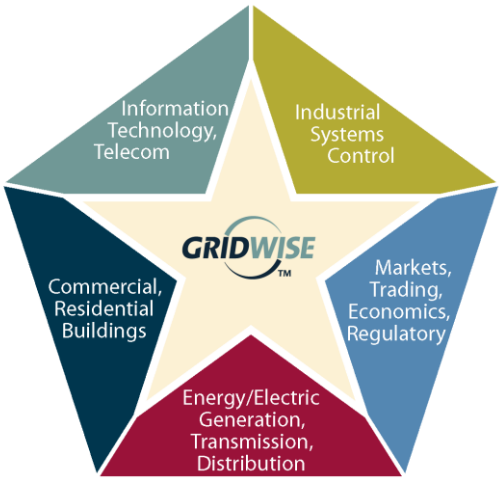

GridWise® Interoperability Context-Setting Framework

Prepared by

The GridWise Architecture Council

March 2008

About this Document –

The GridWise Architecture Council was formed by the U.S. Department of Energy to promote and enable ***interoperability*** among the many entities that interact with the electric power system. This balanced team of industry representatives proposes principles for the development of interoperability concepts and standards. The Council provides industry guidance and tools that make it an available resource for Smart Grid implementations. This document presents a technical perspective for discussing interoperability issues that can benefit projects and standards efforts. You are expected to have a solid understanding of large, complex system integration concepts and experience in dealing with software component interoperation. Those without this technical background should read the *Executive Summary* for a description of the purpose and contents of the document. Other documents, such as checklists, guides, and whitepapers, exist for targeted purposes and audiences. Please see the www.gridwiseac.org website for more products of the Council that may be of interest to you.

GRIDWISE Architecture Council

RIGHT TO DISTRIBUTE AND CREDIT NOTICE

DISCLAIMER

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 automation 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 automation technology that acts on their behalf in response to information from other automation 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 consumer'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 building automation system is to honor the agreement with the electricity service provider and reduce the consumer'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 power 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

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

can be identified and debated, improvements to address issues articulated, and actions prioritized and coordinated across the electric power community.

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* (or architecture) 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]

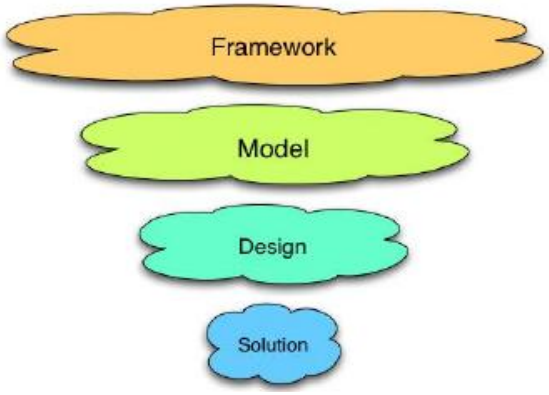

Figure S.1: A Framework Provides High-Level Perspective

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.

Besides introducing new opportunities and benefits, the application of information technology (IT) also introduces a new set of challenges. As they contribute to all economic sectors, traditionally separate applications and infrastructures get more and more interconnected. Effects and decisions within each critical infrastructure influence the other infrastructures much more than before. The framework identifies the key interoperability issue areas and can help resolve interdependencies within the electric system and with other infrastructures. It reflects the increasingly important role of IT in the electric system, resulting in an electricity plus information (E+I) infrastructure. The framework also enables the representation and exchange of ideas with other critical infrastructure domains. It supports comparing, aligning, and harmonizing technical approaches with accompanying management procedures and business processes.

Figure S.2 summarizes the layered interoperability categories according to technical, informational, and organizational groups. In addition to these categories of interoperability, the

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

framework proposes 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.

