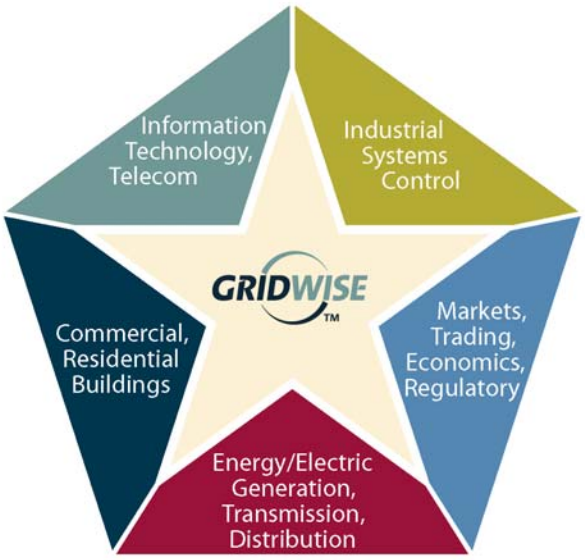

Interoperability Context-Setting Framework—Draft

GridWise Architecture Council
Interoperability Framework Team

January 2007

Prepared for the GridWise Architecture Council

GRIDWISE Architecture Council

DISCLAIMER

This draft document represents an initial step toward establishing a context to for discussing interoperability issues. This document forms a basis for engaging system integration experts in a workshop formed to debate and revise this draft material. It was prepared by the GridWise Architecture Council and employees of Battelle Memorial Institute (Battelle) as an account of sponsored research activities. Neither Client nor Battelle nor any person acting on behalf of either:

MAKES ANY WARRANTY OR REPRESENTATION, EXPRESS OR IMPLIED, with respect to the accuracy, completeness, or usefulness of the information contained in this report, or that the use of any information, apparatus, process, or composition disclosed in this report may not infringe privately owned rights; or

Assumes any liabilities with respect to the use of, or for damages resulting from the use of, any information, apparatus, process, or composition disclosed in this report.

Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the GridWise Architecture Council or Battelle. The views and opinions of authors expressed herein do not necessarily state or reflect those of Battelle.

WARNING - The following material is rated T for technical. You are expected to have a solid understanding of large, complex system integration concepts and experience in dealing with software component interoperation.

Executive Summary

As the deployment of automation technology advances, it touches upon many areas of our corporate and personal lives. A trend is emerging where systems are growing to the extent that integration is taking place with other systems to provide even greater capabilities more efficiently and effectively. GridWise™ provides a vision for this type of integration as it applies to the electric system.

Imagine a time in the not too distant future when homeowners can offer the management of their electricity demand to participate in a more efficient and environmentally friendly operation of the electric power grid. They will do this using technology that acts on their behalf in response to information from other components of the electric system. This technology will recognize their preferences to parameters such as comfort and the price of energy to form responses that optimize the local need to a signal that satisfies a higher-level need in the grid.

For example, consider a particularly hot day with air stagnation in an area with a significant dependence on wind generation. To manage the forecasted peak electricity demand, the bulk system operator issues a critical peak price warning. Their automation systems alert electric service providers who distribute electricity from the wholesale electricity system to consumers. In response, the electric service providers use their automation systems to inform consumers of impending price increases for electricity. This information is passed to an energy management system at the premises, which acts on the homeowner's behalf, to adjust the electricity usage of the onsite equipment (which might include generation from such sources as a fuel cell). The objective of such a system is to honor the agreement with the electricity service provider and reduce the homeowner's bill while keeping the occupants as comfortable as possible. This will include actions such as moving the thermostat on the heating, ventilation, and air-conditioning (HVAC) unit up several degrees. The resulting load reduction becomes part of an aggregated response from the electricity service provider to the bulk system operator who is now in a better position to manage total system load with available generation.

Looking across the electric system, from generating plants, to transmission substations, to the distribution system, to factories, office parks, and buildings, automation is growing, and the opportunities for unleashing new value propositions are exciting. How can we facilitate this change and do so in a way that ensures the reliability of electric resources for the wellbeing of our economy and security? The GridWise Architecture Council (GWAC) mission is to enable interoperability among the many entities that interact with the electric power system. A good definition of interoperability is, "The capability of two or more networks, systems, devices, applications, or components to exchange information between them and to use the information so exchanged."[1] As a step in the direction of enabling interoperability, the GWAC proposes a context-setting framework to organize concepts and terminology so that interoperability issues can be identified and debated, improvements to address issues articulated, and actions prioritized and coordinated across the electric power community.

[1] "EICTA Interoperability White Paper," European Industry Association, Information Systems Communication Technologies Consumer Electronics, 21 June 2004.

By a context-setting framework, we mean something at a high, organizational level (see Figure S.1), some neutral ground upon which a community of stakeholders can talk about issues and concerns related to integrating parts of a large, complex system. Borrowing concepts from the Australian National E-Health Transition Authority, a *framework* sits at a broad, conceptual level and provides context for more detailed technical aspects of interoperability. In contrast, "A *model* identifies a particular problem space and defines a technology-independent analysis of requirements. The *design* maps model requirements into a particular family of solutions based upon standards and technical approaches. Finally a *solution* manifests a design into a particular vendor software technology, ensuring adherence to designs, models, and frameworks." [2]

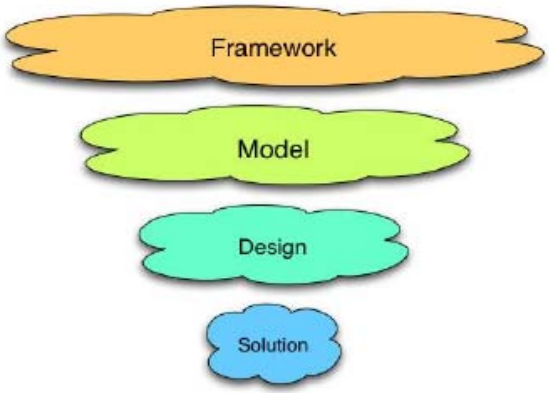

Figure S.1: A Framework Provides High-Level Perspective

The intent of the interoperability framework is to provide the context for identifying and debating interoperability issues to advance actions that make integration within this complex system easier. The framework recognizes that interoperability is only achieved when agreement is reached across many layers of concern. These layers span the details of the technology involved to link systems together, to the understanding of the information exchanged, to the business processes and organizational objectives that are represented in business, economic, and regulatory policy.

Figure S.2 summarizes the layered interoperability categories according to technical, informational, and organizational groups. It also depicts a classification of interoperability issues that cut across the layers. This document introduces these issue areas with the intent to explore and articulate the detailed nature of each issue area in separate documents engaging interested experts in their creation. The cross-cutting issues represent the areas we believe must be focused on to start improving interoperability across the web of electricity concerns.

This document presumes the reader is knowledgeable of complex system integration and the technical, informational, and organizational issues that surround this area.

The GWAC realizes that other versions of this material must be tailored to speak to the interests of other audiences, such as regulators, business decision-makers, system operators, and system suppliers. This material may consist of whitepapers, checklists, or other forms of presentation.

The GWAC plans to hold a workshop with a limited number of system-integration experts to debate and revise this draft framework. Our objective is to provide a good technical foundation and bring clarity of focus to interoperability concerns so that new material can be developed to engage a wider audience. Once there is significant alignment on this initial document, it will

[2] National E-Health Transition Authority (NEHTA), "Towards an Interoperability Framework, v 1.8," August 2005. (www.nehta.gov.au)

serve as an organization tool for the development of a symposium on interoperability. The purpose of such a gathering is to engage all sectors of the greater electricity community in describing interoperability issues, offer and debate possible solutions or actions that would improve the situation, and start prioritizing those actions where reasonable effort can be expended to make significant gain for this community.

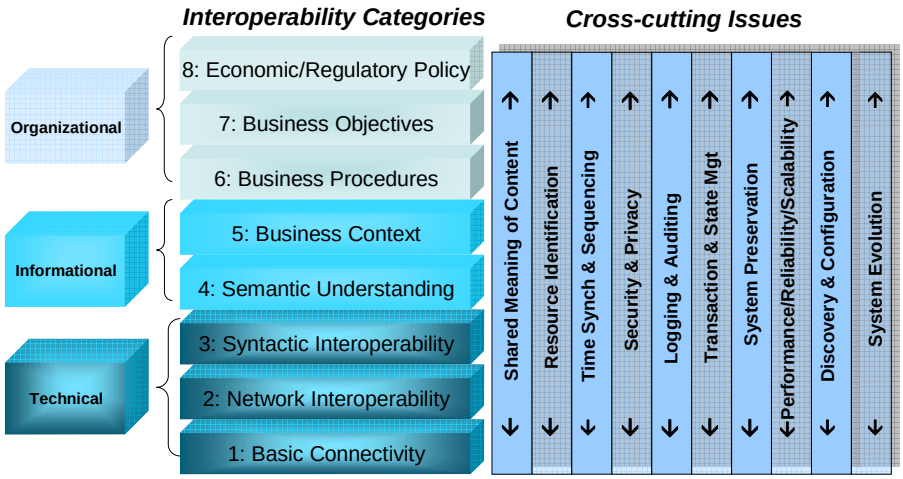

Figure S.2: Interoperability Framework Diagram

To introduce this framework, the document provides some background for this work in the context of past GWAC activity and establishes some basic concepts and terminology. It then proceeds to describe the interoperability categories. Next, we state some important points about the system-integration philosophy that influences the way system components are expected to interface and operate in a collaborative manner in something as complex as the electric power system. These philosophical tenets are important because they emphasize the needs of the system integrator and underlie many of the statements made in the cross-cutting issues that are described in the subsequent section. This is followed by some clarifying examples.

