Proposed "Smart Grid Reference Architecture and Roadmap"

This is a proposed document, and not an official NIST document.

The goal of the document is to provide a ***Smart Grid Reference Architecture and Roadmap****.*

It is a work in progress, with many "holes", but hopefully a reasonably useful organization. If accepted as a possible way forward, it still needs significant input from a significant number of viewpoints.

Please feel free to criticize (but only if you provide solutions), comment, add to, modify, or ignore.

Respectfully, Frances Cleveland

Table of Contents

1. INTRODUCTION TO SMART GRID REFERENCE ARCHITECTURE AND ROADMAP 1

1.1 Purpose of this Smart Grid Reference Architecture and Roadmap Document 1

1.2 DOE Definition of Smart Grid 1

1.3 Smart Grid Domains 2

1.4 NIST Domain Expert Working Groups (DEWGs) 4

2. SMART GRID DOMAIN FUNCTIONAL REQUIREMENTS 6

2.1 Smart Grid Functional Requirements for the Domains 6
2.1.1 Central Generation and Storage Functions 6
2.1.2 Distributed Energy Resources Functions 6
2.1.3 Transmission System Functions 6
2.1.4 Distribution Function Systems 7
2.1.5 Customer – Utility Interaction Functions 9
2.1.6 Electric Market Operations Functions 10
2.1.7 Buildings, Homes, and Industries Functions 10

2.2 Functional Requirements for Cross-Cutting Areas 10
2.2.1 Cyber and Physical Security 10
2.2.2 Network and System Management 11
2.2.3 Specifications and Engineering 11
2.2.4 Conformance and Interoperability Testing 11
2.2.5 Cross-Enterprise Identity Management 11

3. INTEROPERABILITY AND STANDARDS 12

3.1 Interoperability: What Does It Really Mean 12
3.1.1 Interoperability: Analogy to Language 12
3.1.2 Interoperability: Analogy to Societal Rules for Using Language 13
3.1.3 Benefits of Interoperability to Stakeholders 13
3.1.4 Interoperability Challenges: Technical, Security, and Financial 14

3.2 Standards: Meeting the Challenges of Interoperability 15
3.2.1 Purpose of Interoperability Standards 15
3.2.2 Types of Standards 15

4. OVERVIEW OF STANDARDS BODIES 16

4.1 Overview of Information Standards Bodies 16
4.1.1 International Electrotechnical Commission (IEC) TC57 Standards 16
4.1.2 Institute of Electrical and Electronic Engineers (IEEE) 17
4.1.3 Internet Engineering Task Force (IETF) 18
4.1.4 American National Standards Institute (ANSI) 18
4.1.5 National Institute of Standards and Technology (NIST) 18
4.1.6 North American Electric Reliability Corporation (NERC) 18

4.1.7 World Wide Web Consortium (W3C) 19

4.2 Users Groups and Collaborative Efforts within the Power Industry 19
4.2.1 UCA International Users Group (UCAIug) 19
4.2.2 NRECA's MultiSpeak 20
4.2.3 Cigré 20
4.2.4 GridWise™ Alliance 20
4.2.5 Electric Power Research Institute (EPRI) IntelliGrid 20
4.2.6 Vendor Collaborations 21
4.2.7 Utility Standards Board 21

5. EXISTING SMART GRID-RELATED STANDARDS AND RECOMMENDED PRACTICES 22

5.1 Existing Smart Grid Standards for Domains 22
5.1.1 Central Generation and Storage 22
5.1.2 Distributed Energy Resources 22
5.1.3 Transmission Grid 22
5.1.4 Distribution Grid 22
5.1.5 Customer – Utility Interactions 23
5.1.6 Market Operations 23
5.1.7 Building, Home, and Industrial Systems 23

5.2 Existing Smart Grid Standards for Cross-Cutting Areas 23
5.2.1 Cyber and Physical Security 23
5.2.2 Network and System Management 23
5.2.3 Conformance and Interoperability Testing 24

6. GAP ANALYSIS OF POWER SYSTEM "SMART GRID" INFORMATION STANDARDS 25

6.1 Purpose of this Gap Analysis 25

6.2 Gaps in Infrastructure Information Standards 25
6.2.1 Distribution and DER Field Equipment Information Standards 25
6.2.2 Customer Site – AMI, Gateways, and HAN Information Standards 26
6.2.3 Transmission Field Equipment Information Standards 27
6.2.4 Utility Enterprise Information Standards 27

6.3 Gaps in Cross-Domain Standards 28
6.3.1 Cyber Security Standards 28
6.3.2 Standards Interoperability and Conformance Testing 29

6.4 Gaps in Smart Grid Applications – Guidelines and Metrics 29
6.4.1 Purpose of Smart Grid Applications 29
6.4.2 Metrics for Measuring a Smart Grid 30

1. Introduction to Smart Grid Reference Architecture and Roadmap

1.1 Purpose of this Smart Grid Reference Architecture and Roadmap Document

NIST is required to provide an initial "***Roadmap for Smart Grid Information Standards Activities***" by May 2009. It is well understood that extensive and complex Smart Grid power system requirements, defined in business processes and Use Cases, must drive the development of the information system requirements, including information standards. It is also well known, due to years of prior and on-going work, that an extensive set of standards, technologies, and recommended practices already exist, but that in addition, there are a number of gaps in these existing standards that must be filled through extensions and new development. As noted by Dr. Steven Chu, Secretary of Energy, not only is there low hanging fruit, there is fruit already lying on the ground, ready to be picked up. These known gaps in the information standards are those ground-lying fruits for the Smart Grid.

Therefore, the purpose of this document is to provide an overview of the Smart Grid Reference Architecture, including known functional requirements and existing information standards, and to provide a Roadmap to identify and justify the known gaps in these existing standards as obvious areas for immediate action.

At the same time, additional work defining both new Smart Grid power system requirements and the necessary information system capabilities to meet those requirements must be continued. The results of that work can be fed into the Roadmap as they are identified.

1.2 DOE Definition of Smart Grid

The Department of Energy (DOE) discussed the Smart Grid as follows[1]:

"*Think of the Smart Grid as the internet brought to our electric system. [It is] a tale of two timelines: There are in fact two grids to keep in mind as our future rapidly becomes the present.*

The first – *we'll call it "a smarter grid" – offers valuable technologies that can be deployed within the very near future or are already deployed today.*

The second – *the Smart Grid of our title – represents the longer-term promise of a grid remarkable in its intelligence and impressive in its scope, although it is universally considered to be a decade or more from realization. Yet given how a single "killer application" – e-mail – incited broad, deep and immediate acceptance of the internet, who is to say that a similar killer app in this space won't substantially accelerate that timetable?*

In the short term, a smarter grid will function more efficiently, enabling it to deliver the level of service we've come to expect more affordably in an era of rising costs, while also offering considerable societal benefits – such as less impact on our environment.

[1] Litos Strategic Communication (under contract for the DOE) (2008-09-10). *The Smart Grid: An Introduction*. United States Department of Energy. p. 7. http://www.oe.energy.gov/DocumentsandMedia/DOE_SG_Book_Single_Pages.pdf.

Longer term, expect the Smart Grid to spur the kind of transformation that the internet has already brought to the way we live, work, play and learn.

A smarter grid applies technologies, tools and techniques available now to bring knowledge to power – knowledge capable of making the grid work far more efficiently...

- *Ensuring its reliability to degrees never before possible.*
- *Maintaining its affordability.*
- *Reinforcing our global competitiveness.*
- *Fully accommodating renewable and traditional energy sources.*
- *Potentially reducing our carbon footprint.*
- *Introducing advancements and efficiencies yet to be envisioned."*

More succinctly, ***the Smart Grid delivers electricity from suppliers to consumers using digital technology to:***

- ***Increase reliability***
- ***Save energy through improved efficiency***
- ***Reduce overall costs over a reasonable time period***
- ***Minimize security risks***
- ***Minimize environmental impacts.***

1.3 Smart Grid Domains

Although most Smart Grid issues impact all aspects of electric energy delivery, it is convenient to separate the issues into different domains. Specifically, as defined in IntelliGrid, these domains are:

- **Central generation** (and storage), including traditional power plants, renewable energy plants, and other large sources of energy
- **Distributed energy resources**, consisting of smaller sources of generation and storage predominantly interconnected at the distribution level, such as photovoltaics, small wind, and plug-in hybrid electric vehicles
- **Transmission system**, including ISOs, transmission operations, planning, and maintenance, as well as substation automation and synchrophasor measurements
- **Distribution system**, including distribution operations, automation, planning, and maintenance
- **Customer – utility interactions**, covering utility to customer interactions with respect to metering, energy services, PHEVs, and interfaces to customer gateways (with sub-domains of C&I customers and residential/small commercial customers)
- **Market operations**, including energy market, ancillary services, demand response, load management, feed-in tariffs, pollutant cap-and-trade, and other market-based approaches
- **Building, homes, and industries**, covering building management systems, home area networks, industrial energy management systems, and other customer systems.

