Smart Grid:
Interoperability and Standards

Frances Cleveland, Xanthus Consulting International
Forrest Small, Navigant Consulting, Inc.
Tom Brunetto, Distributed Energy Financial Group, LLC

Table of Contents

Executive Summary

The Energy Independence and Security Act of December 2007 recognized the need for a Smart Grid, the modernization of the US electricity system. One of the key requirements of a Smart Grid is the interoperability of the cyber systems that are used to manage the power system. Interoperability among disparate computer systems can only be achieved through the use of internationally recognized communication and interface standards.

A useful analogy for computer interoperability is human interoperability, namely the ability of disparate people speaking different languages to communicate with each other. First, just as international business meetings have agreed to use English as the common "language" standard, computer systems need common cyber "language" standards in order to exchange information with each other. Secondly, cyber standards have analogous components to human languages, namely nouns (data), verbs (messaging), and grammar (rules for exchanging messages). In addition, societal rules guide humans on when to speak at a meeting, (when a computer can send messages), on how to manage security by limiting attendance at a meeting (for a computer by passwords and encryption), and on timeliness of meetings (timeliness of data exchanges).

The perfect example of the benefits of interoperability is the scenario of connecting a new printer, camera, or other new hardware to a personal computer, where the computer handles the entire setup without human intervention. Unfortunately, more complex interactions do not yet have the standards to achieve this, and many more standards need to be developed before this interoperability goal can be achieved in the electric power industry.

Many standards bodies, such as the IEC, IEEE, IETF, ANSI, NIST, NERC, and the W3C are tackling these issues both for the industry at large as well as specifically for the power industry, while Users Groups and Consortia such as the Utility Standards Board (USB) are working to provide input and guidance in developing and implementing these standards.

It is critical to understand that utilities and vendors must often move forward whether or not the standards exist or have been completed. The lag time in developing standards is inevitable, but projects must nonetheless be specified, designed, and implemented without waiting for these standards. In addition, many "legacy" systems cannot be cost-effectively upgraded or replaced to take advantage of relevant standards even when they do exist. Therefore, mechanisms must be utilized for maximizing the benefits that come from interoperability standards while minimizing the delays and expenses of implementing new standards.

In particular, utilities should take the lead in defining the business process requirements, and in specifying and testing the resulting standards in their operations. Vendors may be the technology experts, but the utilities have the requirements expertise.

Interoperability is the key to the Smart Grid, and standards are the key to interoperability. The more involvement by utilities, vendors, and others in the development of standards, the faster the vision of a Smart Grid will be realized.

1 Introduction

1.1 Smart Grid Provisions in H.R. 6, 110th Congress

The Energy Independence and Security Act of December 2007 defines the Smart Grid as follows:

> *"It is the policy of the United States to support the modernization of the Nation's electricity transmission and distribution system to maintain a reliable and secure electricity infrastructure that can meet future demand growth and to achieve each of the following, which together characterize a Smart Grid:*
>
> *(1) Increased use of digital information and controls technology to improve reliability, security, and efficiency of the electric grid.*
>
> *(2) Dynamic optimization of grid operations and resources, with full cyber-security.*
>
> *(3) Deployment and integration of distributed resources and generation, including renewable resources.*
>
> *(4) Development and incorporation of demand response, demand-side resources, and energy-efficiency resources.*
>
> *(5) Deployment of `smart' technologies (real-time, automated, interactive technologies that optimize the physical operation of appliances and consumer devices) for metering, communications concerning grid operations and status, and distribution automation.*
>
> *(6) Integration of `smart' appliances and consumer devices.*
>
> *(7) Deployment and integration of advanced electricity storage and peak-shaving technologies, including plug-in electric and hybrid electric vehicles, and thermal-storage air conditioning.*
>
> *(8) Provision to consumers of timely information and control options.*
>
> *(9) Development of standards for communication and interoperability of appliances and equipment connected to the electric grid, including the infrastructure serving the grid.*
>
> *(10) Identification and lowering of unreasonable or unnecessary barriers to adoption of smart grid technologies, practices, and services."*[1]

This definition of Smart Grid is very broad, encompassing many aspects of electric grid operation and management, and seeking to improve reliability, efficiency, and security, from the generation, transmission, distribution, down to the customer sites. On the other hand, many entities, including the Congressional Research Service, focus the Smart Grid almost exclusively on Advanced Meter Infrastructures (AMI) and the potential services for customers:

[1] US Energy Independence and Security Act of December 2007, TITLE XIII--SMART GRID SEC. 1301. STATEMENT OF POLICY ON MODERNIZATION OF ELECTRICITY GRID

"The term Smart Grid refers to a distribution system that allows for flow of information from a customer's meter in two directions: both inside the house to thermostats and appliances and other devices, and back to the utility."[2]

Although this discrepancy in the definition of Smart Grid could lead to some confusion in general, either definition still depends heavily on the need for interoperability and standards, which are the focus of this paper.

1.2 Glossary of Terms and Abbreviations

The following glossary of terms and abbreviations provides the definitions for many of the concepts and organizations discussed in this paper.

Term/Abbreviation	Definition
AMI	Advanced Metering Infrastructure
ANSI	American National Standards Institute, http://www.ansi.org/
ANSI C12.xx	ANSI standards for metering
Application-level protocols	Protocols which understand the data and therefore know what to do with it (send specific data, store it appropriately, give it to an application program, issue an alarm, etc.)
Cigré	International Council on Large Electric Systems, http://www.cigre.org/
CIM	Common Information Model, IEC 61970
DA	Distribution Automation
DER	Distributed Energy Resources, Distributed Generation and Storage
DOE	Department of Energy, http://www.doe.gov/
EPRI	Electric Power Research Institute, http://www.epri.com
GridWise Alliance	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, http://www.gridwise.org/
HAN	Home Area Network
IEC	International Electrotechnical Commission, http://www.iec.ch/
IEEE	Institute of Electrical and Electronics Engineers, http://www.ieee.org/portal/site
IETF	Internet Engineering Task Force, http://www.ietf.org/
IP	Internet Protocol, provides basic communications between addresses in the form of 168.192.123.001
Media protocols	Protocols which are specific to different media (e.g. cables, wireless, fiber optic, microwave, etc.)