The document closes with an acknowledgement that such a framework is a living document, and therefore, a process needs to be put in place to govern its evolution over time. If such a framework is to be helpful to interoperability improvements, the diverse stakeholders in the electric system must take ownership and have access to participate in its development. This then is the first of an evolutionary series of documents to describe an interoperability framework and articulate interoperability issues that assists discussions with participants at all levels. Providing venues for participation in this work is an important aspect of engaging the electricity community.

Contents

Figures

1 Introduction

The Gridwise Architecture Council (GWAC) exists to enable automation among the many entities that interact with the electric power infrastructure. Though we do not prejudge what this automation will be used for, once it is enabled, we presume that, given opportunity, many possibilities will be explored, and much economic and social good will result. The GWAC mission is merely to enable. The goal is something called *interoperability*, which means something with the following characteristics:

- exchange of meaningful, actionable information between two or more systems across organizational boundaries
- a shared understanding of the exchanged information
- an agreed expectation for the response to the information exchange
- a requisite quality of service: reliability, fidelity, and security.

The result of such interaction enables a larger system capability that transcends the local perspective of each participating subsystem.

A path toward enabling interoperability was outlined in GWAC's "Interoperability Path Forward Whitepaper" [1]. An important early step in the path forward is to develop a common understanding of interoperability, the various levels of interoperability, and a categorization of issue areas where a consensus on improvements can better enable interoperability. This document presents a context-setting framework to organize concepts and terminology so that interoperability issues can be identified and debated, improvements articulated, and actions prioritized and coordinated across the electric power community.

To ease communication between the varied participants involved with the electric system, such a framework attempts to simplify an extremely complex topic. All the while, we must remember that the topic remains complex and crosses many disciplines. This document endeavors to use terms that align with the mainstream nomenclature used in information science, but while communication hopefully is improved, we acknowledge that semantic misunderstanding will remain a stumbling block and an area for continual improvement.

The interoperability concepts of this framework come from work relevant to distributed process integration and interoperation across the economic spectrum that includes many industries. By framing the debate, we endeavor to align thought and vision around the best ideas that exist in this field today, watching for the emergence of new concepts that may better address interoperation issues and expand the community of adopters in the future. With a shared meaning of interoperability and an appreciation of the related complex issues, we look to a path that prioritizes areas where policy agreements and/or standardization can ease integration and interoperability for all participants in the electric system.

1.1 Multiple Viewpoints

Multiple facets contribute to the complexity of interoperability concerns. This document proposes two main dimensions to provide context to interoperability discussions. The first presents a categorization of interoperability into levels much like layers in the Open Systems Interconnection (OSI) 7-layer communication model. The major categories cover technical, informational, and organizational levels. The second dimension presents issue areas for interoperability. Each issue area can cut across the multiple category levels. For example, an issue topic such as security and privacy may have concerns that involve aspects at technical levels, informational levels, as well as organizational levels in the interoperability categorization dimension.

Before introducing the cross-cutting issues, the document states some important points about the system-integration philosophy that influences the way system components are expected to interface and operate in a collaborative manner in something as complex as the electric power system. These philosophical tenets are important because they emphasize the needs of the system integrator and underlie many of the statements made in the cross-cutting issues.

The reader should keep in mind that to achieve interoperation between system components, all relevant cross-cutting issues must be resolved across all of the categorical levels. The intent of the framework is to help bring focus to specific aspects of interoperation in a discussion while keeping that aspect in perspective of the many other items requiring agreement or resolution.

1.2 Background

The GWAC first engaged the electric system community to develop shared thinking around a set of interoperability principles [2]. Through a series of interviews, these high-level statements were debated and revised until they reflected broad agreement on their validity and their wording. The interoperability context-setting framework provides a perspective consistent with these principles. The topics addressed in this document were selected to cover these principles. Throughout the document, you will see references to related principles.

Large-scale system integration is not unique to the electric system. Interoperability issues are being tackled in all economic sectors, including banking, telecom, transportation, and healthcare. We are not alone or isolated in confronting these issues, though the scope of the electric system and the number of collaborating participants makes it particularly complex. The advancements to resolving interoperability problems will ultimately be shared by all sectors of the economy. By being aware of, learning, and borrowing from related efforts, we can influence synergistic directions that increase the chances of success. With this background, the framework borrows heavily from concepts put forth by others [3-8].

1.3 Prerequisites

To achieve complete interoperability, common understanding and agreements must be reached on many levels, from the lowest layers of technology to the policies of government and industry. Relevant aspects of the framework must be articulated to the various audiences associated with these different levels. This is too much for one document to accomplish. Instead, we will develop specialized versions for targeted audiences sensitive to their language and perspective. This document is technical in orientation as it lays the foundation for future, targeted versions.

The audience for this document is expected to be familiar with the issues surrounding the integration of large, networked software systems. This includes concepts associated with enterprise integration and recent trends in e-business collaboration.

1.4 Scope

Consistent with the first business-related principle of interoperability, B01 [2], this document focuses on the interface between two or more interacting parties. This may be associated with inter- or intra-organizational software; however, we emphasize the independence of information technology choices and solution approaches to the business that occurs on either side of the interface.

Our scope concentrates on the situation and needs of the system integrator. Improvements in interoperability facilitate the integrator's job to hook-up and configure the interacting components so that they perform properly. Whereas other aspects of software engineering focus on the developer or end user, this document focuses on concepts and a framework for discussing issues related to developing independent components and collaborative processes so that they can be integrated more easily.

With the support of the context-setting framework, opportunities and hindrances to interoperability can be debated and prioritized for resolution. For example, suggestions can be made to revise an existing standard so that it conforms to the current best practices in information science. In another example, an application segment may ease integration where ambiguous identification is an issue by considering a distributed identification authority that issues identifiers according to an agreed-upon process. The framework does not prescribe solutions, but it enables communities to identify issues, debate them, and take steps toward resolution in a manner that maintains alignment with other facets of interoperation.

1.5 Collaboration Terminology

Suppose two parties, Party A and Party B, decide to collaborate on an activity. To do this, they need to agree on the interaction process between them to support their activity, the information required at each step of the process, and the mechanism they will use to make this information flow between them. We refer to the concepts involved in this electronic interaction as a collaboration model.

As shown in Figure 1 (adapted from [9]), for any interaction to succeed, the parties involved must agree on several elements of communication. The elements of a collaboration model are described in a collaboration agreement. This agreement specifies the interface that each party exposes to the outside world. The interfaces send or receive messages containing information in a certain format (syntax) and with mutually understandable content. The data exchanged can be specified in an agreed-upon structured vocabulary that is common or shared between the two parties.

The collaboration agreement describes the roles and capabilities of the parties to achieve a shared outcome. It specifies the interface, message definition, message content supported between two transacting parties, and the expected response. The collaboration agreement explains what actions (services) its interface can perform, what format it expects in the message being

communicated, what approach to secure that the interaction is used, and what things mean that are contained in the message.

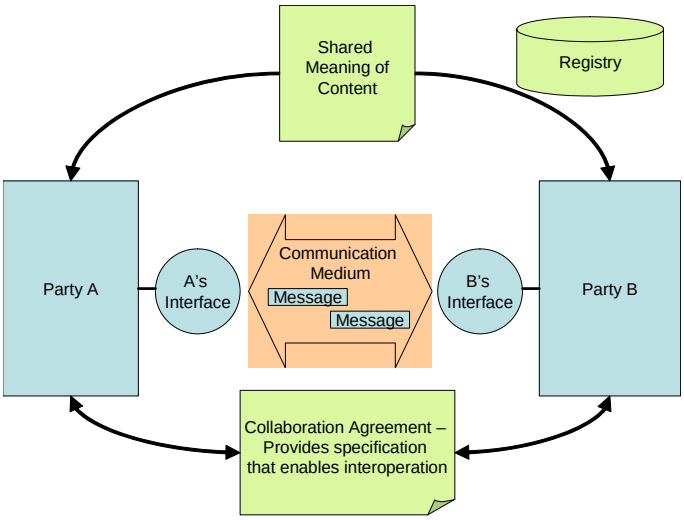

Figure 1: Collaboration Model Elements

An interface is the point of contact that a system element has with its interacting partners, and in particular, between communicating software components. The interface describes the services that a party agrees to support and error handling. Interfaces also specify the proper sequencing of information needed to affect an outcome. For example, before a switch can be opened, it must be selected for operation in a previous message exchange.