Cross-cutting these domains are a couple of critical areas, namely:

- **Cyber and physical security**, for end-to-end security due to inadvertent mistakes/failures as well as deliberate attacks, including security policies, identity establishment, role-based access control, threat detection, threat deferral, procedures and

technologies to function during an attack, procedures and technologies to recover from attacks, and audit capabilities to prosecute or prevent future attacks.

- **Network and system management,** to "manage" the computer and communication systems just as the power system is "managed".
- **Specification and engineering,** to map business processes and functional requirements into detailed specifications and engineering solutions.
- **Conformance and interoperability testing,** to prove vendor implementations are truly conformant with standards and/or are interoperable with other relevant vendor systems.
- **Cross-enterprise identity management,** to ensure information is truly understood across domains and across different corporations.

These domains can be further divided into Environments with similar Smart Grid requirements (see Figure 1). Another way of viewing the Smart Grid domains is shown in Figure 2.

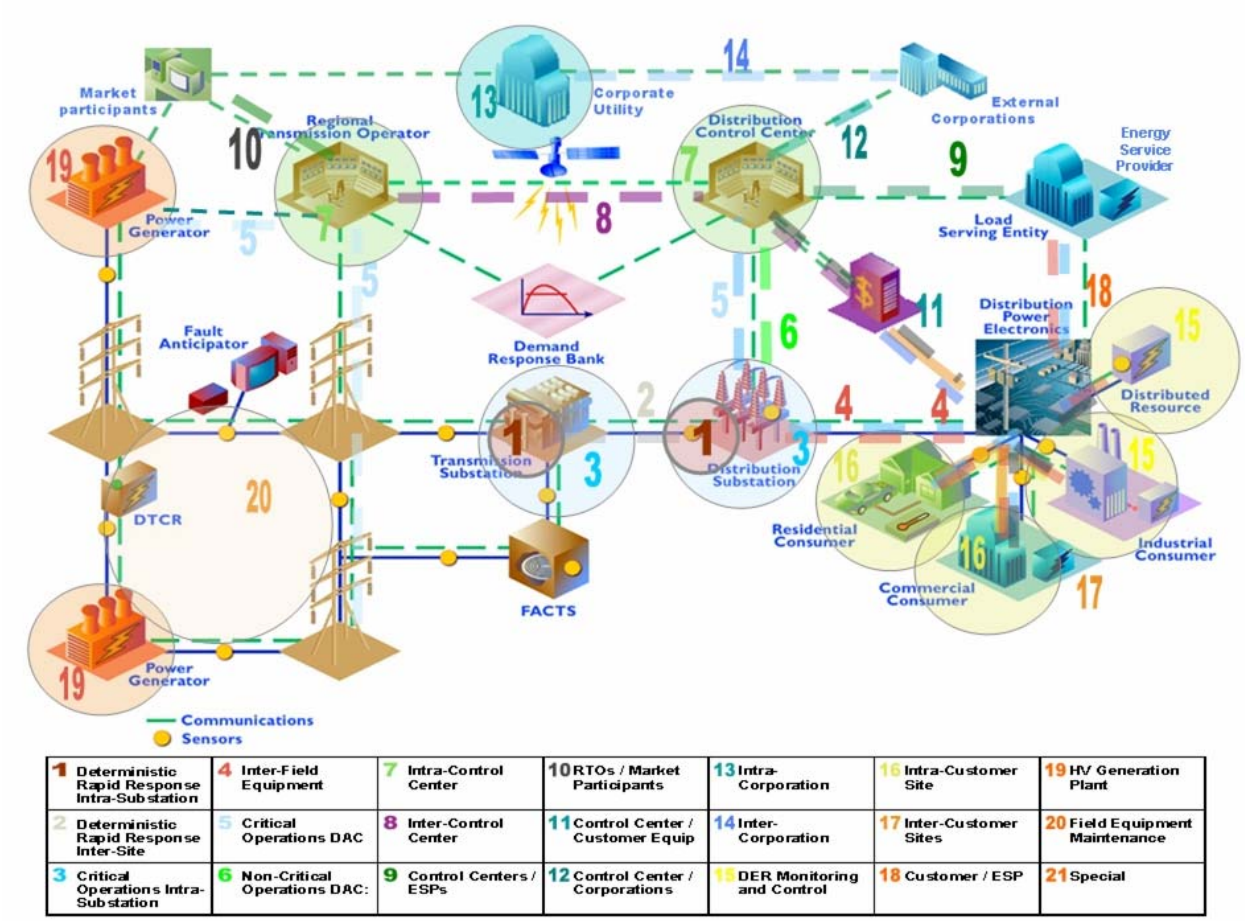


Figure 1: Electric Power Grid Environments

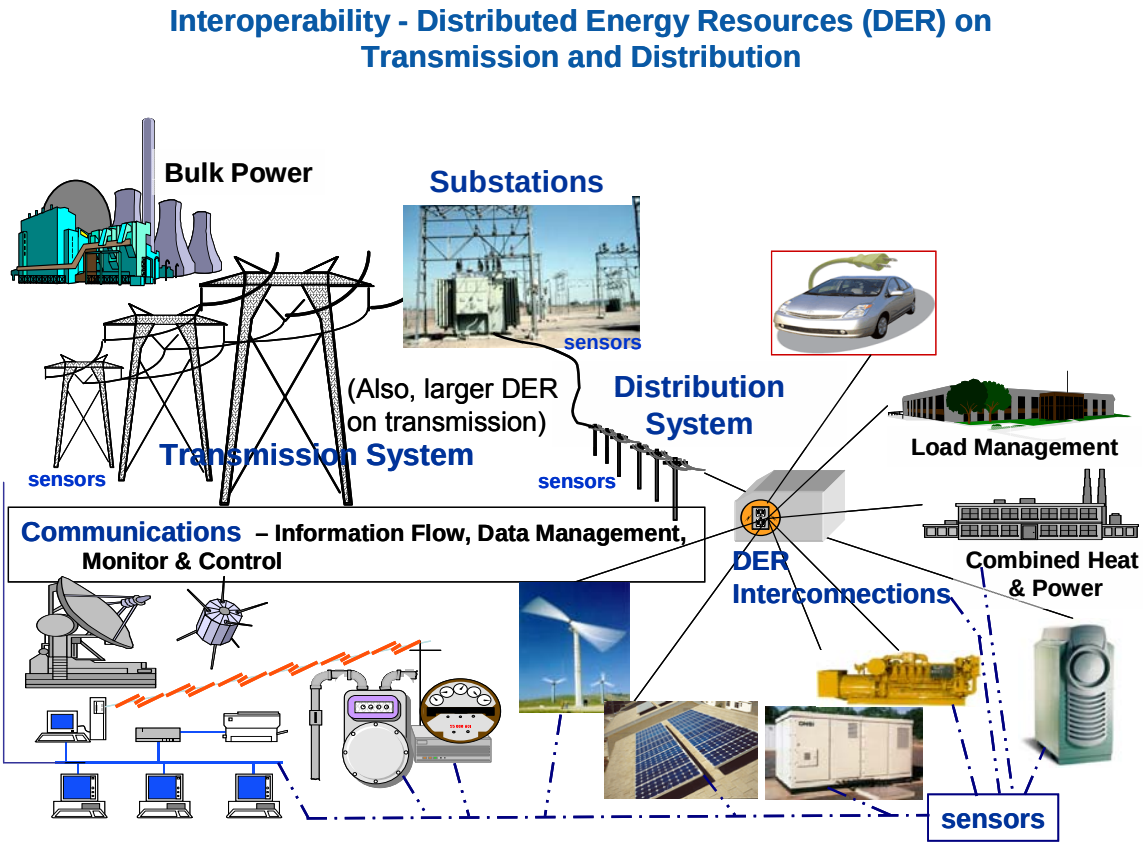


Figure 2: Interoperability across multiple domains

1.4 NIST Domain Expert Working Groups (DEWGs)

As part of the effort to understand the requirements of 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.