[2] Order Code RL34288, Congressional Research Service Report for Congress, Smart Grid Provisions in H.R. 6, 110th Congress

Term/Abbreviation	Definition
NERC	North American Reliability Corporation, http://www.nerc.com/
NIST	National Institute of Standards and Technology, http://www.nist.gov/
OpenSG	Open Smart Grid, a working group under UCA Users Group, http://osgug.ucaiug.org/default.aspx
Transport-level protocols	Protocols which transport data from one system to another across a network, without needing to understand what the data means.
UCA Users Group	Users Group to enable utility integration through the deployment of open standards by providing a forum in which the various stakeholders in the utility industry can work cooperatively together as members of a common organization. http://www.ucaiug.org/default.aspx
UML	Unified Modeling Language
USB	Utility Standards Board, http://usb.sharepointsite.net/default.aspx
W3C	World Wide Web Consortium, http://www.w3.org/
XML	eXtensible Markup Language, developed by W3C
Zigbee Alliance	Alliance on IEEE 802.15.4-based wireless technology, http://www.zigbee.org/en/index.asp

2 Smart Grid Issues

2.1 Smart Grid Vision: Focus on Customer Interactions

Although the Smart Grid is defined more broadly in the Congressional Act, much of the initial focus has been on interactions with customers as one of the methods for improving electric grid efficiency, reliability, and security.

This focus on energy efficiency has recently been made more feasible through enhanced technologies and has become of primary interest due to the growing demands for energy independence, the rapidly increasing cost of energy, and the recognition that significant steps must be taken in response to climate change.

As customers rely more and more on electricity for all facets of personal and business life, and as they place increased demands on the old-fashioned power infrastructure through the addition of wind and solar distributed generation, reliability of the power system has become more critical yet more difficult to maintain.

Security, both for reliability and privacy reasons, is moving to the forefront as an issue that must be solved for all levels of the power system, including down to each customer's site.

Direct interactions with customers through Advance Metering Infrastructures (AMI) are critical for achieving these goals.

2.2 AMI as Key for Realizing Smart Grid

In the past, customers were considered only as passive users of electricity, with utilities charged with providing electricity as a commodity, while fixed tariffs were set by

regulators. The Smart Grid vision changes this paradigm: using primarily price of electricity as the mechanism, customers (and their smart appliances and energy management systems) will actively respond instantaneously, hourly, daily, and even seasonally, to more closely match their energy usage to the actual cost of producing that electricity or to respond to emergency situations, while still retaining customer choice. Conversely, utilities will respond more interactively with customers to meet their reliability and efficiency requirements in a more timely and comprehensive manner.

The AMI systems, and the many other systems surrounding them, help provide the means to achieve this Smart Grid vision. With such an AMI infrastructure now available, many third parties also expect to utilize this direct connection with customers and their facilities. Therefore, AMI is envisioned as more than utilities and customers interacting, and will need significant efforts toward integration and the development of standards in order to realize the true benefits from this enabling technology.

2.3 AMI: Opportunities and Challenges

In order to understand the integration and standards issues related to AMI, it is critical to appreciate the range of opportunities provided by AMI, and to recognize the challenges posed by these opportunities.

2.3.1 AMI Stakeholders and Interactions via AMI Systems

Although there will likely be many more stakeholders in the future as innovative ideas and technology expand the capabilities, some of the main AMI stakeholders, and the types of functions which they could utilize the AMI systems for, include:

- Utility access to meter and end-point information:
  - Meter reading
  - Revenue protection and tamper detection
  - Remote connect/disconnect
  - Meter maintenance
  - Customer service
  - Power quality
  - Marketing: Pricing signals
  - Outage management
  - Distribution operations: aggregated loads
  - Distribution planning: load profiles
  - Emergency management
- Customers access to energy usage, prices, trends, forecasts, emergency information, etc.:
  - Residential customers
  - Smaller commercial customers
  - Larger commercial customers
  - Industrial customers
  - Customers with distributed generation and/or storage
- Vendors of AMI systems and associated utility systems
  - Meter vendors
  - AMI network vendors
  - AMI headend vendors
  - Vendors of applications and systems on an "Enterprise bus" such as MDM, CIS, metering databases, etc

- HAN systems and appliances
  - Customer interactions with HAN systems and appliances via AMI system
  - Vendor interactions with HAN systems and appliances for maintenance, upgrades, and other authorized activities
- Distribution automation functions
  - DA functions using the AMI network for monitoring distribution equipment
  - DA functions using the AMI network for controlling distribution equipment
- Distributed Energy Resources (DER) management
  - Energy service providers using the AMI network for managing DER systems
  - Aggregators using the AMI network for market-related DER management
- Regulators
  - Reports on outage management effectiveness of AMI functions
  - Reports on power system efficiency improvements from AMI functions
  - Reports on demand response reactions from customers
- Society
  - Reduced energy usage due to efficiency improvements
  - Results from demand response reactions
  - Reduced reliance on oil, coal, and other non-renewable energy sources due to increased implementation of renewable energy