The message is the packet of information that is communicated between parties. Protocols specify the format of the message packet and can have several layers of communication-related information in the message header. For our purposes, we focus on the action or service requested and the message content (payload) related to the business at hand.

A shared vocabulary unambiguously defines the real-world concepts that are referenced in an information exchange. It provides a common language (shared meaning) about these things and their relationship to one another. Interacting parties commit to the shared meaning so that they can communicate about message content without necessarily committing to a globally shared theory of operation. These things may be called by different names because of various information-exchange implementations involving different approaches and protocols, but the shared meaning of content serves as a common point for interpretation.

A registry is a separate set of software that stores information about the components involved in an information exchange as well as aspects of the collaboration agreement itself. A registry is a separate repository that is shared by a community of interested parties. It is much like a telephone book, though the community can decide to strictly control access to the registry. Registries need not be centrally managed repositories, but can be distributed and divided into topics serving different needs. Parties can register their devices and interfaces with the registry. One can query the registry's repository to find information about registered subjects such as transacting parties and the communication mechanisms they support.

2 High Level Categorization

The GridWise interoperability context-setting framework identifies eight interoperability categories that are relevant to the mission of systems integration and interoperation in the electrical end-use, generation, transmission, and distribution industries. The major aspects for discussing interoperability fall into the following categories: technical, informational, and organizational.

Most integrators are familiar with interoperation agreements at the technical layers of the interfaces. This encompasses much of the Open Systems Interconnection (OSI) 7-layer communication model [10] where the physical transmission of information is specified, the protocols are defined, and the syntax of the information payload is selected.

We embed human recognizable information into these technical layers. Such informational models include a semantic understanding of the types of things relevant to the information exchange, as well as a description of how these entities are related to one another and perhaps how they are related to similar entities across different business domains.

However, interoperability is driven by the need of businesses (or business components) to share information between others. Business processes enable the necessary information exchange. At the organizational layers, interoperability requires agreement on the business process interaction that is expected to take place across an interface. Such an agreement would describe the service requests and responses that need to support a larger process picture that is shared by the collaborating parties. These processes must also be consistent with the tactical aspects of running the interacting businesses, the strategic aspects shared by the parties of the exchange, and the political environment embodied in economic and regulatory policy that governs such business.

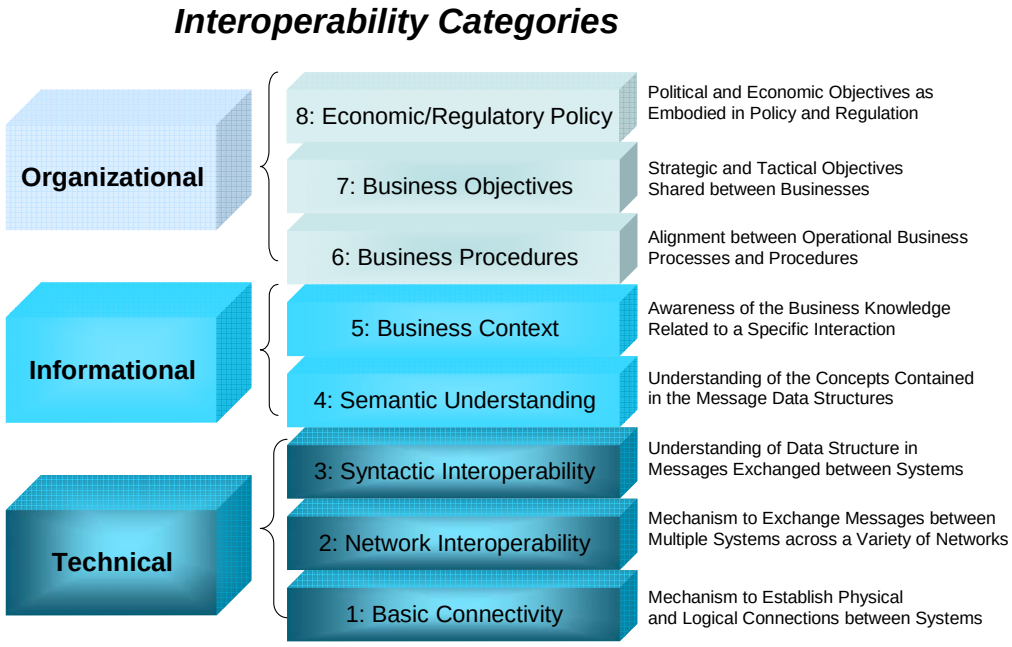

Figure 2: Interoperability Layered Categories

Figure 2**Error! Reference source not found.** depicts these categories of interoperability. The work reflected in [3] and [4] most directly inspires this viewpoint. The following material describes each subcategory. Interoperability categories are layered. Each layer typically depends upon, and is enabled by, the layers below it.

2.1 Technical Aspects

2.1.1 Category 1: Basic Connectivity

Mechanism to Establish Physical and Logical Connections between Systems

The Basic Connectivity category focuses on the digital exchange of data between two systems and the establishment of a reliable communications path. This is achieved by agreeing to conform to specifications describing the data transmission medium, the associated low-level data encoding, and the transmission rules for accessing the medium.

Basic Connectivity includes the physical and data link layers of the seven-level OSI model. These layers provide the following functions:

- Hardware media access and electrical connectivity
- Character encoding, transmission, reception, and decoding
- Low-level data contention and flow control
- Media connection establishment and termination
- Transference of data between network nodes
- Correction of errors that occur during transmission.

Examples of common physical interoperability standards include:

- Ethernet—10 MBPS over Fiber Optic Link
- 100BaseTX—100 MBPS Ethernet over Twisted Pair
- WiFi
- EIA-232
- PPP—Point-to-Point Tunneling Protocol
- Frame Relay.

2.1.2 Category 2: Network Interoperability

Mechanism to Exchange Messages Between Multiple Systems Across a Variety of Networks

Network Interoperability pertains to agreement on how to address the issues arising from transporting information between interacting parties across multiple communication networks.

The protocols agreed upon in this category are independent of the information transferred. They are similar to a railroad train that can carry different types of cars that can be loaded with different payloads, but all conform to the required constraints, such as weight, track size, and coupler specifications. By doing so, they create a rail system that can be scaled up to extend nationwide despite crossing many geographical, organizational, and political boundaries.

This category includes the network, transport, session, and (sometimes) the application layers of the seven-level OSI model. These layers provide the following functions:

- Translation of logical addresses and names into physical addresses in the same way that a phone book translates human names into numbers used by the phone system.
- Transparent and reliable transfer of data between systems. This usually includes end-to-end error recovery and flow control and the assurance of complete data transfer, which includes:
    - Transference of data between the source and destination through network intermediaries, such as switches and routers
    - Management of network congestion
    - Management of message delivery order.

Examples of common Protocol Interoperability standards include:

- FTP—File Transfer Protocol
- TCP—Transport Control Protocol
- UDP—User Datagram Protocol
- IP/IPv6—Internet Protocol (version 6)
- ARP—Address Resolution Protocol
- IPSec—Internet Protocol Security.

2.1.3 Category 3: Syntactic Interoperability

Understanding of Data Structure in Messages Exchanged Between Systems

Syntactic Interoperability refers to agreement on the rules governing the format and structure for encoding information exchanged between transacting parties. As with natural language syntax, documents, paragraphs, and sentences contain words that follow rules and structures for mental decomposing by the reader. Proper syntax enables decomposition of content; it does not mean the content makes sense.

Syntactic Interoperability includes the application and presentation layers of the seven-level OSI model. This layer provides the following functions:

- Translation of character data from one format to another, such as Extended Binary Coded Decimal Interchange Code to American National Standard Code for Information Interchange (EBCDIC to ASCII)
- Message content structure, such as Simple Object Access Protocol (SOAP) encoding
- Message exchange patterns, such as Synchronous Request/Response or Asynchronous Publish/Subscribe.

Examples of common Syntactic Interoperability standards include:

- HTML—Hypertext Markup Language
- XML—Extensible Markup Language
- ASN.1—Abstract Syntax Notation One
- SOAP—Simple Object Access Protocol
- SNMP—Simple Network Management Protocol.