Between and within the domains 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.

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

  - Specifies points of interface clearly
  - Uses open architecture and open standards[1]
  - Specifies results, not a specific technology
  - Promotes interchangeability – encourages vendor competition
- Interconnectivity and Security
  - Has physical and electronic interconnection capability
  - Uses standard communication protocols
  - Makes information available to all authorized devices and users
  - Can manage multiple devices using a common command
  - Meets at least basic NERC cyber-security requirements
  - Has adequate redundancy to ensure reliability and safety
- Evolutionary Capability and Service Life
  - Device is upgradeable via software upload
  - Device/project is backwards compatible
- Collaborator Independence
  - Device/project is transactive rather than command/control

2. Smart Grid Domain Functional Requirements

The following sections identify the key near term and longer term functional requirements within the different domains. This document only identifies the requirements, but points to other documents that describe the details.

2.1 Smart Grid Functional Requirements for the Domains

{**Note**: Use the level of detail found in the Distribution Grid section for the needed additions to the other sections.}

2.1.1 Central Generation and Storage Functions

- ISO/RTO monitoring and control of generation and storage
- Variable renewable energy scheduling and management
- Renewable energy generation meteorological forecasting
- Central generation interconnection planning and implementation

2.1.2 Distributed Energy Resources Functions

- Management of two-way flows of energy
- Distribution automation with DER
- Distribution protection schemes with significant penetration of DER
- Pre-planned and emergency microgrid management and operation
- DER device and plant operations
- DER planning and maintenance management
- Also see distribution operations with DER
- Also see market operations with DER

2.1.3 Transmission System Functions

- Transmission planning, including new transmission construction for managing large solar and wind plants
- ISO/RTO management of transmission
- Transmission operations
- FACTS
- Remedial Action Schemes
- Synchrophasor measurements

2.1.4 Distribution Function Systems

A relatively comprehensive list of Primary Distribution Automation functions (needed by most other functions and providing basic Smart Grid functionality) and Secondary Distribution Automation functions (the functions reliant on the primary functions, but providing significant additional Smart Grid benefits) is shown below. This list will continue to grow as new concepts, technologies, and challenges inspire new functions.

Table 1: Distribution System Functional Requirements

Distribution System Functional Requirements	
Primary Distribution Automation Functions	
a. Monitoring and control of distribution equipment within substations • Distribution SCADA System Monitors Distribution Equipment in Substations • Supervisory Control on Substation Distribution Equipment • Substation Protection Equipment Performs System Protection Actions • Reclosers in Substations b. Local automation of DA equipment on feeders • Local Automated Switch Management • Local Volt/Var Control • Local Field Crew Communications to Underground Network Equipment c. Monitoring and control of DA equipment on feeders • SCADA Communications to Automated Feeder Equipment • SCADA Communications to Underground Distribution Vaults d. Management of Distributed Energy Resources (DER) systems • Protection Equipment Performs System Protection Actions on DER Interconnections • Monitoring of DER Units • Controlling DER Units e. DA analysis software applications • Study-Mode and Real-Time Distribution System Power Flow (DSPF) Model • DSPF /DER Model of Distribution Operations with Significant DER Generation/Storage f. Advanced Metering Infrastructure (AMI) • Implementation of AMI to Industrial, Commercial, and Residential Customers • Direct Customer Load Control	
Secondary Distribution Automation Functions	
Operational DA functions	1. Real-time normal distribution SCADA operations to substations • Alarm Processing • Distributed Energy Resources (DER) in Substations • SCADA System Provides Data to Mobile Computing Devices 2. Local automation of feeder equipment beyond substations • Reclosers Interact with Field Equipment • Local Field Crew Communications to Automated Feeder Equipment 3. Remote monitoring and control of automated feeder equipment, possibly using the AMI system for communications 4. Normal distribution operations using the Distribution System Power Flow (DSPF) model • Adequacy Analysis of the Distribution System to Meet the Load

Distribution System Functional Requirements	
	• Reliability Analysis of Distribution System to Minimize Outages • Contingency Analysis (CA) of Distribution System • Efficiency Analysis of Distribution System • Optimal Volt/Var Control of Distribution System • Relay Protection Re-coordination (RPR) of Distribution System 5. Emergency distribution operations using the DSPF model • SCADA System Performs Disturbance Monitoring • Automated Fault Location, Fault Isolation, and Service Restoration (FLISR) • Multi-level Feeder Reconfiguration (MFR) • Load Management Activities for Emergency Conditions • Mitigating the Effects of Major Storms, Earthquakes, and other Disasters • Enhancing Repair Activities After Major Disasters 6. Distribution system operations training and assessments using the DSPF model • Dispatcher Training Simulation (DTS) • Audit Logging and Reporting • Diagnostic Analyses of Events
Automated Distribution Systems - with Significant DER	1. Planning for interconnection of DER to the distribution system • Assessment of Proposed DER Interconnections • Engineering, Monitoring, and Analyzing DER Interconnections 2. Energy Service Provider (ESP) management of DER units • ESP Monitors Non-Operational Data from DER Site • ESP Manages Market Operations of DER Units 3. Local and basic SCADA operations with DER units • Utility SCADA Monitoring and Control of DER Units • Supervisory Control of Switching Operations with Significant DER • Local Automated Switching Operations (IntelliTeam) with Significant DER 4. Normal distribution operations with significant DER using DSPF / DER models • Adequacy Analysis of Distribution System with Significant DER Generation/Storage • Reliability Analysis with Significant DER Generation/Storage • Contingency Analysis with Significant DER Generation/Storage • Efficiency Analysis with Significant DER Generation/Storage • Optimal Volt/Var Control with Significant DER Generation/Storage • Relay Protection Re-coordination (RPR) with Significant DER Generation/Storage • Assessment of the Impact of/on DER Generation/Storage during Distribution Planned Outages 5. Emergency distribution operations with significant DER using DSPF / DER models • Fault Location, Fault Isolation, and Service Restoration (FLISR) with Significant DER Generation/Storage • Multi-Level Feeder Reconfiguration (MFR) with Significant DER Generation/Storage • Post-Emergency Assessment of DER Responses and Actions 6. Customer-driven actions with significant DER generation / storage • Planned Establishment of Temporary Microgrids • Emergency Establishment of Microgrids during Power Outage or Other Emergencies

Distribution System Functional Requirements	
Customer interactions related to automation	1. Use of Advanced Metering Infrastructure (AMI) information in distribution operations • Automatic Meter Reading (AMR) • Customer Outage Detection and Correlation to Fault Location • Assessment of Customer Power Quality 2. Customer demand response • Customer Response to Demand Response Signals • Analysis of Demand Response • Demand Response Interactions with Home Automation Networks 3. Customer use of DER generation / storage • Customer Use of DER for Self-Supply • Plug-in Hybrid Electric Vehicle (PHEV) as Combined DER Generation and Storage • DER Units Bid into Market Operations
Distribution Planning	1. Operational planning • Assessing Planned Outages • Storm Condition Planning 2. Short-term distribution planning • Short-Term Load Forecast • Short-Term DER Generation and Storage Impact Studies 3. Long-term distribution planning • Long-Tem Load Forecasts by Area • Optimal Placements of Switches, Capacitors, Regulators, and DER • Distribution System Upgrades and Extensions • Distribution Financial Planners
Maintenance, engineering, and construction	1. Distribution system equipment maintenance • Predictive Maintenance Application Assesses Distribution Equipment • Management of Maintenance Assets • Scheduling of Maintenance and Equipment Replacement • Maintenance Updates to Documentation and Maps • Maintenance of DSPF Model and Other DA Applications 2. Distribution system design and engineering • Design and Engineering of Substations and Feeders • Specification of Distribution Equipment 3. Construction management • Asset Tracking and Updating • Planning Construction Projects

2.1.5 Customer – Utility Interaction Functions

This domain covers the utility interactions with the customer site equipment, including meters and interfaces to the Home Area Network (HAN). It does not cover the HAN functions themselves.