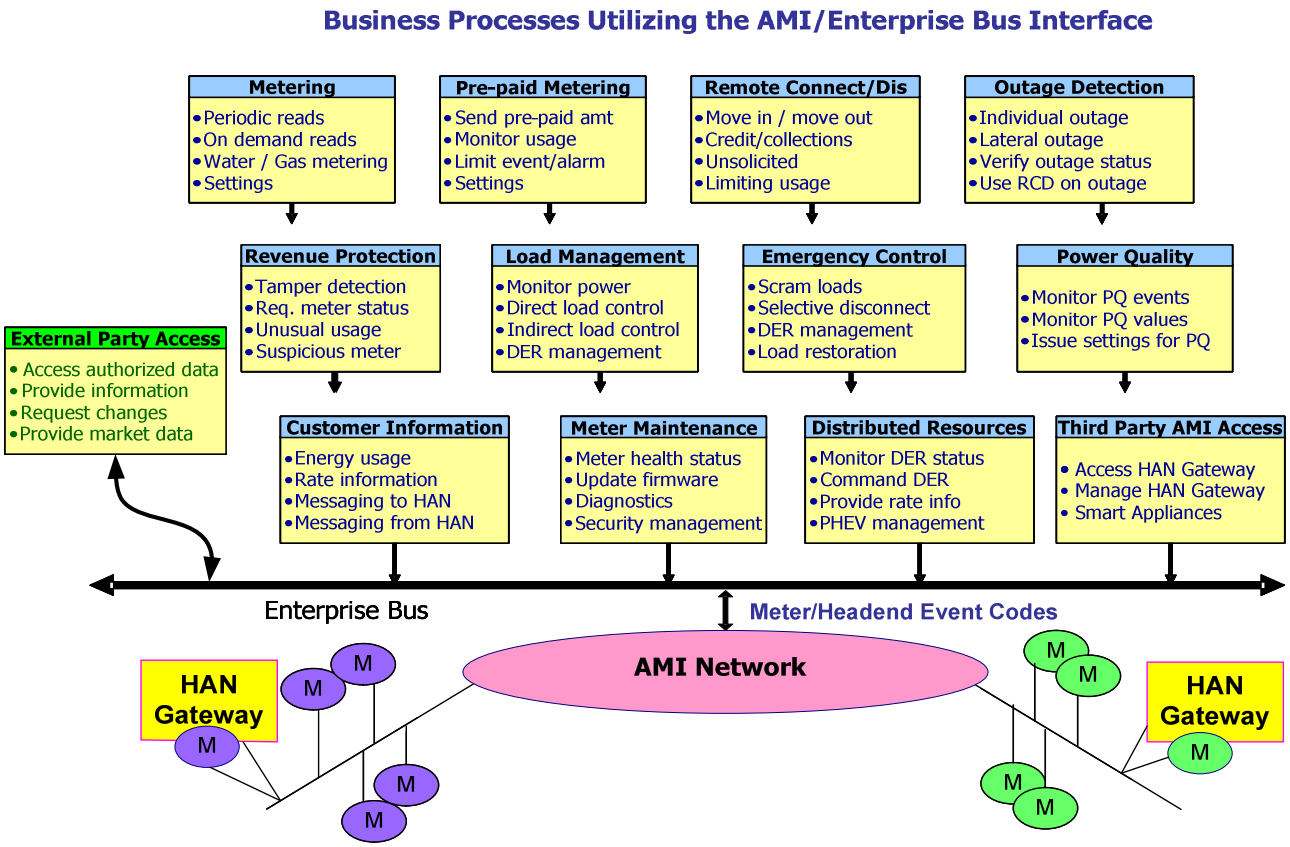


Figure 1: Business Processes Utilizing the AMI/Enterprise Bus Interface

2.3.2 Challenges of AMI Systems

Vendors are developing systems and products designed to meet specific utility requirements. They are directly responsible for the functioning of their own systems, but when they need to exchange information with other vendor systems, they need to make some external agreements on how these information exchanges are designed. If these external agreements are one-on-one, then the vendors should be able to handle them. However, if many vendors are involved, then this approach will not work.

Trying to exchange information among all of these stakeholders and the large variety of systems and products, leads to a Tower of Babel as these different products attempt to interact with each other for various purposes over a variety of communication networks. In addition, security measures could be applied differently by different vendors and for different utility scenarios. Various tariff structures for different regions and differing utility policies would also change what functions are implemented and how they interact with other parts of the AMI system.

Figure 2: The Tower of Babel, Pieter Breughel the Elder (*public domain copy*)

The solution to this Tower of Babel is the development of rules (standards) for interacting (interoperability) between all systems and all products.

3 Interoperability: What Does It Really Mean

3.1 Interoperability: Analogy with 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*"[3]. The second part of this definition is very important: not only must computer systems exchange information, they must also be able to understand that information.

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

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.

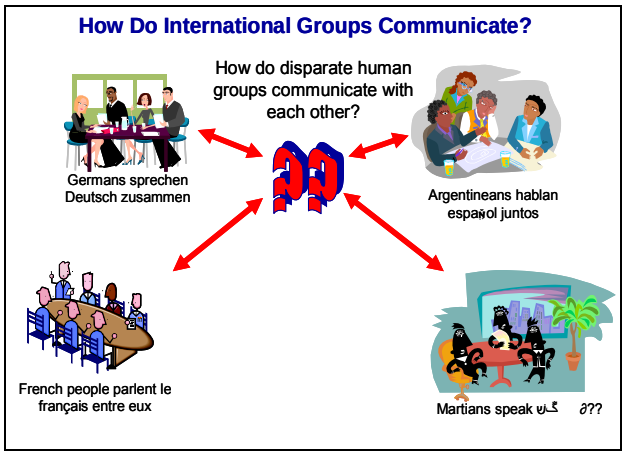


Figure 3: How do international groups communicate?

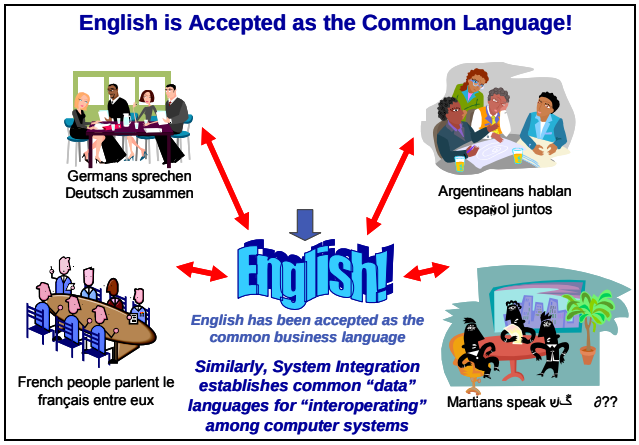


Figure 4: English is accepted as the common language

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 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.

