programmed to take action based on a DR signal, enabling a demand response event to be fully automated, with no manual intervention. It has a highly flexible infrastructure design to facilitate common information exchange between Utility/ISO and end-use participants.

OpenHAN is led by utilities and aimed at the residential space. OpenADR is designed to serve larger customers (commercial and industrial). These two efforts would benefit from additional collaboration to ensure that information common to both is aligned with common semantics. Both efforts have grown out of the efforts of California utilities under the direction of the State of California government. OpenADR has been moved to OASIS for formal standards development. OpenHAN should also move to a formal SDO process and alignment with OpenADR may be more easily supported if OpenHAN is moved to OASIS. Both efforts are encouraged to work closely with stakeholders and NIST on definitions of customer interface(s).

c. Load management for transportation (electric vehicles)

Communication standards for electric vehicles is a priority area due to the potential integration of vehicle batteries as a grid resource, as well as the recognition that vehicle charging will add significant load to the grid. Different organizations are looking at different elements of the communications issues and coordination of these efforts is required. NIST expects that coordination can be monitored and encouraged through a task group effort. The standards are now being developed, but implementations are lacking. Currently, the center of standards development work is SAE, and NIST encourages cooperation with the following efforts.

SAE J2836, Recommended Practice for Communication between Plug-in Vehicles and the Utility Grid (2009 ballot), addresses grid-optimized energy transfer for plug-in electric vehicles – that is, ensuring that vehicle operators have sufficient energy for driving while enabling the delivery of that energy to vehicles in ways that minimize stress upon the grid.

SAE J2847 - Information Report for Use Cases for J2836 (2009 ballot), documents the set of use cases which must be supported by J2836. This includes three use cases (TOU, DR, and price signals) and addresses the following requirements: secure two-way communication with the Energy Services Communication Interface (i.e., Utility), time- or price-based charging preferences based on current electric rate/tier, vehicle charging at any voltage, vehicle roaming and unified billing infrastructure, and customer override/opt-out.

2. Grid reliability and management:

In most areas, the existing U.S. power grid is operated with proprietary systems that are fragmented and isolated. Attempts to create interoperable systems often fail because there is no third-party certification of conformance. Another issue is inherent latency in grid monitoring; a delay of 2 seconds or more before a grid operator sees an event is not uncommon, and this may be too late to take action to control system instability, leading to a blackout. Standards development also has been fragmented in different groups across the industry due to the diversity of “environments,” as shown in Figure 2, with no formal architecture in place. Standardized interfaces for devices are lacking. In addition, there is no communications standards oversight committee to ensure compliance and certification of data sensor devices, communication network devices, and applications.

Some of the standards issues in transmission substations and intertie stations are the following. Advanced standards for field equipment automation are proposed (see Section II.B.2), but lack designs and implementations that use these standards. There are legacy standards that at present cannot meet Smart Grid requirements. Standards are also in different stages of maturity with no migration pathways yet established to reach Smart Grid goals. A need for lower latencies for monitoring grid disturbances with phasor measurement units (PMUs) drives demanding quality-of-service (QoS) requirements as specified for NASPInet.
While much good work in standards development for the grid has occurred and will continue to support the electric energy system, there are requirements for the Smart Grid that are not met by some existing standards. The following efforts are identified to support development of the Smart Grid:

- development of strategies to migrate legacy standards to meet lower latency requirement for substation and transmission tie stations;
- harmonization of the “next generation” suites of standards that meet Smart Grid requirements, such as IEC 61850 with the CIM standards, IEC 61970 and 61968 and more demanding QoS requirements of NASPInet;
- development of new communication protocols such as the NASPInet GridStat for wide area monitoring using phasor measurement units; and
- harmonization of IEC 61850, and ANSI C12.19 and C12.22, which will be published soon.

B. Cross-cutting issues

1. Cyber Security

The cornerstone of a Smart Grid is the ability for multiple agents (e.g., devices, processes) to interact with one another via communications networks. The cyber security strategy for the Smart Grid must examine both domain-specific and common risks when developing a mitigation strategy to ensure interoperability of solutions across domains.