- TOU tariffs, demand response tariffs, feed-in tariffs, and other incentives for customer actions
- AMI systems design and deployment

- Demand response programs design and deployment
- Load management, both direct and indirect
- Interfaces to HAN systems (OpenHAN for residential, OpenADR for larger C&I customers)
- PHEV interconnections and management, including both load and generation capabilities

2.1.6 Electric Market Operations Functions

This domain covers the market operations

- ISO/RTO market operations, including both energy and ancillary services
- DER market operations, including both energy and ancillary services
- Customer load management and demand response market operations
- Communication requirements for retail market operations (e.g. AMI?, Internet?, Other?)

2.1.7 Buildings, Homes, and Industries Functions

This domain covers the functional requirements for systems within buildings, homes, and industries:

- Energy management systems
- Building management systems
- DER management systems
- Home management systems
- ??

2.2 Functional Requirements for Cross-Cutting Areas

2.2.1 Cyber and Physical Security

- Security policies, as well as training and enforcement
- Security risk assessment
- Security requirements
- Security specifications
- Identify establishment
- Authentication
- Confidentiality
- Integrity
- Availability
- Non-repudiation / Accountability
- Intrusion detection
- Audit logging and reporting

2.2.2 Network and System Management

- Network design to meet performance and security requirements
- System design with embedded security tools and mechanisms

2.2.3 Specifications and Engineering

- Specifications need to map the business or functional requirements into engineering requirements
- Engineering design and implementation is needed to develop products and systems from the specifications
- Integration is needed to interconnect all the equipment and systems into a functioning whole.

2.2.4 Conformance and Interoperability Testing

- Conformance testing for vendors against standards
- Interoperability testing of two or more systems with each other to ensure interoperability

2.2.5 Cross-Enterprise Identity Management

One of the key cross cutting issues that must be solved is the "reference data and ID management" across the integration-sphere. Utility enterprise attempts to solve it using ID mapping or Master Data Management. The problem gets a lot more difficult to solve when multiple businesses are involved in an end-to-end business process integration.

There are no known and mature standards that can be readily applied in this area. A combination of centralized ID management and localized mapping services is probably a model that can scale to support Smart Grid needs.

3. Interoperability and Standards

3.1 Interoperability: What Does It Really Mean

3.1.1 Interoperability: Analogy to Language

Interoperability can be defined as "*the ability of two or more systems or components to exchange information and to use the information that has been exchanged*"[2]. The second part of this definition is very important: not only must computer systems exchange information, but they must also be able to *understand* that information.

A useful analogy for cyber interoperability is human interoperability, namely the ability of disparate people speaking different languages to communicate with each other. Within their own groups (or like applications within their own computer systems), the Germans would speak Deutsch, the French français, and the Martians ⌘⌘⌘⌘. But if these groups need to communicate with each other (or like computer systems which need to exchange information), then English has been accepted as the common language. Similarly, common cyber language(s) must be accepted and standardized (see Figure 3 and Figure 4).

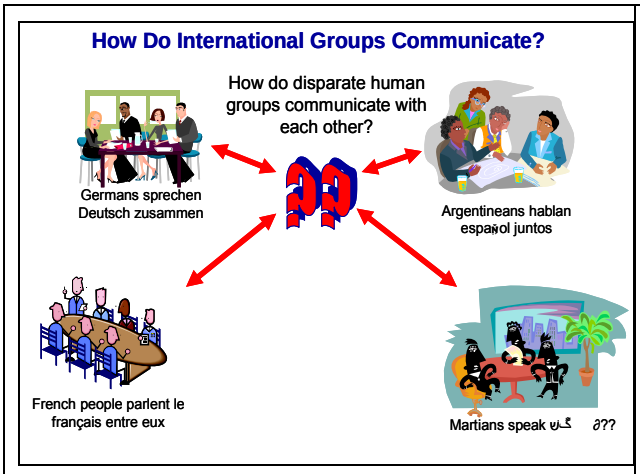


Figure 3: How do international groups communicate?

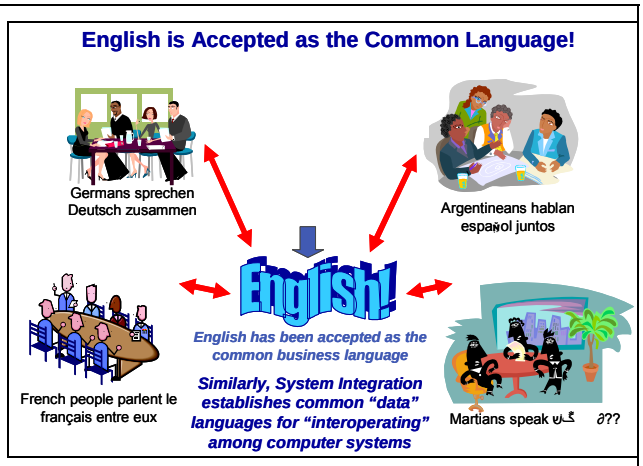


Figure 4: English is accepted as the common language

The analogy with language goes even farther. Just like English, cyber languages must have nouns (data), verbs (send, transmit on event, acknowledge), and grammar (rules for formatting, sending, and responding to messages). In the past, cyber languages were similar to pidgin languages – very simple nouns, verbs, and grammar, just enough to get by for simple transactions. However, as computer systems have become more sophisticated, and as information exchanges need to be more precise, flexible, and covering more topics, "pidgin" cyber has become inadequate. As stated in the second phrase of the definition of interoperability, computer systems must be able to "use" the

[2] [IEEE 90] Institute of Electrical and Electronics Engineers, *IEEE Standard Computer Dictionary: A Compilation of IEEE Standard Computer Glossaries.* New York, NY: 1990.

information, and therefore must understand it completely (first year high school English is not adequate for a Martian to take part in an international conference).

The Internet has provided many of the basic (transport level) components of cyber language, with IP addresses, Ethernet LAN networks, and XML-based technologies. However, it cannot provide the nouns nor the specialized verbs and grammar needed for all industries (application levels); these must be provided by the industries themselves. In particular, nouns for the medical industry are vastly different than the nouns for the financial industry, which are vastly different from the nouns for the power industry. This again is not unlike languages: the English words "cellphone" and "metadata" did not exist 20 years ago, while the words "breaker", "bus", "fuse", and "network" now have vastly different meanings in power industry than in general terminology.

The power industry, particularly through IEC standards, is expanding the vocabulary and grammar of cyber language.

3.1.2 Interoperability: Analogy to Societal Rules for Using Language

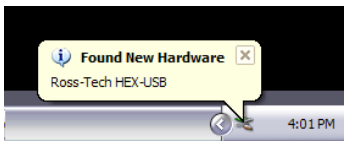
Although a common cyber language is the primary requirement for interoperability, additional requirements also are important. These can be viewed as analogous with societal rules for using language.

Societal rules dictate that a person answering a telephone call says, "Hello," or otherwise indicates that they are now on the call. The caller typically identifies them self in response. The two then take turns speaking. Societal rules also dictate that cellphones should not be used where they interrupt others, such as in theaters or meetings.

In order to have effective communication, everyone should not speak at the same time, and should follow basic rules for interacting. In meetings, a chairperson moderates (but does not dominate) the discussion. Attendees introduce themselves if necessary. Meetings are attended by those that were invited -- if someone should not be in a meeting, they are asked to leave. If discussions become heated, they are halted. If a meeting participant wanders off topic, the meeting leader brings the discussion back to topic. Meetings start at a designated time, and should end as scheduled.

The same types of rules hold true for interoperable cyber systems. Interactions between all systems should be monitored to ensure security and performance rules are being met. Systems should "introduce" themselves. No system should "hog" the network. If a system is disrupting normal interactions (deliberately or inadvertently), it should be cut off. If the interactions are confidential, then any unauthorized system should be locked out. Messages should have well-established time-frames for being exchanged.

3.1.3 Benefits of Interoperability to Stakeholders



An excellent example of the benefits of interoperability is the connection of a new printer or digital camera to a personal computer, where the computer handles the entire integration without human intervention. The moment the new device is connected, the computer displays "*Found New Hardware.*" Moments later it displays "*Found*

an HP xxxx printer" (or other hardware), then displays "*Printer ready to be used.*" The user then merely clicks "print" to print out their document.

If all meters, distribution equipment, substation equipment, back office applications, and SCADA systems could act the same way, then true interoperability would be realized. In this example, no human intervention (other than plugging in the printer) was necessary for the printer to be fully operational. Imagine if the same scenario were to be take place when installing smart meters, connecting distribution automation equipment, or upgrading to a new Meter Data Management system. The savings in personnel effort would be tremendous -- decreasing truck rolls, minimizing engineering time, and avoiding user frustration and mistakes.