2.2 Informational Aspects

2.2.1 Category 4: Semantic Understanding

Understanding of the Concepts Contained in the Message Data Structures

In building a common language, it is not sufficient to understand just the syntax or grammar; one must also understand the definition of the words. Otherwise, one can create sentences that may be nonsense even though they are grammatically correct, like "My galaxy composed a green symphony." The reader knows that galaxies cannot be owned by humans and cannot write symphonies, and that symphonies do not have color, except in metaphor or fantasy.

Such rules fall into the category of "semantic understanding": rules governing the definition of things, concepts, and their relationship to each other. Together, they make up an informational "model" of how the world works. A model is usually "domain-specific," i.e., pertaining to one area of expertise, such as a car, a building, or a power system. In the past, these rules were not written down, but as we have asked computers to control larger portions of our world, we have recognized the need to codify them.

Information models are typically expressed in an object-oriented form in terms of classes, properties, and relationships. Semantic specifications may also model constraints about the information concepts by specifying assertions and inferences that can be used in reasoning mechanisms (e.g., if this, then that). This includes expressions for resolving situations where two differently named classes in different models mean the same thing or when a class is a subset or superset of another class. For instance, a good power system model would need to describe the distinction between a substation transformer and an instrument transformer.

Groups have come together to establish shared semantic understanding within an area of interest or business domain. Examples include,

- Common Information Model (CIM) power model—(International Electrotechnical Commission [IEC] 61970 CIM—based on Resource Description Framework [RDF])
- tModels based on universal description, discovery, and integration (UDDI)
- Object models based on XML schema definition (XSD)
- Object models based on OPC Unified Architecture (a manufacturing automation standard).
- Object models based on the IEC 61850 substation automation standard.

2.2.2 Category 5: Business Context

Awareness of the Business Knowledge Related to a Specific Interaction

Information models can be very large, describing all aspects of the operations of an organization. The idea of establishing a business context refers to restricting and refining the aspects of an information model relevant to the specific business process in question. These restrictions may include the roles of the players involved in the interaction as well as specific rules and constraints on the information exchanged. A business context may draw upon information models from different domains (e.g., electric distribution and factory automation systems).

The business context describes how more general information models are applied within a business-process interaction. The business context can extend or modify the rules and constraints on referenced information models. In practice, the business context often layers upon, and maps to, domain-based semantic information models while adding business workflow constraints and business roles.

For example, a distributed generation (DG) owner negotiates a contract to supply energy on a day-ahead basis from his microturbine. An energy transaction schedule is exchanged between the system operator and the DG operator. The contents of this transaction are derived from a subset of the IEC CIM power model appropriate for a microturbine. For instance, the boiler characteristics are not appropriate in this case, but aspects of the fuel and emissions models may be important. In addition, attributes and rules may need to be added regarding operation at certain times of the day due to noise-abatement requirements.

Web Ontology Language W3C standard (OWL)-enhanced metadata for RDF is a language specification that can help in federating and augmenting existing information models in this manner.

2.3 Organizational Aspects

2.3.1 Category 6: Business Procedures

Alignment between Operational Business Processes and Procedures

Effective information interoperability between business organizations requires that the involved organizations have compatible processes and procedures across their interface boundaries. The rules of engagement consistent with the relevant business process must be agreed upon and aligned for organizations to participate in distributed business transactions. Individual processes supported by interfaces between organizations are consistent with the framework provided by the business objectives category.

For example, a retail electricity provider that contracts for emergency load curtailment from a consumer follows a process to notify the consumer 4 hours ahead of time that an emergency response may be requested with the minimum duration expected. The consumer responds with a participation forecast within 1 hour. In the event of an emergency, the electricity provider notifies the consumer that an emergency is in effect. The consumer responds by curtailing demand. When the emergency is over, the electricity provider lifts the curtailment request by notifying the consumer.

2.3.2 Category 7: Business Objectives

Strategic and Tactical Objectives Shared between Businesses

Effective information interoperability between or within business organizations requires that the strategic and tactical objectives of the organizations be complementary and compatible. This implies that the business and economic drivers must be aligned between the organizations involved for effective distributed business transactions to occur. The business objectives category integrates multiple processes that likely involve multiple interactive interfaces with

other organizations. This category provides a framework within which specific business processes participate. While businesses partner and compete in the marketplace, there is an understanding that partnering and competing in an interoperable manner improves the health of the industry as well as the reliability and service offering to consumers.

Extending the example in the previous category, the retail electricity provider offered the emergency load curtailment agreement for two purposes: 1) so it could operate its distribution feeders closer to their capacity limits, defer capacity upgrades, and more gracefully manage distribution maintenance issues and 2) so it could sell load curtailment services to the regional reliability coordinator. The interactive business procedure for emergency load curtailment with the consumer fits within the business objectives of the provider. This includes aligning the objectives of the electricity provider, the load curtailment participant, and the regional reliability coordinator.

2.3.3 Category 8: Economic and Regulatory Policy

Political and Economic Objectives as Embodied in Policy and Regulation

Business organizations require that the political and regulatory policies that govern commerce provide the proper environment and/or incentives to build business relationships with other organizations, some of which may be considered competitors. This includes national, state, and local governance. Interoperability between organizations in different state and geographical regions may require regulatory alignment at the state/local level or a national policy to provide an environment conducive for business interoperability. In addition, policy can provide incentive and remove impediments for regional or national structures that facilitate interoperation.

For example, for unambiguous vehicle identification, an International Standard Organization (ISO) vehicle identification number (VIN) standard was created. The U.S. government ruled that starting in 1981, all vehicles sold were to have a unique number, and the VIN standard became part of the regulation. This supports insurance and theft concerns among other issues.

In support of interstate business, business laws have been enacted according to a uniform commercial code (UCC). The UCC is not law itself, but is composed of proposals developed and debated by lawyers throughout the country. State and federal commercial laws draw from this foundation.

3 System Integration Philosophical Tenets

As mentioned in the introduction, our emphasis is easing the task of those who integrate and configure automation components into the system. We can arguably best frame the situation when considering interacting components that are managed by different organizations. In such situations, the transacting parties clearly and formally establish the lines of authority and rules of engagement. They maintain their autonomy while collaborating to share their resources in a federated manner [11, 12].

3.1 Agreement at the Interface—A Contract

In any business engagement, the associated parties establish the ground rules and capture them in a contract or an agreement. Sometimes these rules are assumed (such as, we will communicate using the English language), sometimes they are referenced (e.g., consistent with the commercial code of the State of Louisiana), and most of the time, the particulars are documented in a signed contract. Each party exchanges goods and services as an independent entity. The terms and conditions describe how goods and services flow between parties, the price, the scope, the schedule, and the quality of the deliverable. They also describe the consequences for failure to perform. They rarely state how the good or service is created or obtained.

Similarly, we presume that agreements between automation components concentrate at the place where the boundaries of each component meet, their interface. By establishing an interface agreement, each component preserves its integrity. It can change internally and react to various pressures independent of other components as long as it meets its interface agreements.

Interface agreements are important to maintain even within the same organization. The integrity of components established by the same authority can be compromised when designers discover that they can more easily realize new functionality by making coordinated changes in both components and not reflecting the change in the interface agreement. This leads to undocumented assumptions that are lost when designers change or individual components are replaced. The situation is exacerbated in complex systems with thousands or millions of components where central planning and coordination is not humanly possible.

3.2 Boundary of Authority

Though agreements can specify the way in which automation goods and services are developed, competition and innovation is enhanced when the transacting parties concentrate on measurable aspects of the commodity exchanged, such as its scope, delivery schedule, quality, and price. In addition, respecting boundaries clarifies the system-integration activity and reduces the contract-management effort.

The boundary of authority includes addressing rights of privacy and disclosure. Run-time expectations must be met, or the consequences are suffered. This may mean the stipulation of audit trails or other internal controls for review, judgment, and settlement offline.

3.3 Decision Making in Very Large Networks

As organizations grow, the most common approach to "scale up" is to form hierarchies. Each branch performs its function contributing to the objectives of its higher level branch until the objectives of the entire organization are addressed at the top of the hierarchy. For example, hierarchical approaches can be used to organize efforts by function, allowing for higher level aggregations of functions into super functions. They can also organize activity by location and aggregate locations into higher level regions. Decision-making in such an organization usually flows down through the structure, resulting in a chain-of-command style delegation of authority. Such organizations can be very effective in systems where objectives are clear and stable and where consistency can be controlled. These systems are internally homogeneous where even communication across branches of the hierarchy can be standardized.