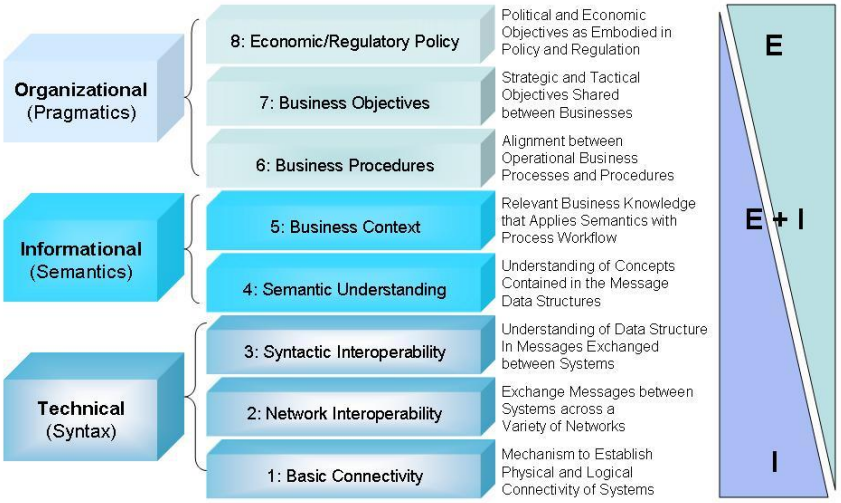

Figure S.2: Interoperability Framework Categories

The audience for this document are system architects and integrators with the ability to participate in establishing a technical foundation to discuss interoperability, articulate issues to achieving interoperability, and develop proposals to improve the situation. It presumes the reader is knowledgeable of complex system integration and the technical, informational, and organizational issues that surround this area. This technical document lays the foundation for future, companion material to targeted purposes and audiences. Ideally, the reader will consider the application of the concepts presented in this material to their field of interest to help address interoperability challenges as well as to provide suggestions on improvements to this material.

The GWAC realizes that other versions of the framework 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.

To introduce this framework, we provide some background for this work in the context of past GWAC activity and establish some basic concepts and terminology. We then state some important points about the system-integration philosophy that influences the way automation 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 about

the interoperability categories and the cross-cutting issues that are described in subsequent sections. The set of layered interoperability categories and the cross-cutting issues is followed by some clarifying examples.

The document closes with an acknowledgement that such a framework is a living concept, and therefore, a process needs to be put in place to govern its evolution over time both in terms of concepts and the material used to convey theses concepts. 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.

The process to specify and develop future material requires the participation of the electricity community. Figure S.3 provides a conceptual view of companion material envisaged to follow from the framework. These works include executive summaries for targeted audiences, technical papers that articulate interoperability issues and proposed approaches to address them, checklists, tools, use case scenarios that provide examples of applying the framework, and other similar documents.

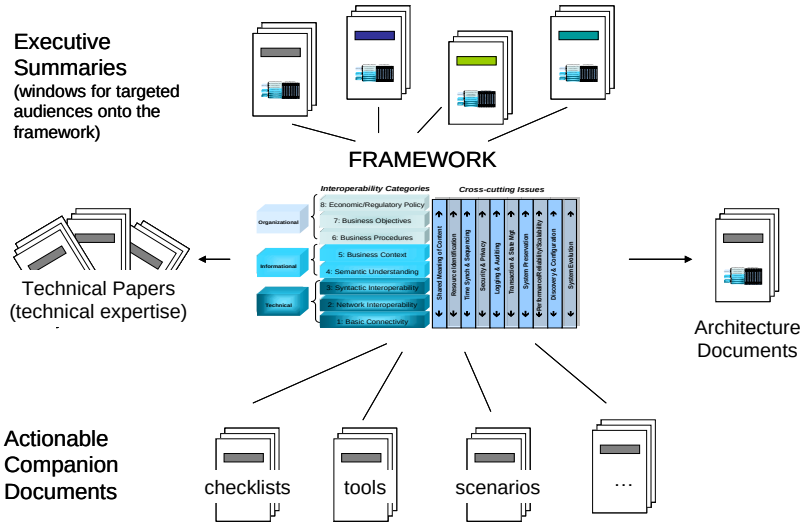

Figure S.3: Interoperability Framework Companion Material

About GridWise® and the Architecture Council

The GridWise vision rests on the premise that information technology will revolutionize planning and operation of the power grid just as it has changed business, education and entertainment. Information technology will form the "nervous system" that integrates new distributed technologies—demand response, distributed generation and storage—with traditional grid generation, transmission and distribution assets. Responsibility for managing the grid will be shared by a "society" of devices and system entities.