3.1.4 Interoperability Challenges: Technical, Security, and Financial

Unfortunately, interoperability is still not there for scenarios more sophisticated than adding a printer to a Microsoft or Apple operating system. Although the Internet has provided many of the transport-level standards (e.g. IP addresses, Ethernet), some systems developed for the power industry still do not use them (e.g. legacy systems often use proprietary protocols). Very few systems have implemented the existing application-level communication standards, and therefore need human intervention to establish translation tables to map data: "the 3rd wire on the 2nd computer card is voltage on phase A" or "the data received is a 1 – does that mean the switch is open or is closed?". This situation is more like a United Nations meeting, where translators must be hired to convert in real-time from the speaker's language to another language – a cumbersome, expensive, and not always accurate methodology.

Furthermore, not all needed standards have been developed yet, much less implemented by vendors. Particularly in the novel realm of AMI, utilities must install proprietary systems, given the long lead time needed for new standards to be developed. Even if a new standard is developed and touted as the perfect answer, "paper" standards always need to go through extensive assessment and testing on "real" systems before they are ready for general deployment.

Security has also made interoperability more of a challenge. No longer can someone just plug in a new device, but it must be authenticated. For instance, if a disgruntled employee plugged in a device that Microsoft thought was a printer, but really was a "Man-in-the-Middle" hacker's device, he could snoop on all information that was being printed. So new measures to ensure the real identity of devices must also be developed and installed.

Financial considerations are also primary in moving toward interoperability. Even if all the new technology, standards, and security were available, no utility could afford to throw out older, non-compliant systems. Therefore migration paths toward interoperability have to be planned, with systems, applications, and devices gradually replaced.

Vendors also cannot afford to upgrade their systems the moment a new standard is approved. This is in part just the time and effort to implement the new standard, but a larger financial burden is in the extensive testing of the upgraded systems – utilities cannot install patches on a weekly basis as Microsoft has forced users of Windows to do, particularly for revenue-sensitive equipment such as meters.

And, as wryly stated by some standards experts, "*The best thing about standards is that there are so many to choose from,*" -- leaving many vendors and utilities perplexed about which standards

will have the staying power and flexibility required to remain relevant for a reasonable number of years.

3.2 Standards: Meeting the Challenges of Interoperability

3.2.1 Purpose of Interoperability Standards

The purpose of interoperability standards is to formalize the nouns, verbs, grammar, and societal rules for exchanging information, or as stated in cyber-speak, to formalize the object model semantics, the messaging syntax, the communication profiles, and the network/security management.

3.2.2 Types of Standards

Standards come in many different flavors, with many different types of standards. Most standards focus on only specific levels (although there are not usually "clean" distinctions between levels). Broadly, there are four levels of cyber standards:

- Media-related standards specific to fiber optics, microwave, WiFi, CATV, wires, telephones and cellphones
- Transport-related standards such as Internet standards including Ethernet, IP, TCP, HTTP, OPC
- Application-related standards such as HTML, XML, IEC 61850, Common Information Model (CIM), and MultiSpeak
- Security-related standards such as AES 256, PKI, secret keys, and Certificates

Often de facto standards are developed either by a dominant corporation (e.g. IBM's ASCII and Microsoft's OLE) or by a consortium of interested vendors (e.g. Zigbee Alliance). These de facto standards have not been "blessed" by a standards organization, but can nonetheless be widely used. In many cases, successful de facto standards eventually become formalized into real standards. In other cases, recommended practices can help narrow the choices.

Another aspect of standards is that they cannot be too rigid, but must still leave flexibility for systems to add new functionality or select certain options. Many standards come with both mandatory requirements and optional selections, as well as with "extension rules" for expanding the standards in a consistent manner for new functions. This is often viewed as the 80/20 rule, namely that standards should address about 80% of the interoperability needs, but typically at least 20% must remain for vendor-specific requirements or utility-specific requirements, as well as the flexibility to meet unforeseen requirements in the future.

Most standards are developed by vendors and consultants, with some, but very often not enough, utility involvement.

4. Overview of Standards Bodies

4.1 Overview of Information Standards Bodies

4.1.1 International Electrotechnical Commission (IEC) TC57 Standards

The interrelationship between IEC TC57 information modeling standards is illustrated in Figure 5.

IEC 61850 is used for field communications. This illustration shows as horizontal layers the three components to an information exchange model for retrieving data from the field, namely, the abstract information models, the service models, and the communication protocol profiles that the abstract information models are mapped into. The different IEC 61850 information models are shown as vertical bars:

- Substation automation (IEC 61850-7-4)
- Large hydro plants (IEC 61850-7-410)
- Distributed energy resources (DER) (IEC 61850-7-420)
- Distribution automation (under development)
- PHEV and additional DER (under development)

IEC 61970 and IEC 61968, the Common Information Model (CIM), is used for enterprise-level communications. The CIM is an abstract model of utility-specific data. Service models such as the GID are defined, but no mapping between the CIM to these service models is specified. The different IEC Common Information Models (CIM) are shown horizontally:

- Transmission CIM (IEC 61970)
- Distribution CIM (IEC 61968)

IEC 62351 security standards cut across the other IEC standards, and consist of:

- Protocol-specific security standards for IEC 61850, IEC 60870-5, IEC 60870-6 (ICCP), and by extension, DNP3 (IEC 62351, Parts 3-6)
- Network and System Management (NSM) (IEC 62351-7)
- Role-Based Access Control (RBAC) (IEC 62351-8)

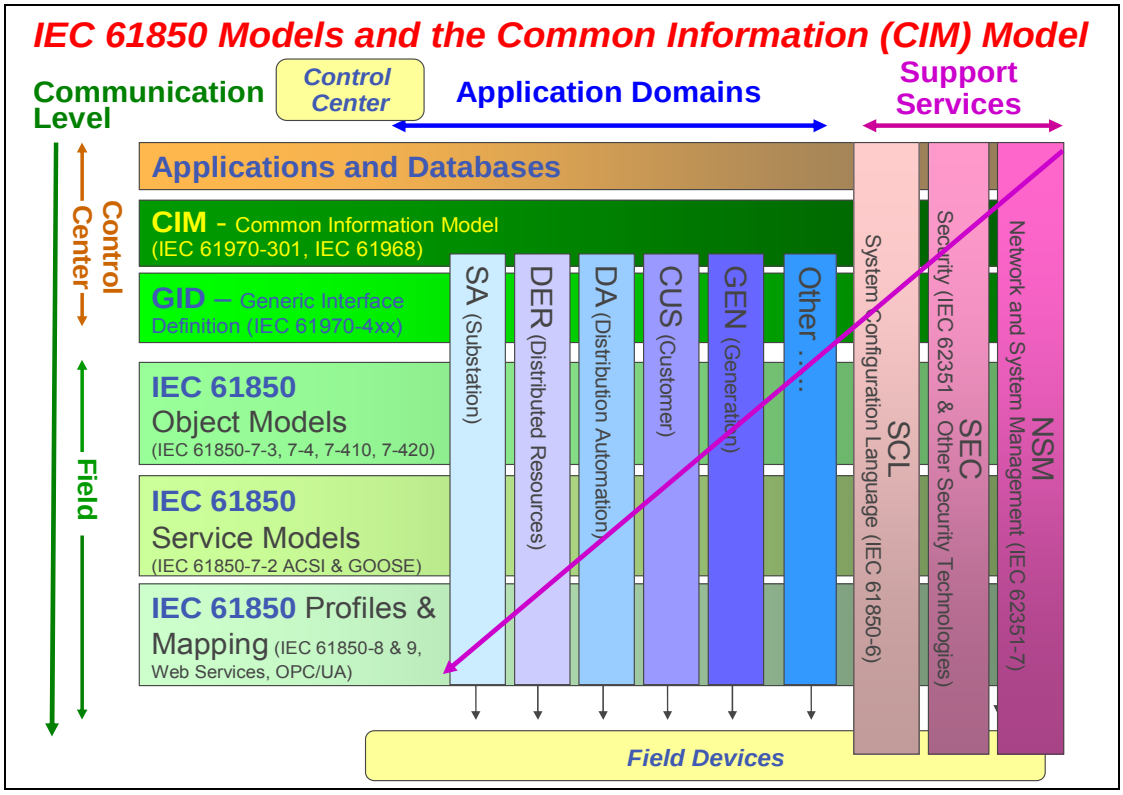


Figure 5: IEC TC57 Information Standards

4.1.2 Institute of Electrical and Electronic Engineers (IEEE)

The IEEE has a similar methodology to that of the IEC for developing draft and, ultimately, final standards, only IEEE voting is performed by members of the working groups, not by National Committees. Membership in working groups is much more flexible, typically requiring only that members show up for the meetings and actively participate in the work.