Despite the success of hierarchical decision-making approaches, they begin to falter when put to the task of organizing the interactions of very large networks or "hyper-networks" [12]. The electric system is such a very large network. Though the hierarchical paradigm is replicated in many subsystems of many organizations that participate in this network, the hyper-network itself has fluid objectives and many inconsistencies, and it is anything but homogeneous. This is not a moral finding, but a comment on its justifiably evolutionary nature. The miracle that the network survives is due to the collaborative interactions of its participants in a decentralized decision-making process. To paraphrase economist F. A. Hayek [13], decision-making is left to the individual organizations, subsystems, and persons acting in their own best interests while setting up information mechanisms to influence decisions that are good for the overall system. Though the resources in the electric system may aggregate in a hierarchical manner (premises to distribution feeders to sub-transmission to bulk transmission, etc.), much of the decision-making is done autonomously (e.g., system protection or balancing area control).

The analogy in the design of automation systems of many interacting components is the distributed, multi-agent environment. In these networked systems, software agents personify the intelligent, decision-making aspects of a system component. They act in response to the information at their disposal, with the resources under their control. They have a clear boundary of authority and honor contracts of behavior with the other agents with whom they collaborate.

More importantly for interoperability, the characteristics of distributed (decentralized) decision making in a multi-agent approach not only ease scalability issues; they also simplify the component integration and upgrade process. By virtue of these components striving to be self-contained, they can be more easily "wired" into the system and help automate the work of configuring and adapting themselves into a continually changing environment.

4 Cross-Cutting Issues

Cross-cutting issues are topics that need to be addressed and agreed upon to achieve interoperation. They usually are relevant to more than one interoperability category of the framework. This section proposes to organize interoperability issues into a series of topics. The long-range goal is to articulate these topics in detailed technical papers. These topics would then become the basis for soliciting proposals to resolve issues where their impact to interoperability can be prioritized and where establishing agreement on specific directions for resolution can advance the cause.

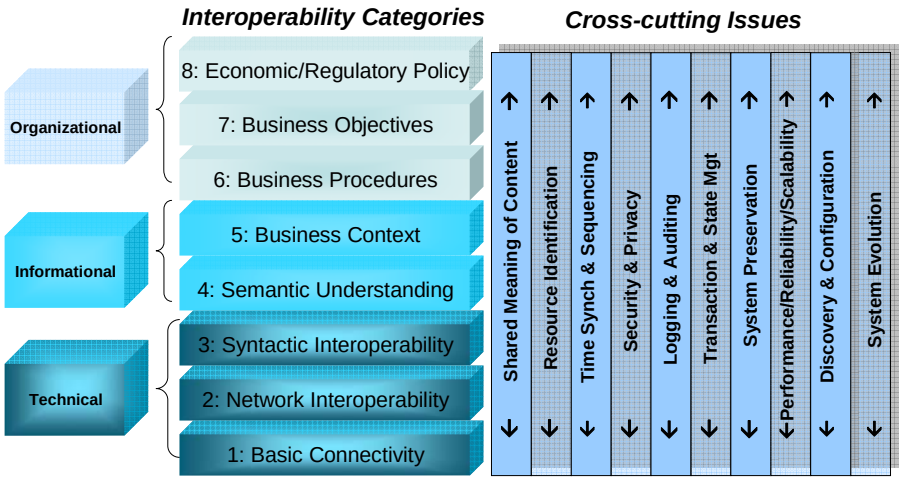

Figure 3: Interoperability Context-Setting Framework Diagram

Figure 3 depicts the cross-cutting issues spanning all categories. Though this may not be true for each topic, further discussions about these issues are needed to determine the relevance of different issue topics for each interoperability category.

4.1 Shared Meaning of Content

Effective communications at all interoperability categories require that the vocabularies and associated concepts and definitions used by all parties and systems be interpreted in context both correctly and with clarity (Principle I04 [2]). To this end, information models establishing a common semantic understanding are emerging in multiple communities and companies. Developing a subset of these models that are appropriate to the interaction in question is one dimension of the problem. Another dimension is to bridge between communities with independently evolved semantic understandings.

Database definitions or schemas can represent real-world concerns and capture semantic agreement. A drawback is that they tend to force agreement at an implementation level (e.g., a shared relational database) rather than providing flexibility to implementations. Semantic technologies are emerging from the field of knowledge representation to help provide tools with the ability to model semantic understanding while providing flexibility to implementation choices. They can also flexibly create mapping between overlapping content models (semantic federation).

The meaning of message content at the lower layers of interoperability categories is irrelevant; however, information models that define a shared semantic understanding are being established for multiple communities and companies. Still, shared meaning of content issues arise when attempts are made to integrate systems that bridge between different communities. To resolve them may require agreements at the Semantic Understanding category and above. That is, strategies for addressing shared-meaning issues may be appropriate all the way up to the Economic/Regulatory Policy category.

An example of an issue with a shared meaning of content is when systems are integrated with multiple components from different suppliers. One system may refer to a circuit breaker model as a breaker, while another may call it a switch. The integrator must determine concepts with the same meaning even though they have different names. Even when a community standardizes on a common semantic model, the common model must map to the internal information structures used by software on either side of the interface.

4.2 Resource Identification

A resource refers to an instance of an information-modeling concept, such as a generator, refrigerator, or building owner. Effective systems interoperation requires that resources, at all interoperability levels, can be unambiguously identified by all systems that need to interact (Principle I03 [2]). Identification schemes are set up within the scope of a system or subsystem, but when systems talk to other systems, identification schemes can clash.

One approach to incompatible identification is to create translation tables that allow each pair of parties to understand each other. This scheme is quite workable for interoperability that only involves two parties in a fairly isolated and simple exchange, but as integration becomes more dense and complex, assigning a shared identifier that each party translates to his/her local naming is usually desirable.

How do a set of parties exchanging messages about a resource agree on the same specific identifier? Usually the answer has these parts: 1) agreement on the format for the identifier, 2) agreement about who has the authority and responsibility to assign the identifier for any specific object, and 3) a system for communicating an identifier assignment to the other parties that need to know it.

Resource identification issues appear in different forms and are resolved in many ways. For example,

1. Indentity in Modeling Concepts: Assume that two interacting parties need to exchange information about generators. Both have information models of generators that allow users to add generators. When they do this, the modelers in each system assign names according to their own naming conventions, which typically means that the names are different. To communicate with each other, the parties have some choices. One way is to create a correspondence table that matches the names of generators that are meant to be the same with each party. Another way is to develop a business process to support one, agreed-upon name for the generator. The process says a) who is going to provide the originating definition of a given object and b) who needs to be notified.

2. Identity in Addresses: Within its scope, the Internet addresses the issue of unique identification on several levels. For example, an IP address uniquely defines an addressable network end-point that is used by Domain Name Service (DNS) to map to domain names that uniquely define a network end-point containing resources which are accessed using a universal resource locator (URL) that uniquely defines a resource, such as a web page, contained within the domain. These identification schemes and the business process to create and maintain them are an integral part of the Internet. But clashes still occur. An identification resolution scheme was created as the Internet began to support voice telephone traffic so that telephones could access Internet endpoints and vice-versa.

4.3 Time Synchronization and Sequencing

Information that flows between interoperable systems needs to maintain a common understanding of quality-of-service, time, and sequencing (Principle I05 [2]). These directly affect how and when information is interpreted. The electric system, by its nature, is a high-speed, real-time system that reacts very quickly to disturbances and load shifts. Systems that monitor and control devices throughout different parts of the electric system must maintain a common understanding of time and time-dependent order. The requirements for precision depend upon the application.

The time and date format are also relevant (e.g., GMT, data types …). Scheduling is another aspect of time.

For example, the propagation of a power-system fault that spans the monitoring of supervisory control and data acquisition (SCADA) systems requires that the SCADA systems be tightly synchronized in time so that the root cause can be quickly identified through sequence-of-events analysis. Fault propagation spreads very rapidly, and small deviations in time can quickly hide or mislead diagnostic efforts.

As another example, phase-angle data must be tagged with microsecond resolution and then transferred in the millisecond time frame for processing and situational assessment reporting.

4.4 Security and Privacy

Information security and privacy issues encompass four areas of concern:

1. Confidentiality—the information exchanged or action taken is privately held for the purposes of the business transacted and protected from unauthorized parties.
2. Integrity—the information received is the actual, unaltered information intended for the exchange.
3. Availability—the information is exchanged in a timely manner for the intended purpose between parties who have access rights to the data.
4. Accountability—a historical trail exists to show that actions related to business interactions cannot be repudiated.

Security and privacy includes aligning security policies such as user, application, and system authentication and authorization. The same open communication protocols that permit the

Internet to expand rapidly through lower-cost and efficient systems integration also make increased malicious attacks possible. Electric system interactions must be protected from attacks that could affect system reliability as well as damage business and regulatory agreements.

Security and privacy must be maintained through all levels of interoperability from automated control through business transactions (Principles B01, I07 [2]).