3.2 Interoperability: Analogy with Societal Rules for Using Language

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

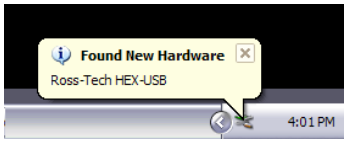
On a telephone call, societal rules specify that the person answering should say "hello" or otherwise indicate that they are now on the call. The person calling typically should identify themselves. The two people then should take turns speaking. Cellphones should not be used where they interrupt other activities such as in theaters (and meetings).

In order to have an effective meeting, not everyone should speak at the same time, but should follow basic rules for interacting. Preferably a chairperson moderates (but should not dominate) the discussions. Attendees introduce themselves if necessary. If someone should not be in the meeting, they should be asked to leave. If too-heated discussions start, they should be stopped. If one person tries to sabotage the discussion, some mechanism should prevent them from destroying the meeting. Meetings start at a particular time, and should end at a particular time.

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

3.3 Benefits of Interoperability to Stakeholders

The perfect example of the benefits of interoperability is the scenario of connecting a new printer, camera, or other new hardware to a personal computer. The moment the new device is connected, the computer says "*Found New Hardware*". Moments later it says "*Found an HP xxxx printer*" (or other hardware), then states "*Printer ready to be used*". The user then merely clicks "print" to print out their document. No fuss, no complicated actions by users.



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 to make the printer fully operational. Imagine if the same scenario were to be take place when installing smart meters, or connecting distribution automation equipment, or upgrading to a new Meter Data Management system! The savings in personnel effort would be tremendous, cutting down on truck rolls, minimizing engineering time, and avoiding user frustration and mistakes.

3.4 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.

And 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 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 ones will end up having the staying power and flexibility to be relevant for a reasonable number of years.

4 Standards: Meeting the Challenges of Interoperability

4.1 Purpose of Standards

The purpose of cyber 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.

4.2 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 speaking, there are four levels of cyber standards:

- Media-related standards, specific to fiber optics, microwave, WiFi, CATV, wires, telephone, cellphone, etc.
- Transport-related standards, such as the Internet standards: Ethernet, IP, TCP, HTTP, OPC
- Application-related standards, such as HTML, XML, IEC 61850, Common Information Model (CIM)
- 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.

Sometimes, when the requirements are less conducive to standards or the question is really which standards to use, recommended practices are developed instead.

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 not nearly enough) utility involvement.

4.3 Power Industry Standards Bodies and Key Interoperability Standards

4.3.1 General Methodology for Developing Standards

Work on interoperability standards requires many different types of effort by both users and vendors:

- Recognition of the need for a standard in a particular area. This often does not take place until a few systems have been implemented using ad hoc or proprietary solutions.
- Involvement of users (utilities) to develop the business scenarios and Use Cases that drive the requirements for the standard. All too often users leave the standards development up to vendors, who may not recognize all the needs and potential capabilities that should be included.

- Clear definition of the scope and purpose of the standard. Sometimes a standards effort is started with a vague scope, and either overlaps or even contradicts some existing, adequate standards, or fails to address enough of the area to be useful.
- Review of existing standards, including Internet standards, to determine if they can meet the need with possibly only minor modifications or selection of options.
- Development of a draft standard based on the users' requirements as well as the technology experience of the vendors.
- Widespread review and pilot implementations of the draft standard to resolve ambiguities, imprecise requirements, and incomplete functionality.
- Finalization of the standard, full implementation of the standard by vendors, and specification of the standard by users.
- Significant interoperability testing of the standard by different vendors with different scenarios
- Amending or updating the standard over time to reflect findings during these interoperability tests.

The need for the involvement of users in the development of standards cannot be emphasized enough. Unfortunately, users often feel that vendors have the technology expertise needed to develop the standards and therefore can undertake standards development on their own, without fully recognizing that the first step should be that users develop the business requirements that should then drive the standards.

4.3.2 International Electrotechnical Commission (IEC)

The International Electrotechnical Commission (IEC) is the leading global organization that prepares and publishes international standards for all electrical, electronic, and related technologies, primarily for the electric power industry, although some electrical-related work in industrial processes is also undertaken.

The IEC Council consists of National Committees, one from each country which is a member of the IEC. Under the IEC Council are Standards Management Boards (SMBs) which coordinate the international standards work. This standards work is performed through the many Technical Councils (TCs), each tasked with specific areas. For instance, TC 57 is tasked to develop standards for communications and interoperability, and is home to all the Working Groups which are developing many of the Smart Grid interoperability standards.

The Working Groups consist of Technical Experts authorized by their National Committee to participate in the 2-4 meetings a year, with significant work undertaken between meetings. In the US, the National Committee is sponsored by ANSI. All voting is done by the National Committees. A typical timeframe for developing a new standard is about 3-5 years, during which time a standard starts as a Working Document (WD) being developed in the Working Group, then sent to all National Committees for review as a Committee Draft (CD), next resent to the National Committees for review and vote as a Committee Draft for Vote (CDV), then finally issued as an International Standard (IS). The IEC then sells these standards on their web site.

Since the IEC is widely recognized as THE international standards body for power system standards in most countries in the world, it is therefore one of the key standards organizations for the power industry. IEC TC 57 has developed specialized communications standards for the power industry, with on-going work to expand and enhance these standards:

- IEC 61850 for substation automation, distributed generation (photovoltaics, wind power, fuel cells, etc.), SCADA communications, and distribution automation. Work is commencing on Plug-in Hybrid Electric Vehicles (PHEV).
- IEC 61968 for distribution management and AMI back office interfaces
- IEC 61970 (CIM) for transmission and distribution abstract modeling
- IEC 62351 for security, focused on IEC protocols, Network and System management, and Role-Based Access Control

IEC Technical Council 13 handles metering. Currently an effort is about to start between TC13 and TC57 to jointly work on communications for metering, specifically for AMI.