In addition, the IEEE working groups develop many other types of documents, including Recommended Practices, Technical Reports, Conference Papers, and other non-standards-oriented documents.

The IEEE has developed many standards, but those of greatest interest for communications and interoperability are:

- IEEE 802.3 (Ethernet)
- IEEE 802.11 (WiFi)
- IEEE 802.15.1 (Bluetooth)
- IEEE 802.15.4 (Zigbee)
- IEEE 802.16 (WiMax)
- IEEE P1547 series on DER interconnection (some complete, some pending)
- IEEE P2030 Guide for Smart Grid Interoperability of Energy Technology and Information Technology Operation with the Electric Power System (EPS), and End-Use Applications and Loads (pending)

4.1.3 Internet Engineering Task Force (IETF)

The IETF is responsible for Internet standards, many of which are now widely implemented in private Intranets as well. A Request for Comment (RFC) document is the mechanism used by the IETF to develop, send out for comment, and finalize standards. Usually, RFC specifications must be implemented by more than one vendor before they can be fully accepted as standards.

Some of the key IETF RFCs are:

- RFC 791: Internet Protocol (IP)
- RFC 793: Transport Control Protocol (TCP)
- RFC 1945: HyperText Transfer Protocol (HTTP)
- RFC 2571: Simple Network Management Protocol (SNMP)
- RFC 3820: Internet X.509 Public Key Infrastructure (PKI) for security

The full list of relevant IETF standards needs to be identified, although a draft list can be found on the IntelliGrid web site.

4.1.4 American National Standards Institute (ANSI)

Like the other standards organizations, ANSI has working groups which work on specific standards, and update them as necessary. The most relevant ANSI standards for interoperability of AMI systems include:

- ANSI C12.19 (metering "tables" internal to the meter). This document is currently under revision
- ANSI C12.22 (communications for metering tables)

4.1.5 National Institute of Standards and Technology (NIST)

NIST has developed Special Publications in the 800 series which provide documents of general interest to the computer security community. These are more guidelines than standards, but are very important for moving toward secure interoperability. Two documents of particular interest for the Smart Grid are:

- NIST SP-800-53: Recommended Security Controls for Federal Information Systems
- NIST SP-800-82: Guide to Industrial Control Systems (ICS) Security

4.1.6 North American Electric Reliability Corporation (NERC)

NERC has recently issues security standards for the bulk power system. Although these security standards are explicitly for the bulk power system, it is clear that many of the requirements also apply to distribution and AMI systems, and may eventually become standards for these systems as well. The NERC CIP 002-009 Security Standards cover:

- (2) Critical Cyber Asset Identification, (3) Security Management Controls, (4) Personnel and Training, (5) Electronic Security Perimeter(s), (6) Physical Security of Critical Cyber

Assets, (7) Systems Security Management, (8) Incident Reporting and Response Planning, and (9) Recovery Plans for Critical Cyber Assets

4.1.7 World Wide Web Consortium (W3C)

The W3C develops interoperable technologies (specifications, guidelines, software, and tools) for the world wide web, including:

- HTML for web page design
- XML for structuring documents and other object models
- Web services for application-to-application communications, such as SOAP for transmitting data

4.2 Users Groups and Collaborative Efforts within the Power Industry

Standards can only define exactly how a specific interface must be structured, but do not address which standards may be the best for different requirements, or which optional parameters to implement. Standards cannot be developed in a vacuum, so input for updates and corrections, based on real-world implementation, need to be fed back to the various standards groups. Additionally, education and training on the capabilities of different standards are vital to utilizing the standards correctly and effectively.

Many users groups, collaborative efforts, associations, alliances, and other non-standards organization provide these refinements, feedback, and educational programs. Some of the key groups related to Smart Grid requirements are described below.

4.2.1 UCA International Users Group (UCAIug)

The UCA International Users Group (UCAIug) was developed specifically to address user requirements for the IEC standards as well as, more recently, AMI- and Smart Grid-related issues. In particular, three active subcommittees cover:

- IEC 61850
- CIM
- OpenDR

Within UCAIug, CIMug is a forum to include all parties interested in using CIM for utility system integration.

Very active working groups and task forces are addressing AMI issues (OpenAMI), security for AMI (AMI-SEC), Home Area Networks (OpenHAN), and AMI Enterprise issues (AMI-Enterprise).

AMI-ENT under Open SG is another user driven group that are developing use cases, requirements and integration services (both XSD and WSDL) for AMI related system integration, which provide a foundation for Smart Grid.

AMI-SEC is developing security requirements and specifications for AMI systems.

4.2.2 NRECA's MultiSpeak

The National Rural Electric Cooperative Association (NRECA) is sponsoring a very successful industry-wide consortium, called the MultiSpeak® Initiative, consisting of software vendors, consultants, and utilities. The initiative is sponsored by the National Rural Electric Cooperative Association and has focused on well-defined interoperable interfaces for smaller utilities that often lack the resources to develop their own protocols. The MultiSpeak specification defines each application interface in a very clear manner through the command and payload semantics without a need to rely upon the possible variations of information infrastructure (e.g., "middleware") at the utility. This approach facilitates interoperability between vendors and results in interfaces that interoperate among business partners. Feature sets are scalable to better enable appropriate integration, and there are clear rules for extending the protocol. The data model is maintained in XML schema form and interfaces are defined using either web services or a messaging framework. The MultiSpeak specification covers the same domain as IEC 61968, Distribution CIM.

Presently MultiSpeak defines 25 interfaces for functions such as meter reading, connect/disconnect, meter data management, outage detection, load management, GIS, SCADA, demand response, and distribution automation control. All of these interfaces are mature and interoperability testing is provided for all of the interfaces by an independent, third party service testing laboratory.

4.2.3 Cigré

Cigré, the International Council on Large Electric Systems, is a parallel organization to the IEC, but focuses on discussions and reports related to key issues for the electric power industry, and are typically authored by utility personnel.

Cigré has a number of working groups which are tasked with developing reports on communications, cyber security, and interoperability issues. Some of these reports are used to suggest the types of standards that should be developed, usually by the IEC.

4.2.4 GridWise™ Alliance

The GridWise Alliance "*is a consortium of public and private stakeholders who are aligned around a shared vision. A vision of an electric system that integrates the infrastructure, processes, devices, information and market structure so that energy can be generated, distributed, and consumed more efficiently and cost effectively; thereby achieving a more resilient, secure and reliable energy system.*" The GridWise Alliance is working with the Department of Energy and helps to sponsor conferences and workshops, such as the GridWise Architecture Council, Grid Interop, GridWeek, and EPRI's IntelliGrid projects.

4.2.5 Electric Power Research Institute (EPRI) IntelliGrid

In 2003, the Electric Power Research Institute's (EPRI) initiated the IntelliGrid project to develop guidelines on interoperability and standards, and the IntelliGrid reports were published in 2005. Since then, EPRI has sponsored projects with utilities to use the IntelliGrid recommendations.

4.2.6 Vendor Collaborations

Many collaborations and alliances of vendors have been initiated to resolve the details of standards and to develop vendor agreements on which aspects of the standards are to be implemented. Some relevant vendor alliances and collaborations include:

- Zigbee Alliance
- HomePlug Powerline Alliance
- The combined Zigbee/HomePlug working group to develop the Smart Energy Profile
- ISA SP-100 wireless radio groups

4.2.7 Utility Standards Board

The Utility Standards Board (USB) is a group of utilities working jointly to develop de facto standards related to the interface between the AMI system and utility systems (see Figure 6), including back office metering, billing, and revenue protection, as well as distribution operations such as outage management, power quality, and load management.

This funded effort provides utilities with excellent forums for discussing AMI issues, and is providing significant input into the formal IEC standards-development process as the de facto standards are released through the UCA Users Group to the IEC.