4.5 Logging and Auditing

Depending upon the interaction agreements between parties and industry or government oversight, a historical trail may need to be supported (Principles B05, R02 [2]). Logging and auditing processes and procedures need alignment across the transacting interface. Troubleshooting and debugging problems that span disparate system boundaries can be difficult because information can be lost or distorted if it is not retained long enough, or evidence is referenced rather than stored with the archive. Agreements on what is logged, the accuracy of time tagging and event sequencing, data retention policies, and security and privacy concerns must be established.

Within an organization, common system management facilities can greatly ease the effort needed to maintain and support ongoing systems operation. They also permit easier centralization of support facilities, thereby reducing cost and reducing mean-time-to-repair. Such facilities will likely not exist across organizations because of different technology choices. It can also be difficult to institute such coordination within large organizations because of pressures from different segments of the organization to evolve separately.

4.6 Transaction and State Management

Transactions and state management provide the mechanisms necessary to maintain system data integrity and consistency during fault conditions that interrupt complex distributed operations (Principle I08 [2]). Transactions have a start and finish envelope. This allows the parties of the transaction to react properly in the event that an initiated transaction does not complete properly. For example, it may be appropriate to roll back or undo the partial implementation of a transaction so that the valid state before the transaction is preserved. This prevents partial success from leaving durable information in an indeterminate or corrupt state. Management of transactions that cross organizational boundaries must consider proper operation at the boundary under all potential failure mode conditions.

For example, the Internet interacts in a stateless manner; that is, each page request stands on its own without any awareness of what happened previously. A server responds to a client's request by gathering the appropriate information and sending it off, and then the connection is broken. This is a scalability feature that allows hypertext transfer protocol (HTTP) servers to respond to many requests without keeping all the connections open. The downside is that the state really needs to be managed so that a connection can be reestablished for an interactive session to continue. This is done by storing information about the state of the session with an identifier of the interacting party. This way, when the party makes his/her next request, the following phase of work can continue. This paradigm of state management contrasts with mechanisms where channels of communication remain open, and state awareness is assumed up to date as long as the parties continue to communicate.

4.7 System Preservation

The integrity and safe operation of the electric power system must be placed above the health of any one of its components. As parties transact business through their interfaces, they must consider the potential impacts of their actions or inactions to the health of the larger system. In exceptional situations, such as loss of communication in the middle of a transaction, parties need to see that system health is not jeopardized. Actions by transacting parties in these contingencies must move to system safe positions of operation (Principles B02, U02 [2]).

For example, a distributed generator is contracted to support a segment of a distribution system under periods of high load and low voltage. The generation connection is equipped with a circuit breaker and relay equipment that will automatically isolate the unit if a distribution system fault is detected, or the voltage rises too high. The generator is requested to operate for a scheduled period through the appropriate communications interface. During the time of operation, the communications link is lost. The parties to the transaction previously agreed that, for the sake of system preservation, the generator should continue to run in this contingency.

4.8 Performance, Reliability, and Scalability

Distributed processes must meet expected interaction performance and reliability requirements with the capability to scale over time to meet anticipated growth projections. Performance requirements include response latencies and transaction throughput as they relate to the effectiveness of the shared process. Insufficient performance can discourage users and prevent necessary services from being provided. Once the shared process works in a timely manner, then reliable information exchange becomes critical for continued acceptance. Successful business interactions often fuel further growth. Automation interfaces should be capable of scaling up and delivering on their commitments as the number of anticipated interactions increases with no impact to performance, reliability, and interoperability (Principle I09 [2]).

4.9 Discovery and Configuration

An important aspect of systems composed of collaborating partners is how they become configured so the components interact properly once made operational. In the large, complex electric system, components enter and leave the system on a continual basis so that the system itself is constantly evolving. To simplify the integration or revision of components in a collaborative environment, more automated techniques are emerging to discover components. Once discovered, other tools can describe how to interact with a component so that the transacting parties are configured for proper operation (Principles B02, U01, I06 [2]).

Discovery and configuration can apply at the interacting component level where interrogation interfaces can be supported to find out characteristics of the component (such as name, type of equipment or service, and other attributes), and configuration interfaces can be supported to negotiate options of operation. Discovery and configuration can also apply to seeking out potential collaborating partners and discovering their supported interoperability agreements. Public or private registries can be supported with discovery interfaces to find collaborating partners and obtain their information-exchange agreements for interoperability. The registry concept can also be used for announcing a component's existence or demise and reserving things such as names or obtaining a unique identifier.

Discovery and configuration mechanisms are also important aspects of communication network device management systems that enable communication network services to be centrally managed rather than configured and managed at the application level as point-to-point connections.

For example, ebXML [7] is an e-business technical specification under the Organization for the Advancement of Structured Information Standards (OASIS) that supports the definition of collaboration agreements (descriptions of how to interact to configure and interoperate with a component) with a discovery mechanism that allows businesses to go to a registry to find partners with relevant services and posted collaboration agreements. Similarly, UDDI is a technical specification also under OASIS for a business registry that supports the description and categorization of business services, the discovery of business services through query, and the contract information necessary to access the business services.

In both examples, the interoperability categories of Business Strategy and Economic/Regulatory Policy continue to play important roles in the ability of these approaches to facilitate interoperability on a large scale.

4.10 System Evolution

As described in the section on system preservation, a collaborating component within the system must not operate to the degradation of the system. As components continually enter or leave the system, they must do so without disrupting the overall operation of the system. The electric system cannot go down while a new component changes its status in the system. Such a change should only have a local impact. Well-designed interface contracts between parties allow freedom of implementation on either side of the interface so that internal changes do not affect the interoperation with other components. However, at times, new versions of a collaboration agreement may need to change. In this event, the introduction of such a change into the system should consider techniques that do not have widespread impact. An upgrade path needs to be put forth that allows older (legacy) versions to work with newer (emerging technology) versions of automation interfaces (Principles B02, U01, I10 [2]).

For example, a collaboration agreement with a component requires the use of a specific version of a protocol. This same agreement is used in 100,000 devices. The devices can have their firmware upgraded over the network to support a new version of the protocol. Rather than stop supporting the old protocol, the firmware upgrade supports both old and new versions so that collaborating partners can independently upgrade their interfaces, and the system can evolve without significant disruption.

5 Example Scenarios

5.1 Mrs. Meg A. Watts and Her Thermostat

This scenario is intended to illustrate the GridWise Interoperability Context-Setting Framework using a fictional sequence of events. These events deal with the possible future deployment of programmable communicating thermostats (PCTs), demand response programs, and advanced metering infrastructure in the state of California. This scenario is based on an earlier, more detailed version developed by Mr. Roger Levy for the California Energy Commission (CEC) [14].

5.1.1 Mrs. Meg A. Watts Moves In

The year is 2010. Margaret Watts is a 78-year old widow who has just moved into a newly-built retirement home in California at the urging of her family. She is on a fixed income, so any program that can reduce her power bill would be welcome. Due to health problems, she requires 24-hour monitoring equipment and cannot have her power curtailed. She is not very comfortable with technology.

The builders of her condo installed a programmable communicating thermostat. When Meg moves into the condo, her son Les calls the local utility, which mails out a package with instructions on how to set it up so that Meg can register in a demand-response program that will help reduce her power bill.

When Les follows the directions, light-emitting diodes (LEDs) on the thermostat light up showing that it has established communications with the utility. He waves what looks like a special barcode from the package near the thermostat, and the display tells him that it has confirmed that Meg is enrolled in a demand response program. It also notes that it has registered her medical exemption for emergency curtailment.

Les sets the thermostat for 72 degrees, and after helping her move her belongings, leaves to let her get herself organized.

What they didn't see:

When the thermostat powered up, the ZigBee transceiver in the thermostat contacted the electrical meter in Meg's condo and established a connection.

Smart Thermostats Legislated. By law, the thermostat was required to contain a communications interface so that it could react to emergency load curtailments initiated by the California ISO. The law in question is known as Title 24 and requires that smart thermostats be included in all new buildings. Title 24 does not specify the interfaces to be used. Instead, the interfaces were agreed upon by the power utilities, thermostat suppliers, and heating, ventilation, and air conditioning (HVAC) industries and were published separately. The CEC implemented this legislation as one measure that would help the state meet electricity demands in the light of an increasing population and lack of new generation or transmission.

Interfaces Required, But Options Permitted. Meg's utility had opted to use a two-way wireless mesh network to communicate with its meters. Such an option was permitted by the Title 24 legislation. Therefore, the utility ensured that the condo builder was supplied with ZigBee expansion cards for all its thermostats. The utility's meters all included ZigBee transceivers because the California Public Utilities Commission had ruled that all advanced metering infrastructure (AMI) systems in California "must be capable of interfacing with load control communication technology."

Standard Physical Connections. The builder bought the thermostat at a local home renovation store. However, the ZigBee cards fit perfectly because the thermostat suppliers, communication system suppliers, and utilities had agreed to all use the secure digital input/output (I/O) standard, the same interface used for digital camera memory.