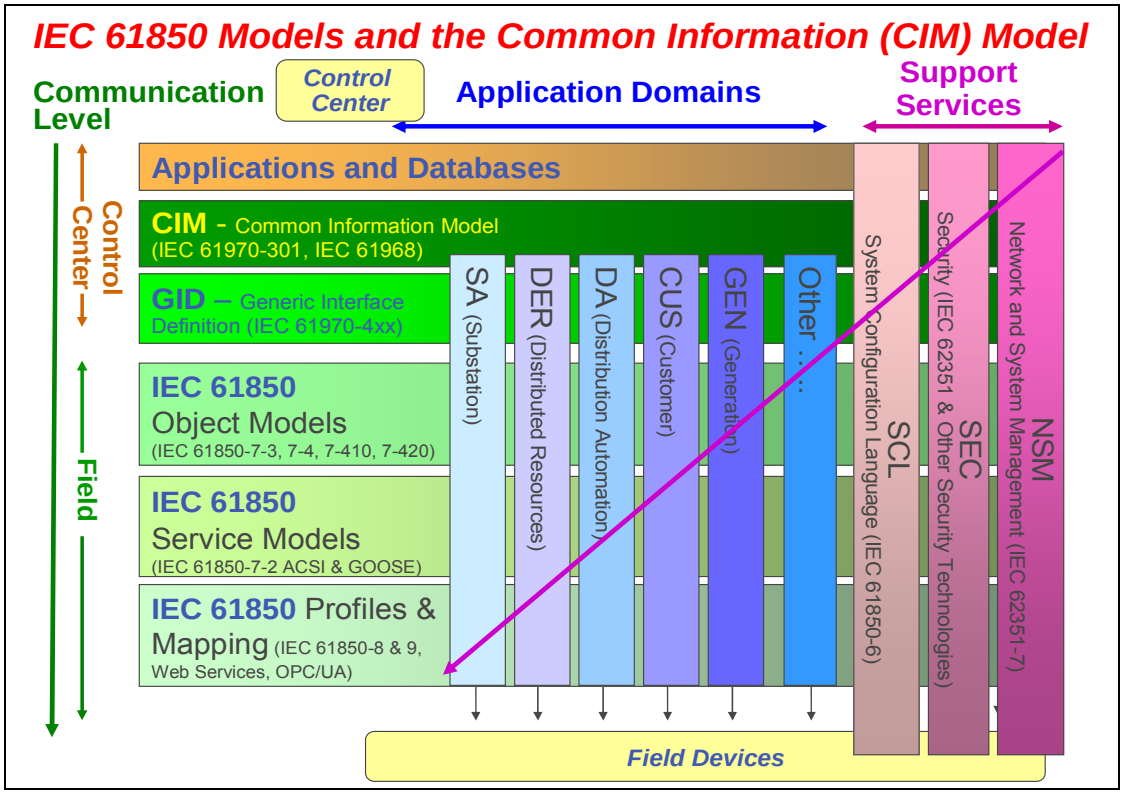


Figure 5: IEC Communication Standards

4.3.3 Institute of Electrical and Electronic Engineers (IEEE)

The IEEE has a similar methodology to the IEC's for developing drafts and then final standards, only the 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 the ones of most 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)

4.3.4 Internet Engineering Task Force (IETF)

The IETF is responsible for the Internet standards, many of which are now also widely implemented in private Intranets. The term RFC means Request for Comment, and is the mechanism used by the IETF to develop, send out for comment, and finalize standards. Usually an RFC specification must be implemented by at least a couple of vendors before it is fully accepted as a standard.

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
- Many other RFCs – too many to list – but used for the Internet and private internets

4.3.5 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)

4.3.6 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 that are of particular interest for 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

4.3.7 North American 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 those functions. 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

4.3.8 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

4.4 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 into the standards groups. Education and training on the capabilities of different standards are also 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.

4.4.1 UCA International Users Group

The UCA International Users Group was developed specifically for addressing user requirements for the IEC standards as well as, more recently, with AMI and Smart Grid issues. In particular, three active subcommittees cover:

- IEC 61850
- CIM

- Open Smart Grid (previously OpenDR). 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)

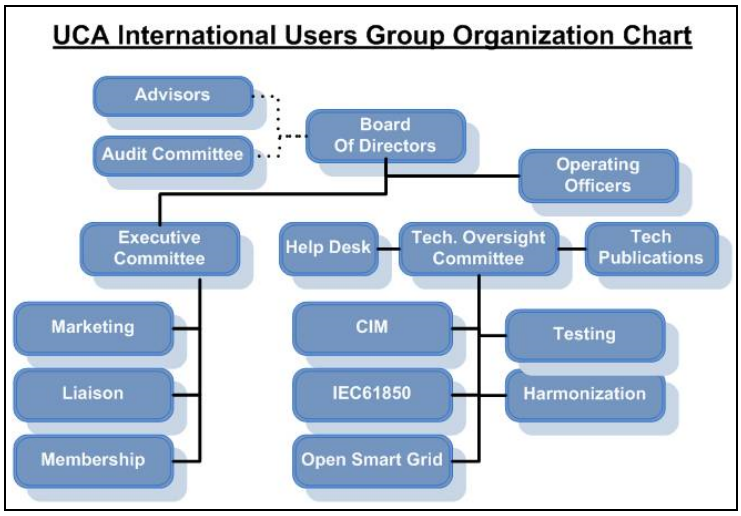


Figure 6: UCA International Users Group (UCAIug)
(Open Smart Grid was previously OpenDR Subcommittee – name being debated)

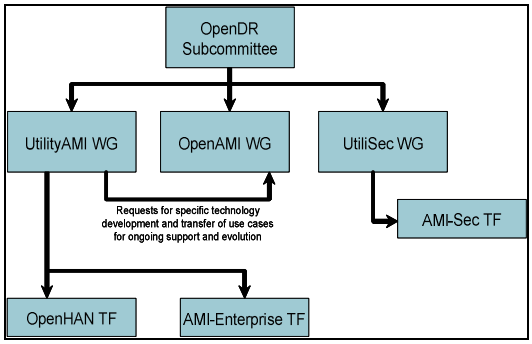


Figure 7: Open Demand Response Subcommittee in the UCAIug

4.4.2 Cigré

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

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 types of standards that should be developed, usually by the IEC.