Through their participation in the USB, utilities are taking the lead in providing the Business Processes as a foundation for developing interoperability standards.

Current work includes:

- Meter/Headend Event Codes
- Remote Connect/Disconnect
- Outage Management

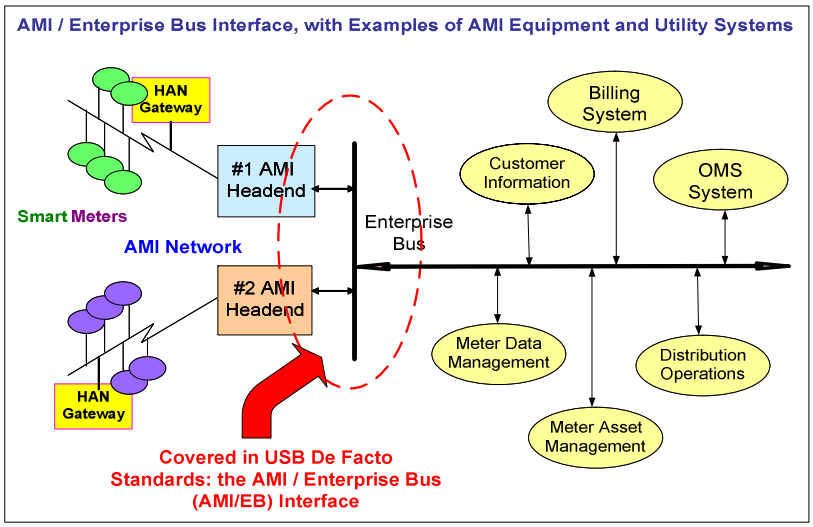


Figure 6: USB Scope: AMI/Enterprise Bus Interface

5. Existing Smart Grid-Related Standards and Recommended Practices

EPRI's IntelliGrid Architecture identifies many standards, widely used technologies, and recommended practices. (Temporarily, the web site http://intelligrid.ipower.com/IntelliGrid_Architecture/Overview_Guidelines/index.htm provides public access to these slightly dated (2004) lists of standards.)

The sections below identify the key existing standards that are related to the Smart Grid.

5.1 Existing Smart Grid Standards for Domains

5.1.1 Central Generation and Storage

- DCS management systems
- ICCP (informal name for IEC 60870-6 TASE.2)
- ??

5.1.2 Distributed Energy Resources

- IEEE 1547 for DER physical and electrical interconnection
- IEEE 1547.3 for information modeling recommendations
- IEC 61850-7-420 for information exchanges with DER devices and systems

5.1.3 Transmission Grid

- IEC 61850-7-4 for substation automation
- IEC 61970 Common Information Model (CIM) for enterprise modeling of the transmission system
- DNP3 for SCADA
- IEEE ??? for synchrophasor measurements

5.1.4 Distribution Grid

- IEC 61968 CIM for distribution in the enterprise
- MultiSpeak for small distribution utilities
- IEC 61850 for distribution automation (under development)
- DNP3 for SCADA
-

5.1.5 Customer – Utility Interactions

- ANSI C12.19 for meters
- ANSI C12.22 for communications with meters
- IEC DLMS/COSEM for European metering
- IEEE 802.11 for WiFi
- IEEE 802.15.4 with additions by Zigbee Alliance for meshed radio networks
- IEEE 802.16 WiMax
- HomePlug for HAN using power line
- Smart Energy Profile (combining Zigbee and HomePlug)
- OpenHAN specifications for connections between AMI and HAN

5.1.6 Market Operations

- FERC's Open Access Same-Time Information System (OASIS) for market operations
- State regulations and tariffs (many and often very different)
- Pollutant Cap-and-Trade system (still being defined)

5.1.7 Building, Home, and Industrial Systems

5.2 Existing Smart Grid Standards for Cross-Cutting Areas

5.2.1 Cyber and Physical Security

- Security policies, as well as training and enforcement
- NERC CIP standards for transmission critical assets
- Expansion of NERC CIP to distribution {Add paragraph 7 in section B1}
- Expansion of NERC CIP to customer site?
- AMI-SEC security requirements
- IEC 62351 for IEC protocols and Role-Based Access Control
- Many IETF Internet cyber security services and technologies, such as passwords, PKI, TLS, intrusion detection, IPSec, VPNs, etc. (see IntelliGrid Architecture http://intelligrid.ipower.com/IntelliGrid_Architecture/Technology_Analysis/Anl_Security_Overview.htm
- IEEE 802.11i security for wireless protocols
- Physical security, including locks, 5 or 6-sided containers, video surveillance, etc.

5.2.2 Network and System Management

- Functional requirements for network and system management
- Network management systems such as SNMP v3 and HP OpenView
- System management via IEC 62351-7 NSM standard (in process)

5.2.3 Conformance and Interoperability Testing

- Conformance testing for vendors against standards
- Interoperability testing of two or more systems with each other to ensure interoperability

6. Gap Analysis of Power System "Smart Grid" Information Standards

6.1 Purpose of this Gap Analysis

NIST is required to provide an initial "***Roadmap for Smart Grid Information Standards Activities***" by May 2009. It is well understood that extensive and complex Smart Grid power system requirements, defined in business processes and Use Cases, must drive the development of the information system requirements, including information standards. However, it is also well known, due to prior and on-going work, that there are a number of gaps in the existing standards that must be filled through extensions and new development. As noted by Dr. Steven Chu, Secretary of Energy, not only is there low hanging fruit, there is fruit already lying on the ground, ready to be picked up. These known gaps in the information standards are those ground-lying fruits for the Smart Grid.

Therefore, the purpose of this document is to identify and justify those known gaps in information standards as obvious areas for immediate action.

At the same time, additional work defining both the Smart Grid power system requirements and the necessary information system capabilities to meet those requirements must be continued. The results of that work can be fed into the Roadmap as they are identified.

6.2 Gaps in Infrastructure Information Standards

6.2.1 Distribution and DER Field Equipment Information Standards

Although this document discusses only the gaps in standards, a more complete discussion of Distribution Automation and DER functional requirements can be found in the California Energy Commission (CEC) draft "***Benefits and Challenges of Distribution Automation – Use Case Scenarios***" (link on http://xanthus-consulting.com/pages/publications.htm).

The following standards activities need further development and/or extensions.

Requirement for Standard	Justification for Standard
1. **Need to extend IEC 61850 to distribution automation.** This is under development but does not have the impetus to move forward quickly.	IEC 61850 is an information model, so it is widely seen as the best approach to communications with field equipment. Given that premise, the information model needs to be expanded into additional areas, including distribution automation. Justification for distribution automation includes increased reliability, increased efficiency, increased safety, decreased on-going costs (once it is implemented), and increased environmental benefits.

Requirement for Standard	Justification for Standard
2. **Need to extend IEC 61850 for more Distributed Energy Resource (DER) equipment**. Currently IEC 61850-7-420 for DER covers wind (actually IEC 62400-25), photovoltaic systems, fuel cells, diesel generators, batteries, and combined heat and power (CHP). Needs extension to PHEV, additional storage devices, microturbines, gas turbines, etc.	IEC 61850-7-420 for DER has just been standardized and is being implemented (primarily in Europe), but needs to be expanded to other DER so that the full suite of DER devices can be covered by one information model-based protocol.
3. **Need to develop an IEC 61850-lite**, in which the information models can be mapped to a protocol with less overhead than the current MMS-based mapping.	Distribution automation and DER devices may have only narrowband communications channels or limited data exchanges due to data costs if telecommunication providers are providing the communication channels. In addition, some inexpensive devices (e.g. sensors, collectors, or "software agents") may not want or need to implement the full IEC 61850 capabilities, in order to minimize compute constraints or development costs.
4. **Need to ensure AMI communications systems use open standards capable of interfacing to DER and distribution automation equipment.** ANSI C12.22 is being revised, Europe uses DLMS/COSEM, and AMI vendors are frantically developing their systems over a wide range of media, from PLC, to BPL, to Zigbee meshed radios, to UtiliNet radios, to GPRS, etc, etc.	Since AMI systems are going to become widespread, they will inevitably want to be used for more than meter reading or other purely metering functions. They could be used for monitoring DER at the customer site, for DA monitoring and possibly control, for access by third parties to gateways into the customer HAN, etc. Right now, AMI vendors are using proprietary or semi-proprietary communication protocols "just to get the AMI systems implemented". The AMI systems should be able to handle, at a minimum, the IEC 61850 object models mapped to an "appropriate" protocol (possibly IEC 61850-lite when it is developed).