The GridWise Architecture Council mission is to enable all elements of the electric system to interact. We are an independent body that believes tomorrow's electric infrastructure can be more efficient and secure by integrating information technology and e-commerce with distributed intelligent networks and devices. To achieve this vision of a transformed electric system, the GridWise Architecture Council is defining the principles for interaction among the information systems that will effectively and dynamically operate the grid. The Council, which is supported by the U.S. Department of Energy, includes thirteen representatives from electric energy generation and delivery, industrial systems control, buildings automation, information technology and telecom, and economic and regulatory policy.

The GridWise Architecture Council is shaping the guiding principles of a highly intelligent and interactive electric system—one ripe with decision-making information exchange and market-based opportunities. This high-level perspective will provide guidelines for interaction between participants and interoperability between technologies and automation systems. We seek to:

- Develop and promote the policies and practices that will allow electric devices, enterprise systems, and their owners to interact and adapt as full participants in system operations.
- Shape the principles of connectivity for intelligent interactions and interoperability across all automation components of the electric system from end-use systems, such as buildings or HVAC systems, to distribution, transmission and bulk power generation.
- Address issues of open information exchange, universal grid access, decentralized grid communications and control, and the use of modular and extensible technologies that are compatible with the existing infrastructure.

The Council is neither a design team, nor a standards making body. Our role is to bring the right parties together to identify actions, agreements, and standards that enable significant levels of interoperation between automation components. We act as catalysts to outline a philosophy of inter-system operation that preserves the freedom to innovate, design, implement and maintain each organization's role and responsibility in the electrical system.

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 a concept called *interoperability*, which incorporates 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 interconnected system capability that transcends the local perspective of each participating subsystem.

A commonly understood objective for interoperability is the concept of "plug-and-play". With plug-and-play, the system integrator is able to configure an automation component into the system simply by "plugging" it in. Behind the scenes, automated processes determine the nature of the newly connected automation component and the component determines the nature of the system so that it is properly configured and can begin to operation properly. If we consider the level of integration involved as a length or distance, then the "distance to integrate" for plug-and-play is small [1].

As attractive as this concept is, achieving plug-and-play is not easy and in many, complex situations it is not practical to specify standard interfaces to this level of detail. For example, consider specifying an interface to an electricity market. Market participants may use software tools to manage the resources that they trade. Integrating these tools with the market interface usually requires some manual changes so the interface agreements are satisfied. The greater the customization and effort to make and test these changes, the greater is the distance to integrate. However, standards or best practices can be used to shorten this distance. For example, a commonly used information model

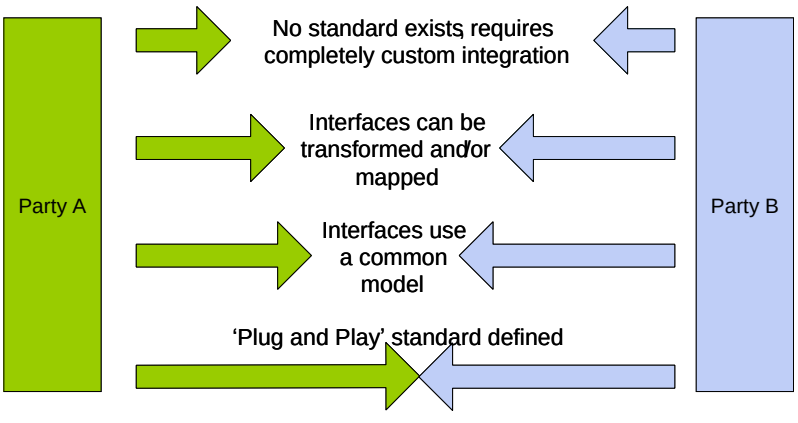

Figure 1: Distance to Integrate

can provide semantics that a community of integrators readily understands. Standard syntax, such as XML, provides a familiar format and structure for use without significant training. With time, things can more closely approach plug-and-play. At least by reaching agreements in specific areas of interoperation, a community can improve system integration and the effort to achieve interoperation. Figure 1 visualizes this concept.

Why do we want to improve interoperability? Reducing the distance to integrate has a direct impact on installation and integration costs; however, it also creates well-defined points in a system of automation components and business enterprises that allow for new automation components and businesses to connect. This can enable one automation component to be substituted for another with a reasonable amount of effort; it can also provide a path to upgrade automation components in a localized fashion that preserves overall integrated system operation. The power system must accommodate such upgrades so that it can evolve to satisfy changing resources, demands, and more efficient technologies. Substitutability can create an environment where multiple vendors can compete to provide the same automation component capability, where things such as price and reliability become distinguishing characteristics. The same well-defined point of connection can also allow for new capabilities or features to be integrated into the system.