Naming and Identification. The "barcode" on Meg's installation package contained a radio frequency identification (RFID) transmitter that contained her account number and other information. The thermostat transmitted this information over the ZigBee link to the meter, which forwarded it over the AMI network to the utility customer service system, which then enrolled her into the demand response program. The RFID system uses a standardized method of naming and identifying equipment, premises, accounts, and other elements of the utility infrastructure.

Interoperable Networks. The core technology used to carry the account information was the Building Automation and Control Network (BACnet™), encapsulated within the IP and carried over the AMI network. Using BACnet™ ensured compatibility with software already used by the thermostat suppliers. The AMI wireless mesh network itself was proprietary, but because it was carrying standard IP and using standardized interfaces at the network edge, the utility could use the same back-office systems to communicate over other networks. For instance, the meter belonging to Meg's son Les, who lives in a home up in the hills, communicates over a WiMAX wireless technology-based infrastructure. In addition, a security policy is put in place to address security threats appropriate to the risks. Technologies are selected (e.g., use of IPSec) consistent with the security policy.

5.1.2 A Critical Peak Occurs

One morning at breakfast, Meg is reading her morning newspaper and notices that it has a banner on its front page. The banner indicates that due to hot weather conditions, the California ISO has called for a "critical peak price" (CPP) day. Prices on electricity will be increasing eightfold. Turning on her TV, she checks the local news and realizes that the CPP was actually called the day before, and she hadn't yet noticed.

She remembers what Les told her about her new thermostat and checks the hallway. Sure enough, a blue LED is flashing on the thermostat, indicating a CPP is coming. The temperature is still at 72 degrees.

Later in the day, she is making tea when she hears the thermostat beep. The blue light is now solid, and she notes that the temperature has been adjusted to 76 degrees. The thermostat has a button that would allow her to override what it's doing. However, Meg just smiles, since Les

told her having the thermostat set the temperature back automatically ensures she will get a lower bill.

What she didn't see

Agreed-upon Business Objectives and Procedures: When the ISO announced the CPP, Meg's utility called the print and electronic media to let them know that it was happening. Through prior agreements or self-interest, they passed the announcements on to their subscribers.

The utility also transmitted a message across its mesh radio and WiMAX advanced metering networks indicating that a CPP event was coming. This message caused the flashing blue LED on Meg's thermostat to light.

According to the contract that Meg signed, she must indicate her agreement to participate in a pricing or reliability-related demand response event within a certain interval after being notified. The thermostat does this for her automatically based on whether she overrides the temperature settings. Other customers who signed up for different programs may find that if they do not reduce their usage as agreed, the utility will simply curtail their load at the meter.

Process Alignment: The actual message transmitted by the utility to Meg's thermostat through her meter was one of a limited set of messages agreed upon by the thermostat suppliers and the utilities in response to the Title 24 legislation. These messages include:

- Set your clock.
- A pricing event (like a CPP) is starting at a given time.
- A reliability event is starting now.
- An emergency event is starting now.
- The previous event was cancelled.
- Display a notice (like the one Les saw accepting Meg's exemption from emergency events).

The Title 24 legislation requires that the reliability and emergency events be expressed in terms of the number of degrees of temperature offset, or the absolute temperature setting for the thermostat.[3] The industry encoded these requirements in the definition of the messages.

[3] Arguably more consistent legislation with the interoperability principles would have been to specify that energy be reduced by certain levels, or the consumer could accept the consequences. Interoperability principle B01 encourages interactions that avoid specifying implementations of the collaborating party as long as the agreed-upon product or service is satisfied. Were this the case, non-HVAC equipment, such as water heaters, refrigerators, and pool pumps, could also be aggregated with the HVAC equipment by an energy management system for the premise.

5.1.3 An Emergency Occurs

Later in the day, Meg is playing cards with some friends when the thermostat beeps again. She gets up from the table to check.

This time, a red LED is lit, indicating that an emergency situation is underway. "Oh, drat," says one of her friends, peering over her shoulder. "Now the house will be hot when I get home. They'll have turned my air conditioning right off." Another woman says, "I'll have to reset all my clocks. I'm on the supersaver plan, and they just disconnect my electricity when this happens."

Meg holds her hand over a vent. "Mine is fine," she says. "It must be that exemption that Les told me about." Her friend snorts, "I think I'm staying here a while. It'll be more comfortable."

What they didn't see

Business Objectives: The CPP event was not sufficient to prevent an imbalance in supply and demand in Meg's area of California. This imbalance, combined with a fault on a key transmission line, forced the utility to declare an emergency event in cooperation with the California ISO.

The utility installed this system in part to meet regulatory requirements, but also in part to defer its own costs of building additional generation and transmission. On this day, the deferment is not sufficient to prevent an emergency situation. However, thanks to its investment in this standardized communications network, the utility can reduce demand considerably without having to put a large number of its customers in the dark. In most cases, customers like Meg's friends will simply have the inconvenience of the loss of air conditioning and lower priority loads, such as pool pumps.

In addition, the use of a single network for AMI and demand response permits the utility to reduce costs while continuing to meet regulatory requirements.

For their part, the thermostat suppliers' incentive is a wider market. Since the utilities all agreed on national or international standards, the suppliers can sell their products over a wider area and reduce costs.

Agreed-upon Processes and Semantics: In addition to the definition of the messages, the utilities and thermostat suppliers agreed how the thermostat should behave when it received each of the messages. For instance, the thermostat will permit Meg to override a pricing event because she has a contract in place to do so, even if it costs her more money. And this particular thermostat will ignore emergency events that would shut off her air conditioning completely because it has been programmed to do so due to her medical exemption. However, Meg's neighbors will not be so fortunate. Their thermostats know that an emergency event message means they are not permitted to override without the consequences of high prices or loss of power at the meter.

At the time of Meg's unusual day, her utility is trying to get the thermostat suppliers to agree to yet another level of semantics—a common coding for what the LEDs on the outside of the thermostats mean.

Business Context: Meg's utility has actually agreed on not just a model for thermostat operation, but on an information model for the utility industry, known as the CIM. The thermostat model uses a subset of the CIM in message definitions and the only messages the PCT needs to know. This is its "business context."

However, in the back office of the utility, the data feeding back to the utility's information systems about the progress of the CPP event and the subsequent emergency event drive outage detection and simulation software that permits the utility to recover from the emergency much more quickly. These applications use a much wider business context that covers a much more complex model of utility operations.

5.1.4 Meg and the Framework

The following table summarizes how Meg A. Watts' experience with demand response can be expressed in terms of the GridWise Interoperability Framework.

Programmable Communicating Thermostats		
Interoperability Category	**Tools, Systems, Key Actors**	**Examples of interoperation across organizational boundaries where agreements must be reached**
ORGANIZATIONAL		
Economic/Regulatory Policy Political and economic objectives as embodied in policy and regulation	CEC California Public Utilities Commission (CPUC) Public and Private Stakeholders	- The CEC is concerned about meeting demand, given large population increases and lack of new generation or new transmission lines in California. - CEC issues Title 24 policy ensuring that new homeowners will have interoperable PCTs. - Policy specifies that PCTs must have standard interfaces. - Policy permits utilities to use their own networks. The default is FM broadcast. - Administrative Law Judge ruling on CPUC requirements states that AMI systems must be "Capable of interfacing with load control communication technology."
Business Objectives Strategic and tactical objectives shared between businesses	Electric Utilities System Suppliers Customers	- Suppliers and utilities agree on how the demand response (DR) interfaces will be standardized. - Suppliers market compliant PCTs to home improvement retailers. - Suppliers base the interfaces on national and international standards, widening the market base. - Suppliers agree to forward RFID information to utility over ZigBee link to improve ease of use and customer service. - Utilities defer costs of additional generation. - Utilities can meet regulatory requirements for both

Programmable Communicating Thermostats		
Interoperability Category	**Tools, Systems, Key Actors**	**Examples of interoperation across organizational boundaries where agreements must be reached**
		advanced tariffs and PCTs using the same AMI network, reducing costs. - Utility uses mailed-out packages and the communications network to automate registration for demand-response programs. - Utility issues warnings of upcoming pricing events ahead of the event in compliance with regulatory policy and for enhanced customer service. - Customers (or their PCTs) are required to respond with their plans to opt in or out of reliability events within a predefined interval from the announcement. - Customers failing to meet contractual agreements for energy reduction may be curtailed at the meter by the utility.
Business Procedures Alignment Between Operational Business Processes and Procedures	Electric Utilitites System Suppliers Customers	- Utility issues DR messages over AMI network whenever ISO issues emergency warning. - Utility issues event notifications not only transmitted over the AMI network, but also announced over electronic media. - PCTs have internal rules for behavior when they receive each type of event. - E.g., pricing events and some levels of reliability events can be overridden, emergency events can't. - PCT messages supporting procedures: clock set, price event, reliability event, emergency event, cancel event, display message. - Title 24 policy requires that the process use both absolute setpoints and offsets of temperature.
INFORMATIONAL		
Business Context Awareness of the business knowledge related to a specific interaction	Electric Utilities System Suppliers	- PCT object classes are part of the IEC 61968 distribution CIM, but residential PCTs only need to worry about DR-specific objects, not about load models or market operations. - Object classes defined for each PCT message.
Semantic Understanding Understanding of concepts contained in the message data structures	Electric Utilities System Suppliers Consultants Standards Organizations	- IEC 61968 distribution extensions to CIM. - PCTs could standardize on meaning of LEDs in the future.
TECHNICAL		
Syntactic Interoperability	System Suppliers Consultants Standards	- BACnet™ encapsulation within IP. - Other parts of AMI system may use XML.