4.4.3 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 sponsor conferences and workshops, such as the GridWise Architecture Council, Grid Interop, GridWeek, and EPRI's IntelliGrid projects.

4.4.4 EPRI's IntelliGrid

In 2003, EPRI initiated the IntelliGrid project to develop guidelines on interoperability and standards; the IntelliGrid reports were published in 2005. Since then, EPRI has sponsored projects with utilities to use the IntelliGrid recommendations.

4.4.5 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
- ISA SP-100 wireless radio groups

4.4.6 Utility Standards Board (USB)

The USB is a group of utilities who have agreed to work jointly to develop de facto standards related to the interface between the AMI system and utility systems, 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 has provided 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.

In fact, this effort is one of the few where utilities are taking the lead in providing the requirements, the Business Processes, as a foundation for developing interoperability standards.

Current work includes:

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

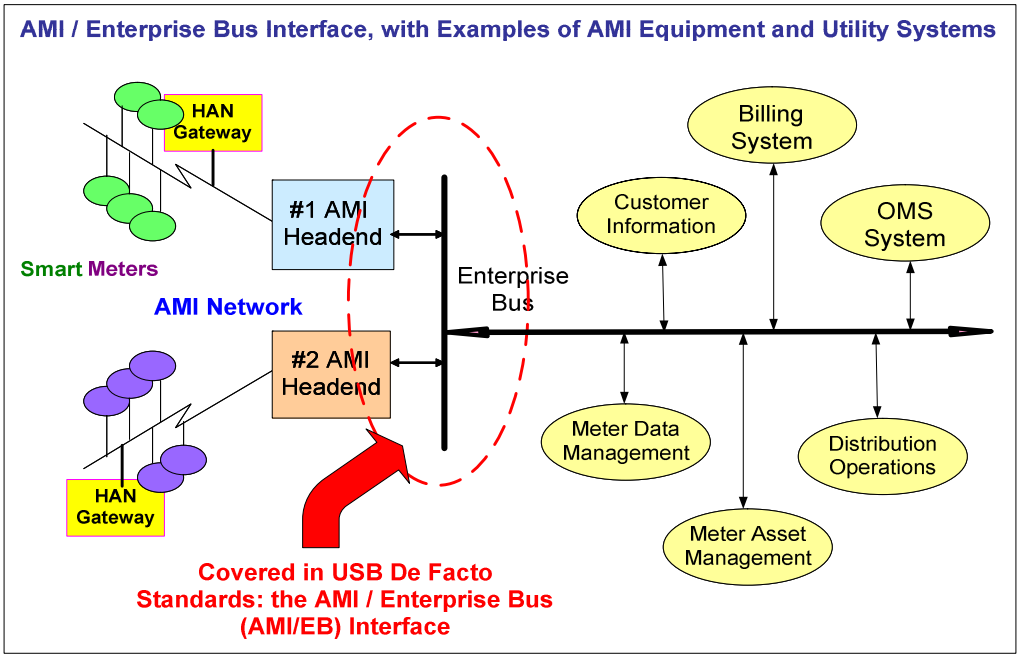


Figure 8: USB Scope: AMI/Enterprise Bus Interface

5 Conclusions

5.1 Smart Grid Broader Issues

Although this paper is focused on AMI interoperability and standards, Smart Grid also requires interoperability and standards in many other aspects of power systems, including:

- Distribution operations, in which Distribution Automation (DA) is increasingly becoming necessary to manage the distribution system more efficiently and reliably. Outages may be detected by AMI systems, but "smart" operation of the distribution system will avoid these outages in the first place.
- Transmission operations, in which information needs to flow not only within a utility but to other neighboring utilities and the responsible independent system operators. Although the primary trigger of the August 13, 2003 blackout was equipment failures, the reason that these failures caused the blackout was due to information failures. Interoperability standards are being developed but need to be tested, refined, and implemented more widely to alleviate such cross-utility information failures.
- Distributed Energy Resources (DER) installations, in which generation and storage units are being interconnected with the distribution system. These distribution systems were not designed to handle significant amounts of DER, and distribution operations are not designed to manage the resulting novel and market-driven power flows. If Plug-in Hybrid Electric Vehicles (PHEV) reach the volume some analysts expect over the next few years, distribution operations will become even more complex as customers buy and sell power. Again, information from the wide

variety of DER systems is needed for utilities to ensure efficient and reliable service while responding to the varying market and customer demands.

Each of these areas warrants a similar assessment as laid out in this paper for AMI of the requirements and the cyber standards that are being developed and implemented to meet those requirements.

5.2 Life-Cycle Cost Savings from Interoperable Standards

Life-cycle cost savings are the most important benefit from interoperable standards. Decisions often have to be made which involve determining whether future savings are worth initial cost increases. The Smart Grid vision should look to future cost savings rather than just initial costs. This is often difficult, partly because immediate costs are often the main focus of attention, and partly because future cost savings are less easy to determine, or to "prove" before the fact.