While we emphasize the local point of interaction aspect of interoperation, attention must also be given to broader system issues. Not only must the local dynamics of an interaction be resolved, but the implications of behavior between automation components and business enterprises must be understood in the context of larger system dynamics. Seemingly, unrelated processes may interact in unforeseen ways to affect system stability in positive or negative ways. The way individual automation components and businesses interact may need to reflect constraints imposed because of larger systemic dynamic conditions.

A path toward enabling interoperability was outlined in GWAC's "Interoperability Path Forward Whitepaper" [2]. 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.

1.1 *Why Develop a Framework?*

The context-setting framework was developed as a tool in support of making the GridWise vision reality. To understand the value of the framework it is necessary to remember that GridWise is not an engineering product to deliver power, but that it is an entirely new way to think about how we generate, distribute and use energy. The framework strives to communicate and organize ideas about distributed system integration that can be used by decision makers, architects, designers, and solution providers within the electric system community. This document supports the discussion of ideas and steps to improve the present system integration situation by providing a structure to identify domains of concern and their interdependencies that need to be addressed through follow-on activities.

Our society is in a paradigm shift regarding the management and evolution of our electric infrastructure as well as other critical infrastructures and the resulting system engineering processes. The traditional approaches helped us to set up successful infrastructures for energy, water, transportation, communication, and many more. System engineering focused on all aspects of the lifecycle of a system, being able to draw clear lines between the system and its environment. This paradigm started to shift with the development of information technology (IT) in the recent decades. IT in the form of communication and computing power is ubiquitous. It allows a new way of information generation and transformation that influences the rules that govern all infrastructures.

While this introduces a new set of opportunities and potential benefits, IT also introduces a new set of challenges. As they contribute to all economic sectors, traditionally separate applications and infrastructures get more and more interconnected. Effects and decisions within each supply chain or critical infrastructure influence the others much more than before. The framework identifies the key interoperability issue areas and can help resolve interdependencies within the electric system and with other infrastructures. It reflects the increasingly important role of IT in the electric system, resulting in an electricity plus information (E+I) infrastructure. The framework also enables the representation and exchange of ideas with other supply chain and critical infrastructure domains. It supports comparing, aligning, and harmonizing technical approaches with accompanying management procedures and business processes.

Within the electricity community, the framework represents a context-setting level in a serious of specification and actions necessary to support the engineering and management processes required to make the GridWise vision a reality. The framework concept was inspired by a similar coordinating effort by the National Electronic Health Trust of Australia [3]. The framework sits at the top level of a hierarchy of well-known system engineering categories:

- A *framework* captures the key domains and their interdependencies in a way that partners can address how their contributions are placed within the overall context. As such, a framework makes no architectural or technical recommendations but establishes a context to discuss alternatives and complementary approaches. The framework is a high-level, operational view common to the electricity community used to communicate within the electricity system to compare, align, and harmonize solutions and processes as well as with the management other critical infrastructure.
- The next category comprises *architectures*. Architectures are the blueprints for solutions addressing the issues identified in the framework. Architectures s are derived from the framework by modeling (which means creating meaningful abstractions from reality to identify a bounded and solvable problem space). Many architectures can be derived from the framework and alternative architecting principles and techniques can be applied. The framework is the means to compare alternatives on the operational level and supports managers and decision makers in the process of selection, migration, and development.
- Based on architectures, system engineers create *designs*. In this category, technology and standards become important. While the architecture is the blueprint for the system, the design category comprises the blueprints for the implementing automation components that have to deliver the required functionality.

- Finally, *solutions* are implemented designs, which are real systems with real use in the real world. This includes not only the automation components, but also the meters and sensors necessary to collect the information.

The management procedures and business processes in each category above are as important as the technical specifications. To bring together different groups and support evolutionary trends, the framework is technology and standard agnostic, but processes following recommended practices support standards-based solutions more than proprietary solutions. In the framework, concrete standards are only used as examples to clarify principles. The identification of applicable standards takes place in the modeling process and is captured as part of the resulting architecture.

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.