Programmable Communicating Thermostats		
Interoperability Category	**Tools, Systems, Key Actors**	**Examples of interoperation across organizational boundaries where agreements must be reached**
Understanding of data structure of messages exchanged between systems	Organizations	
Network Interoperability Mechanism to exchange messages between multiple systems across a variety of networks	System Suppliers Consultants Standards Organizations	- Wide area wireless mesh network to meter. Currently, only interoperable within utility; may change in future. - IP, IPsec - Security measures prevent messages from being hacked. - Meter acts as router for the PCT messages.
Basic Connectivity Mechanism to establish physical and logical connections between systems	System Suppliers Consultants Standards Organizations	- Connector to HVAC. - Secure Digital I/O expansion connector. - ZigBee interface to meter. - IEEE 802.11 wireless mesh network. - Other parts of the AMI system use WiMAX (IEEE 802.16); IP network permits same upper layers used on both. - RFID tag for medical exemption.

5.2 Congestion Management Market

The following example examines aspects of developing a power grid congestion-management market through all of the categorical interoperability layers in the framework. The examples for areas where agreements must be reached are not comprehensive, but are meant to provide clarity and distinction to the significance of each layer. It does not attempt to describe many of the cross-cutting issues that need to be resolved.

Congestion Management Market		
Interoperability Category	**Tools, Systems, Key Actors**	**Examples of interoperation across organizational boundaries where agreements must be reached**
ORGANIZATIONAL		
Economic/Regulatory Policy Political and economic objectives as embodied in policy and regulation	FERC NERC/ERO RTO/ISOs State Regulators Market Participants	- Federal Energy Regulatory Commission (FERC) Order 888: open access to transmission and distribution (T&D) infrastructure. - Regional Transmission Operators/Independent System Operators (RTO)/ISOs creation: authority given to organizations structured independent of generation and load-serving entities. - Energy Markets: optimize resource scheduling using market forces to relieve congestion. - North American Electric Reliability Council/Electric

Congestion Management Market		
Interoperability Category	**Tools, Systems, Key Actors**	**Examples of interoperation across organizational boundaries where agreements must be reached**
		Reliability Organization (NERC/ERO) reliability standards and rules that will affect congestion management for RTO/ISOs and balancing authorities.
Business Objectives Strategic and tactical objectives shared between businesses	NERC/ERO RTO/ISOs Market Participants	- Qualify buyers and sellers who can compete in an open market environment. - Create markets with rules sensitive to congestion constraints and share information about congestion situation. - Participants forecast and learn about congestion situations and participate in market to optimize profits while obeying rules. - Prospective participants can electronically find the market rules and interface specifications from a registry maintained by the RTO/ISO. - Alignment of individual procedures to fit with each other to comprehensively accomplish market objective.
Business Procedures Alignment between Operational Business Processes and Procedures	RTO/ISOs Market Participants	- Procedure for finding market rules and interface specifications. - Procedure for qualifying a participant to a market. - Procedures for participating in a market (e.g., posting market open, status, bid/ask, confirmation, and closure—includes congestion relief incentives). - Announcing market clearing. - Procedures for payment collection and settlement.
INFORMATIONAL		
Business Context Awareness of the business knowledge related to a specific interaction	RTO/ISOs Market Participants System Suppliers Consultants	- Use OWL to federate and extend IEC 61970 CIM with accepted e-market ontology (information model). - Extend ontology for market specific concepts and relationships. - Specify message content statements consistent with federated ontology that support market business procedures. - Specify market rules and interface definitions to support market discovery and registry.
Semantic Understanding Understanding of concepts contained in the message data structures	RTO/ISOs Market Participants System Suppliers Consultants Standards Organizations	- IEC 61970 CIM - OASIS ebXML e-business ontology - OASIS UDDI based tModels
TECHNICAL		
Syntactic Interoperability Understanding of data	System Suppliers Consultants Standards Organizations	- OASIS ebXML message syntax - W3C SOAP message syntax - OASIS UDDI registry and discovery syntax - W3C XML

Congestion Management Market		
Interoperability Category	**Tools, Systems, Key Actors**	**Examples of interoperation across organizational boundaries where agreements must be reached**
structure of messages exchanged between systems		
Network Interoperability Mechanism to exchange messages between multiple systems across a variety of networks	System Suppliers Consultants Standards Organizations	TCP IP IPSec
Basic Connectivity Mechanism to establish physical and logical connections between systems	System Suppliers Consultants Standards Organizations	100BaseTX PPP—Point to Point Tunneling Protocol Frame Relay

6 Governance

The interoperability framework is a living, evolving set of material that influences the ongoing work of the GWAC and those involved in resolving interoperability issues related to the electric power system. The intent is to create derivative material to communicate effectively to multiple audiences whose participation is important to the advancement of interoperability in the electric system. Mechanisms to correct, update, and clarify this framework document and its derivatives are necessary.

Further action is required to complete this section. Items to consider in developing the governance for this material include the following:

- An interoperability framework must consider the needs and views of the full range of stakeholders in an integrated view of the electric system. This requires the representation of various segments and a consensus-making process for decisions about update plans, actual revisions, and complementary material.
- Establish a revision control process.
- Establish a document posting policy
- Governance processes should measure successes and shortcomings of the interoperability context-setting framework material and drive improvement.

7 Acknowledgements

The creation of this document has been a collaborative effort of the GridWise Architecture Council. Particular recognition is given to the members of the Interoperability Context-Setting Framework Team and supporting contributors: Ron Ambrosio, Dave Cohen, Rik Drummond, Grant Gilchrist, Erich Gunther, Dave Hardin, Mike McCoy, Don Watkins, and Steve Widergren.

8 References

[1] GridWise™ Architecture Council, "Interoperability Path Forward Whitepaper," November 2005. (www.gridwiseac.org)

[2] GridWise™ Architecture Council, "Interoperability Constitution Whitepaper," October 2005. (www.gridwiseac.org)

[3] National E-Health Transition Authority (NEHTA), "Towards an Interoperability Framework, v 1.8," August 2005. (www.nehta.gov.au)

[4] Tolk, A., "Coalition Interoperability: Beyond Technical Interoperability – Introducing a Reference Model for Measures of Merit for Coalition Interoperability," 8th International Command and Control Research and Technology Symposium, June 2003.

[5] Healthcare Information and Management Systems Society (HiMSS), "Interoperability Definition and Background," June 2005. (www.himss.org)

[6] OPC Foundation, "OPC Unified Architecture Release Candidate Specification, Part 1: Concepts," June 2006. (www.opcfoundation.org)

[7] Gibb, B., S. Damodaran, ebXML Concepts and Application, Wiley Publishing, Inc., 2003, ISBN: 0-76454960-X.

[8] Barkmeyer, Edward J. et al, "Concepts for Automating Systems Integration," NISTIR 6928, U. S. Department of Commerce, February, 2003

[9] IEEE P1547.3 "Guide for Monitoring, Information Exchange, and Control of Distributed Resources Interconnected with Electric Power Systems," proposed guideline, October 2006, in final ballot.

[10] Zimmermann, H., "OSI Reference Model — The ISO Model of Architecture for Open Systems Interconnection," IEEE Transactions on Communications, vol. 28, no. 4, April 1980, pp. 425 - 432.

[11] Putman, J., Architecting with RM-ODP, Prentice Hall PTR, 2001, ISBN 0-13-019116-7, pp 601-633.

[12] Denning, P, R. Hayes-Roth, "Decision Making in Very Large Networks," Communications of the ACM, November 2006, pp 19-23.

[13] Hayek, F., "The Use of Knowledge in Society," American Economic Review, XXXV, No. 4, September, 1945, pp 519-530.

[14] Levy, R., "A Vision of Demand Response – 2015," PIER Interim Report, prepared for the California Energy Commission, CEC-500-2006-001, January 2006.