FERC Order 706 approved the current NERC CIP Cyber Security standards in January 2008. Phased-in compliance audits for the current NERC CIP Cyber Security standards begins July 2009 with compliance audits for all NERC registered entities and all requirements starting by January 2011. In addition, FERC Order 706 directed NERC to develop date-driven modifications concerning a number of oversight and technical issues related to cyber protections and directed NERC to monitor NIST cyber security standards to “determine if they contain provisions that will protect the Bulk-Power System better than the CIP Reliability Standards.”

In October 2008, the NERC CIP Standards Drafting Team (SDT) adopted a multi-phase approach for revising the CIP Cyber Security standards. Revision 1 addresses date-driven directives included in FERC Order 706, clarifications, and conformance edits approved by 75% of the SDT. Later Revision(s) will address additional cyber security issues.

The NERC CIP SDT adopted an aggressive approach to developing the NERC CIP, Revision 1 standards. NERC CIP, Revision 1 Draft standards were completed in November 2008 and were released for industry comment in December 2008. The NERC CIP, Revision 1 standards are scheduled for Ballot in April 2009 and submission to Regulators in June 2009.

The development of NERC CIP, Revision 2 began in February 2009 to address issues raised in FERC Order 706, industry comments raised early in the drafting process, and will consider other cyber security standards and guidelines including NIST. The NERC CIP, Revision 2 standards are scheduled to be submitted to Regulators by December 2010.

Currently, the NERC CIP Cyber Security standards only apply to the Bulk Power System and use an asset-based approach rather than a system-based approach to security, which could potentially lead to security gaps. The NERC CIP Cyber Security standards do not address the cyber security requirements of the other domains (e.g., home to grid, building to grid, industrial to grid), nor do they address the
cyber security requirements between these domains. There are other cyber security standards that are in
development that could address components of the Smart Grid:

- ISA99/IEC 62443 suite of standards for Industrial Automation and Control System security
- NIST Special Publication (SP) 800-53 security controls for federal agencies, including those who are
  part of the Bulk Power System (e.g., Tennessee Valley Authority, Bonneville Power Authority).
- Advanced Metering Infrastructure (AMI) Security Task Force (AMI-SEC), which is defining
  common requirements and standardized specifications for securing AMI system elements.

The development of the NERC CIP Cyber Security standards for the Bulk Power System should be
supported as well as the current efforts to harmonize the NERC CIP, ISA99/IEC 62443, and NIST SP
800-53 security standards. These standards should be assessed for applicability and interoperability within
a risk management framework.

2. Utility-system integration

To be effectively integrated, systems within the grid must be able to interact with each other without
special effort. In early days of grid automation the focus was on getting systems within a substation that
were connected by a dedicated communication infrastructure to exchange basic control information. The
DNP-3 and IEC 60870 standards were designed to provide this functionality. These standards work well
within a single substation, but are not well suited to inter-substation communication. While DNP-3 and
60870 have both been updated to support exchange over TCP/IP, they are not well-suited to complex
distributed networks.

An effort to improve upon IEC 60870 by using the EPRI Utility Communication Architecture along
with the expertise gathered from experience with IEC 60870 culminated in the IEC 61850
“Communication networks and systems in substations” standard. IEC 16850 provides abstract data
models for the substation that can be mapped on to a variety of protocols. Some of the supported
protocols include MMS and web services. OPC XML and DNP3 mappings are all under development.

The scope of 61850 was originally just the power grid substation and included:

- Requirements for functions and device models;
- Intelligent Electronic Device (IED) configuration description language;
- Communication structure for substations and feeder equipment; and
- Abstract communication service interface.

Presently the scope of IEC 61850 is being expanded to cover more than the substation and projects
are underway to cover:

- hydro plants (new work)
- Communication between substations (new work)
- Communication between control centers and substations (new work)
- Adaptation of wind turbines (new work)

A second edition of IEC 61850 is expected to be released soon that will tighten up gaps in the first
specification. Although basic communications can be implemented readily, different vendor
implementations of advanced functions may not interoperate well. The standard contains many
implementation choices with few mandatory items, but the new edition should help address these
problems.