1.2 *Multiple Viewpoints*

Multiple facets contribute to the complexity of interoperability concerns. The framework presumes some important points about the system-integration philosophy that influences the way automation 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 subsequent sections.

Beyond the philosophical tenets, the framework 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 [4]. 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.

The reader should keep in mind that to achieve interoperation between automation 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.

1.3 *Background*

The GWAC first engaged the electric system community to develop shared thinking around a set of interoperability principles [5]. 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 the framework were selected to cover these principles. Throughout the description of the framework in this 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][6][7][8][9][10][11].

On April 11 and 12, 2007, the GWAC held a workshop with 45 experts in complex software system integration and interoperability representing various aspects of the electric system including reliability coordinators, electric power company automation, buildings automation, and industrial systems automation, as well as the information technology and communications that enable this automation. The participants found that, overall, a draft version of the context – setting framework appeared sound. They also provided excellent recommendations on clarifications, modifications, and future extensions to that draft framework document. This version incorporates the valuable near-term recommendations from the workshop [12].

1.4 *Scope*

Consistent with the first business-related principle of interoperability, B01 [5], the context-setting framework 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 automation components so that they perform properly. Whereas other aspects of software engineering focus on the developer or end user, the framework focuses on concepts and a structure for discussing issues related to developing independent automation 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 *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.

1.6 *Framework Progression*

This version of the context-setting framework document represents a transition point from an introductory phase of development that reflects participation from system integration experts at the Interoperability Workshop to a foundation phase that solicits material from a wider community on the nature of interoperability, interoperability issues, and action steps to improve system integration in ways that enable the GridWise vision. As a result, a set of companion material is envisaged to follow this to this document.

The process to specify and develop future material requires the participation of the electricity community. Figure 2 provides a conceptual view of companion material envisaged to follow from the framework. These works include executive summaries for targeted audiences, technical papers that articulate interoperability issues and proposed approaches to address them, checklists, tools, use case scenarios that provide examples of applying the framework, and other similar documents.

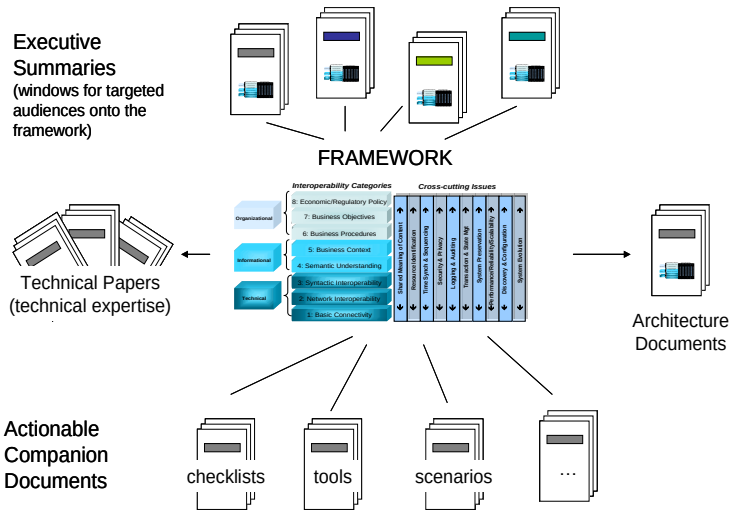

Figure 2: Interoperability Framework Companion Material

This material will begin to appear at the first Grid Interop forum to be held in the last quarter of 2007. This meeting will engage a larger cross-section of the electricity community including technical, business, and policy decision-makers, As a result of that meeting, new material will be developed and existing material will be refined or converted into new products that reflect the needs of setting a foundation for advancing interoperability. Future forums will build on this foundation as we move to a phase that expands community awareness about interoperability concerns and directions. This will involve working with standards and trade organizations in all the relevant sectors, developing supporting materials, and initiating actions that address interoperability. Lastly, as community awareness expands, the emphasis of the next phase will be to nurture an interoperability culture. In this phase, methods, tools, and processes become mature resources for architects, business managers, and policymakers to continuously improve interoperability as a normal course of their work.