Although the following diagram may seem obvious, it can be very important to keep its lessons in mind as decisions are being made: ***does the future worth of Technology A outweigh the increased initial costs over Technology B?***

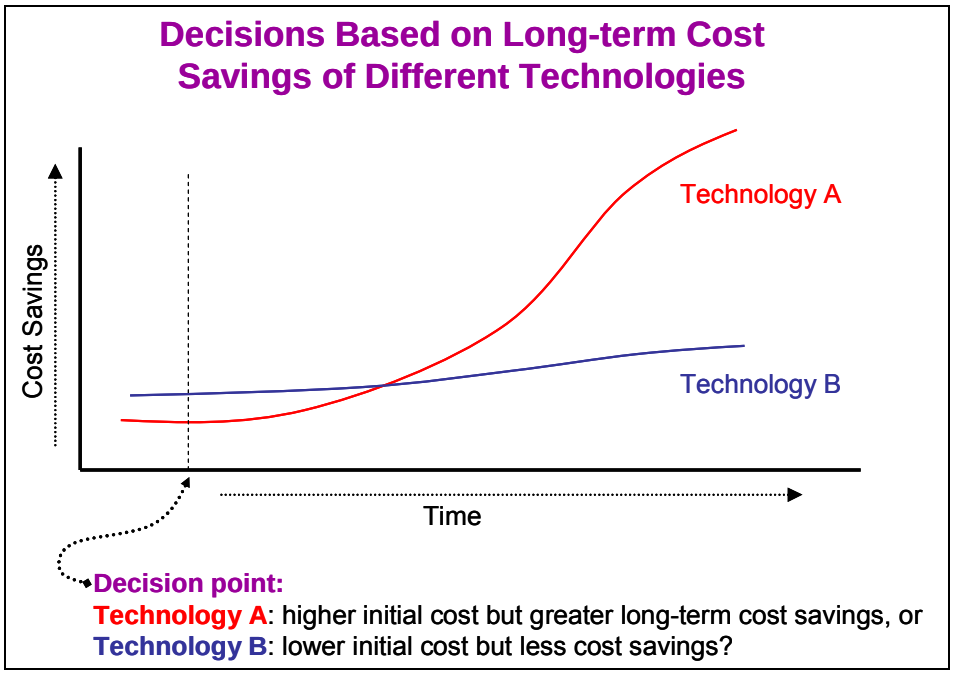


Figure 9: Decisions should be based on long-term cost savings

It is clear that interoperability and the use of standards can improve cost savings over the long term by providing the on-going engineering savings, the life-cycle maintenance savings, and the flexibility to upgrade and replace modules through simple "plug-and-work" techniques. The false economies of short-term planning should be avoided if at all possible.

5.3 Utility Involvement in the Standards Process

As mentioned throughout this paper, utilities need to be more involved in the standards and interoperability process, because only utilities can really understand the business and functional requirements and because they will ultimately be the users of the resulting standards. If the standards do not meet a utility's needs, they will gather dust on an (electronic) shelf while the utilities are scrambling to patch together their many non-interoperable systems.

The most important steps in the development of standards is the understanding of the actual business requirements. This understanding should be provided by (preferably multiple) utilities through the development of their Business Processes (also called Use Cases). Often utilities start with a simple narrative of a business process, then with the assistance of Standards Experts, expand the narrative into a series of well-defined steps or into drawings called Activity Diagrams.

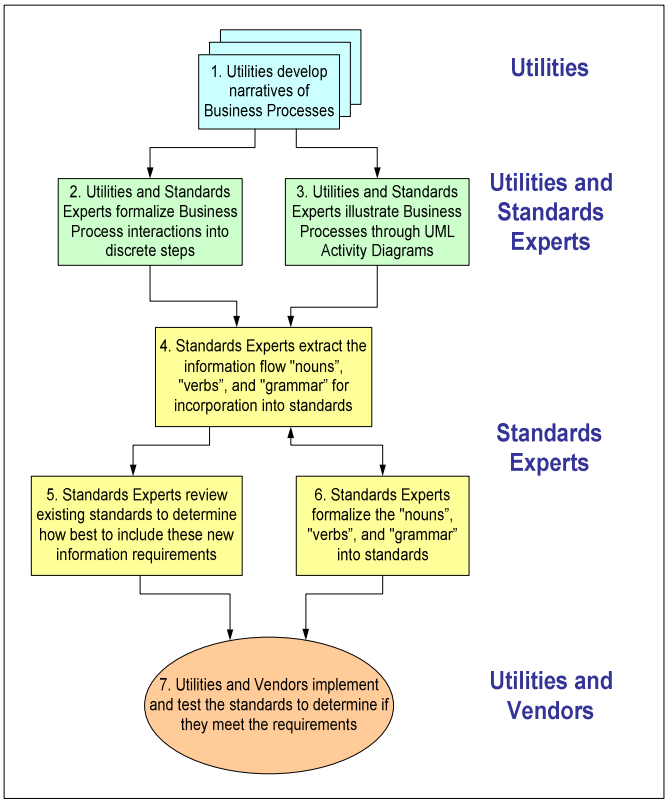


Figure 10: Procedure for Going from Business Processes to Standards

From these steps or diagrams, Standards Experts can then extract the information flows that will be transmitted across system interfaces, converting them into "nouns", "verbs", and "grammar" for inclusion into standards. After reviewing relevant existing standards, the Standards Experts can then formalize the new requirements either into these existing standards or into new standards. Finally, utilities and their vendors will implement and test the standards to ensure they really do meet the requirements.

Utility involvement is truly vital, but all too often they do not get involved in the standards process, relying on consultants and vendors (who may have interest only in specific products) to determine even the business requirements.

5.4 Maximizing the Benefits of Interoperability Standards

In a nutshell, ***Smart Grid capabilities, in whatever form they eventually take, will need to rely on an information infrastructure based on interoperability standards***.

Just like electric power utilities must design, manage, and maintain the power system infrastructure to provide reliable energy to their customers, so too will the Smart Grid information infrastructure need to be designed, managed, and maintained to provide the reliability to support this intelligent power system.