The next step towards the new distributed network Smart Grid paradigm is the IEC 61970 and 61968
known as the Common Information Model (CIM) standards. These two standards were developed for
the next generation grid to allow application software to exchange information about the configuration and
status of an electrical network. The CIM currently takes the form of a Unified Modeling Language
(UML) model showing the types of information and the relationships between the information types.
This UML model can be used to generate code structures such as XML schemas, database schemas and Java class libraries. By using this approach the burden to implement the standards is reduced and compatibility between applications is increased.

The 61970 series covers transmission systems, including Energy Management Systems (EMS) and Supervisory Control And Data Acquisition (SCADA) systems. The 61968 series covers distribution systems. Standards in this series include distribution management systems, outage management systems, metering, Geographic Information Systems (GISs), and asset management, among others. The purpose of the CIM standards is to define a reference set of definitions that can be used as the basis for development of new protocols. As a result, the CIM standards do not attempt to provide plug-and-play interoperability, and different implementations used in different utilities typically cannot interoperate unless the utilities have worked cooperatively from the beginning of the projects to define the same rules.

MultiSpeak™, sponsored by the National Rural Electric Cooperative Association (NRECA) for smaller co-op utilities lacking resources to develop their own protocols, takes a different approach. It rigidly defines the interface so that different vendors' products can interoperate without the need for development of extensive custom interfaces, but this interface does not take into account the possible variations of information infrastructure at the utility. Although it provides interoperability between vendors very quickly, its feature set is limited and not easy to expand or adapt to new uses. Presently there are more than 30 interfaces defined for functions such as meter reading, connect/disconnect, meter data management, outage detection, load management, SCADA, and distribution automation control.

3. Standards Development and Conformity Testing

Conformity testing verifies that products do adhere to the specifications defined in the standards under test. It can accelerate development of the standard itself as well as accelerating the development of compliant products, and increasing confidence in the standards and products that have undergone the testing.

Conformity testing, together with reference implementations and lessons learned from Smart Grid demonstration projects including those funded by DOE, can further accelerate the development of standards. Development of the reference implementation brings to light inconsistencies and ambiguities in the standard under development. The reference implementation gives the standards participants confidence the standard-under-development actually works, which can prevent unnecessary changes once the standard is published. In addition, Smart Grid demonstration projects offer valuable testing grounds for evaluating and improving standards. Experiences from these projects should be publicly shared, regardless of whether they are federally funded or not. Once a standard has been published, conformity testing can accelerate product development by giving vendors well-defined criteria to meet.

Creating a conformance assessment test for a standard provides a set of rules and associated tests that a vendor can use to test their product while it is being developed. Without conformity testing it can be difficult for a customer to determine which products to purchase. Customers might well find that two products claiming compliance may not work together often leading to increased costs to troubleshoot and fix the problems. Ultimately this can result in the perception that the standard is too poorly defined to ensure interoperability.
IEC 61970/61968 for Enterprise “IT” Integration

IEC 61850 for Real-Time Field Automation, DER and RT Customer Systems/Vehicle Integration

IEEE/IEC P37.118/61850 For Phasor Measurement Units

SAE/61850 For PHEVs

ANSI C12 Revenue Metering

ASHRAE/ANSI 135 for Building Automation

Figure 1. Smart Grid Domains showing some relevant standards².

² From Joe Hughes, Industry Level Architecture Development Strategies for Customer Communications, EPRI
Figure 2. The Electric Power Grid Subdivided into Environments\(^3\)

---

\(^3\) Hughes, Joseph, Intelligrid\(^{TM}\) Architecture in Brief, EPRI
Note:

“inter-system” interfaces are those interfaces between the boundary of the utility’s transmission, distribution and customer systems and the boundary of another entity’s systems or devices (i.e., the interface between a utility meter and customer device, or between utility grid management system and RTO system).

“intra-system” interfaces are those interfaces within the boundary of the utility’s system of transmission, distribution and customer systems (e.g., interface between utility meter and utility communication network or utility fault detector and distribution management system).

---

4 From Smart Grid Standards Adoption: Utility Industry Perspective, OpenSG Subcomittee and Smart Grid Utility Executive Working Group, UCAIU/G