6.2.2 Customer Site – AMI, Gateways, and HAN Information Standards

Requirement for Standard	Justification for Standard
1. **Review possible constraints in the current finalizing of ANSI C12.22 for communications with the meter.** ANSI C12.22 is being revised, but there are concerns that the results may not meet the requirement to base standards on broader information models – the results may be too metering-only focused (i.e. too focused on ANSI C12.19 metering).	Since AMI systems are going to become widespread, they will inevitably want to be used for more than meter reading or other purely metering functions. (see above)
2. Move toward AMI/HAN standards, based on the OpenHAN specification. The OpenHAN specification (not a standard) was recently developed, but currently there is no actual standard for this interface between the AMI system and the HAN	The AMI systems have their own (often proprietary or based on ANSI C12.22) communication standards to the meter. Within the HAN, HomePlug and Zigbee have standards, but are now working together to develop Zigbee Smart Energy Profile

Requirement for Standard	Justification for Standard
3. Work with Zigbee Smart Energy Profile working group to ensure the information model is complete or can utilize the IEC 61850 information model and/or the CIM information model.	Zigbee Smart Energy Profile for the HAN environment is being developed, but may not yet understand the breadth of requirements that it may ultimately have to handle. This means that the requirements across the AMI/HAN gateway need to be understood, described, and converted into information models.
4. Develop support for ZigBee Smart Energy Profile in IEC61968 and MultiSpeak	Actions that will be taken by HAN devices that are compatible with the ZigBee Smart Energy Profile will have consequences in back office systems. Data models and interaction models must be developed and supported by both IEC61968 and MultiSpeak to support these requirements.

6.2.3 Transmission Field Equipment Information Standards

Requirement for Standard	Justification for Standard
1. **Complete Wide-Area Phasor Measurement monitoring standards.** Work is on-going in this area but is not complete.	Wide area phasor measurements can provide early warning of potential problems as well as input to make rapid (~ 4 ms) control actions to mitigate emergency conditions.
2. Extend IEC 61850 between substations. Some protective relaying and certain other functions require communications between substations, for which 61850 should be used.	IEC 61850 is designed to be used within substations. However, functions such as protective relaying need to communicate between substations. The same protocol should be used for this function.
3. Extend IEC 61850 from the substation to the control center. Since the data in the substation uses the 61850 information model, this data should be reported to the control center using the same information model.	IEC 61850 models all the equipment and functions in the substation. If those models could be brought back to the control center, then this same powerful information model would be used for SCADA and other applications, thus minimizing translations and expensive and data maintenance activities that sometimes lead to insecure and/or unsafe situations.

6.2.4 Utility Enterprise Information Standards

Requirement for Standard	Justification for Standard
1. **Develop Interoperability Standards for the IEC 61970 Common Information Model (CIM).** The CIM for transmission (IEC 61970) does not specify formats or messaging methods for exchanging CIM information, thereby requiring each implementation to develop their own formats and messaging requirements.	The IEC 61970 CIM for transmission is strictly an abstract model with no standardized mechanism for mapping the information model to communication formats and messages, thus making different implementation not interoperable. If CIM format and messaging standards were developed, then CIM implementations could be interoperable.
2. Revise and update parts of IEC 61968 Common Information Model (CIM) for distribution. CIM for distribution has recently developed some messaging schemes for exchanging CIM information interoperably. However, earlier parts of IEC 61968 do not yet have interoperable messaging schemes.	The IEC 61968 CIM for distribution is currently not usable except for the very latest part (Part 9), since the messaging schemes and the CIM model were not well enough defined to allow vendors to implement them. However, if these older parts are revised, then interoperability of the messages may be achieved. These revisions are in the IEC TC57 WG14 roadmap, but will need significant effort to achieve.

Requirement for Standard	Justification for Standard
3. Develop harmonized profiles between MultiSpeak and IEC 61968.	As the IEC61968 profiles described in item 2 above become available, it will be important to develop mappings between the existing MultiSpeak interfaces and the new IEC 61968 interfaces so that products and software developed to be compatible with the different standards can interoperate.
4. Expand IEC 61968 CIM for DER and PHEV. Although IEC 61850-7-420 for DER has been completed (with more DER models still pending, including PHEV), no CIM models for any DER or PHEV have yet been developed.	IEC 61850 is designed for field communications, while CIM is for enterprise communications. Therefore, CIM models need to carry the 61850 models of DER into the enterprise.
5. Expand MultiSpeak. MultiSpeak, developed by NRECA and very successfully implemented for many smaller utilities, is being expanded as version 4, with more updates to come.	MultiSpeak meets the requirements of the smaller utilities very effectively, but needs to be expanded to add support for HAN and DER, more use of information modeling techniques, and more compatibility with IEC 61968.

6.3 Gaps in Cross-Domain Standards

6.3.1 Cyber Security Standards

Requirement for Standard	Justification for Standard
1. **Extend NERC CIP 002-009 to Distribution and AMI.**	Although explicitly for transmission, and using an asset-based approach which may not always be applicable, the NERC CIP still has very powerful requirements. In particular, these requirements can be used by utilities to develop the security policies that are critical for true security.
2. Complete the IEC 62351-8 Role-Based Access Control (RBAC). RBAC is a general security concept for managing access to information and assets. The RBAC model for utilities is being standardized in the IEC.	RBAC should be used for managing access to all information and assets, but needs both standards and guidelines for clarity and interoperability particularly across different security domains.
3. Complete the IEC 62351-7 Network and System Management (NSM). NSM monitors not only communication networks, but also systems, applications, and databases.	The main purpose of NSM is to detect anomalies which could be intrusions, mistakes, or failures, but which could adversely affect the operation of the grid. In the August 2003 blackout, although the initial cause was equipment failure, the real cause was lack of information flowing to where it was supposed to flow due primarily to mistakes.
4. Develop Key Management Strategies. Key management of the millions of devices and meters is becoming a critical issue, since truck rolls are too expensive for manual key entry, and some communication infrastructures may not be adequate for handling key updates.	Cyber security is only as good as the secrecy of the cyber keys used not only for encryption but also just for authentication. Key management over narrowband communication channels to inexpensive end devices needs resolution and standardization.

Requirement for Standard	Justification for Standard
5. **Develop more detailed security requirements for AMI systems**. AMI-SEC has developed high level security requirements for AMI systems, but these are not detailed enough to provide explicit security requirements for different functions using the AMI systems.	AMI systems are becoming an enormous communications infrastructure that reach into all customer sites. Ensuring that these AMI systems are truly secure enough for the different functions that can be performed across them, is critical. That assurance can only come from more detailed security requirements linked to the different functions.

6.3.2 Standards Interoperability and Conformance Testing

Requirement for Standard	Justification for Standard
1. **Perform interoperability testing for IEC 61968-9**. Interoperability testing is planned for this part in late 2009.	Interoperability testing, along with conformance testing, is the best method for confirming that a standard is performing correctly and actually doing what it is supposed to do. These tests can also feed back to the standards group on issues where the standards are unclear, missing, or incorrect.
2. Perform conformance and interoperability testing of IEC 62351 security standards.	Testing is the most effective way to ensure that these security standards actually provide the level of security expected. Any issues, such as security holes or inconsistencies, can be fed back to the standards group.
3. Perform interoperability testing on harmonized profiles between MultiSpeak and IEC 61968.	Once a mapping between MultiSpeak V4 and IEC61968, Part 9 has been finalized (planned for late 2009), then it will be critical to test for interoperability between appropriate profiles of the two standards.

6.4 Gaps in Smart Grid Applications – Guidelines and Metrics

6.4.1 Purpose of Smart Grid Applications

Applications actually drive the requirements for the infrastructure information standards. However, they themselves should not be standardized, since standards should apply across interfaces, not within software applications. However, many guidelines and examples of business processes should be developed on what functions will be a part of a "Smart Grid".

The benefits of a Smart Grid are expected to be:

- Improving power system reliability
- Improving power system efficiency
- Improving cyber security and safety
- Decreasing utility and/or customer costs over a defined timeframe
- Minimizing the impact on the environment

6.4.2 Metrics for Measuring a Smart Grid

Metrics should be developed to determine the "smart gridedness" of different functions which claim to further these goals.

TBD