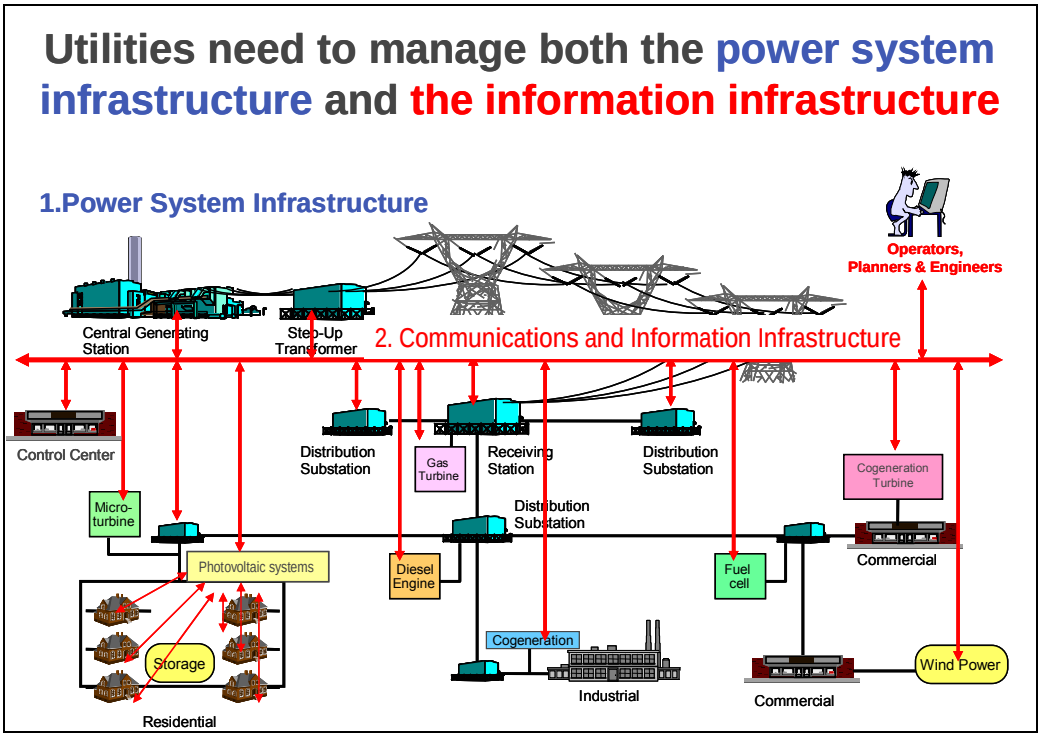


Figure 11: Utilities need to manage both the Power System Infrastructure and the Information Infrastructure

That said, it is also critical to understand that utilities and vendors must often move forward whether or not the standards exist or have been completed. The lag time in developing standards is inevitable, but utilities and vendors must nonetheless specify, design, and implement systems without waiting for these standards. In addition, many "legacy" systems cannot be cost-effectively upgraded or replaced to take advantage of relevant standards even when these do exist.

Therefore, mechanisms must be utilized for maximizing the benefits that come from interoperability standards while minimizing the delays and expenses of implementing new standards. Some of these mechanisms are:

- **Design systems based on standards**: Even if standards are not yet available, their ultimate use should be designed into the systems, and included in the life-cycle planning. In particular, security mechanisms should be designed in, even if the precise security standards are not available. This may seem a little like fortune-telling, but often the key elements of standards are known long before they are finalized.
- **Use state-of-the-art technologies as much as feasible**: Usually standards are based on the latest technology developments, so that even if the actual standards are not yet available, the shift from the state-of-the-art technologies to the actual standards will require fewer upgrades or replacements. For instance, the use of IP addressing, Ethernet, security technologies, and XML-based data definitions and messaging will make the implementation of the newer standards easier.

- **Modularity**: If systems are developed as modules (software, firmware, and hardware modules), then certain modules can be reprogrammed or replaced with the standards when they become available.
- **Flexibility**: Systems should be designed so that as standards are implemented, the systems can recognize the upgrades and reconfigure themselves appropriately.
- **Assume change will occur**: In the cyber world, equipment and systems have a life-time of a few years, not a few decades as in the power world. Therefore much shorter system life-cycles need to be expected, planned for, and budgeted.
- **Implement draft standards**: Although final standards can take years, draft standards are often 90% complete within a much shorter time. Combined with the flexibility to upgrade modules, systems can implement these draft standards and expect only minimal upgrade efforts.
- **Use adapters around legacy systems**: Systems which can not cost-effectively be upgraded to the new standards can have wrappers or adapters placed between them and the new systems using the standards. This insulates the legacy systems while still permitting the standards to be implemented.
- **Participate in standards development**: Standards are only as good as the true business requirements are understood. Utilities in particular are urged to participate at least in the requirements phase of standards development.

Interoperability is the key to the Smart Grid, and standards are the key to interoperability. The more involvement by utilities, vendors, and others in the development of standards, the faster the vision of a Smart Grid will be realized.

Biographies

Utility Standards Board (USB) – Sponsor of this paper

Frances Cleveland *is President and Principal Consultant for Xanthus Consulting International. She has managed and consulted on Smart Grid information systems, interoperability, and security projects for electric power utilities for over 30 years, covering energy management systems, distribution automation, substation automation, distributed energy resources, advanced metering infrastructure, and energy market operations. Ms. Cleveland has participated in information standards development through the IEC and IEEE as convenor of IEC TC57 WG15 on security and as chairperson of the IEEE PES Power Communications Committee. She is currently the Technical Advisor to the USB.*

Forrest Small *is a Director in the Energy Practice of Navigant Consulting. He helps clients make strategic decisions related to advanced electric power technology and how it influences their businesses. He is focused on the convergence of the Smart Grid and renewable energy resources, and how these complementary platforms can be leveraged to meet energy and business challenges. Forrest's seventeen year career began in transmission planning and operations at Central Maine Power Company where he was responsible for developing strategic system development plans, including the interconnection of merchant generation. For the past nine years he has been a management consultant assisting clients with a range of complex business challenges including technology strategy, utilities privatization, business process management, and performance improvement.*

Tom Brunetto *is a Managing Partner with DEFG LLC and a senior executive with more than thirty years of experience in the gas and electric industry. His expertise includes general management, operations, product-business development, regulation, and sales and marketing. Mr. Brunetto is skilled in business strategy, start-up management, supply chain, business transformation and operational excellence, and customer care. He is a co founder of the CCRC and leads the DETech utility consortium. Recently Mr. Brunetto conducted assignments on business sustainability and aligning the value of carbon reduction with DR, EE and distributed resources activities, and he is assisting utilities to establish standards for the Smart Grid and AMI.*