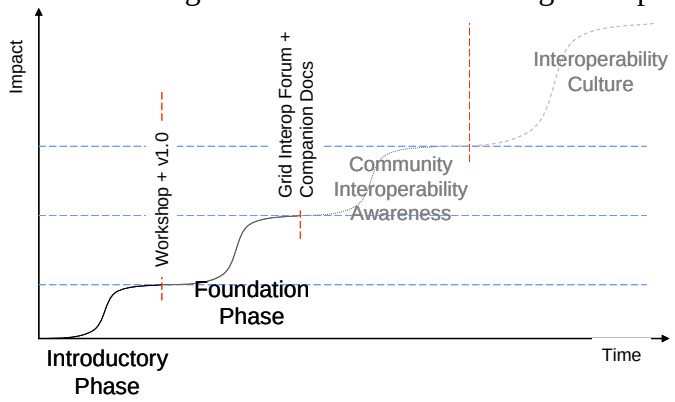

Figure 3: Phases for Progressing Interoperability

1.7 *Collaboration Terminology*

This document discusses the information exchange between computer-based technology using electronic communications media to coordinate operation and achieve goals related to the electric power system. The computer-based technology may exist in devices, software applications, or systems that control or coordinate devices, applications, or other systems. Throughout the document, the term "automation component" is used to express an intelligent piece of the electricity system. This piece can be an intelligent device (e.g., breaker, waterheater, distributed generator, transformer) or a system (e.g., transmission control center, building energy management system, substation automation system) or a software application (e.g., SCADA, billing system, feeder load balancing program). The common denominators between all automation components are 1) they can execute software programs and 2) they can communicate with other automation components in the application of their programs.

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 4 (adapted from [13]), 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.

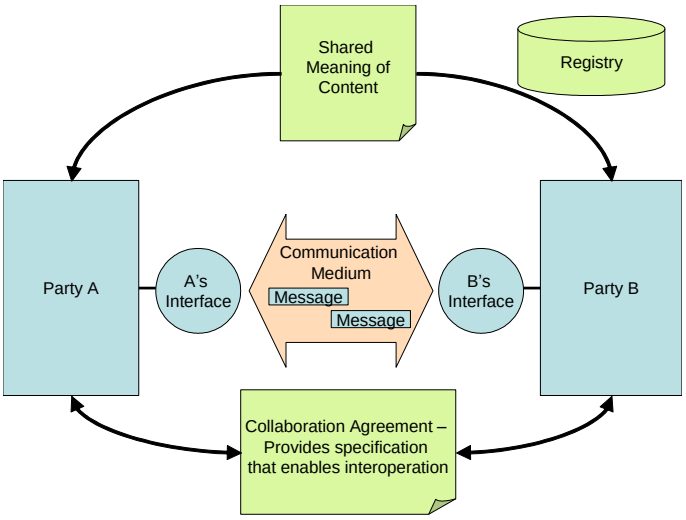

Figure 4: Collaboration Model Elements

An interface is the point of contact that an automation component has with its interacting partners, and in particular, between communicating automation components. The interface describes the services that a party agrees to support including 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 automation 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. System Integration Philosophy

As mentioned in the introduction, our emphasis is easing the task (reducing the distance to integrate) of those who integrate and configure automation components into the system. We can arguably best frame the situation when considering interacting automation 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 [14][15].

2.1 *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 automation component preserves its integrity. It can change internally and react to various pressures independent of other automation components as long as it meets its interface agreements.

Interface agreements are important to maintain even within the same organization. The integrity of automation 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 the software of both automation components and not reflecting the change in the interface agreement. This leads to undocumented assumptions that are lost when implementers change the software of an automation component or individual automation components are replaced. The situation is exacerbated in complex systems with thousands or millions of automation components where central planning and coordination is not humanly possible.

Designers specify intelligent devices and automated systems to provide desired capabilities or services. Even though the design requirements of a complex device or software system may need to accommodate a certain amount customization in each installation, reuse is an important goal. Similarly, common concepts may be sharable in a consistent fashion across a set of automation component interface agreements. For example, the same concepts of payment terms or scheduled delivery in a contract or interface agreement for energy from an automated building system could be used for a fuel cell or a micro-grid. The concept of polymorphism in computer science provides for a single definition to be used in multiple business contexts. This encourages consistency and eases system integration because common concepts become well-known and readily recognized. System integration situations can also become more scalable as integration tools can assist in connecting a heterogeneous mix of automation components with similar interface agreement concepts.

2.2 *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.

In the electric system, resources are aggregated in a hierarchical fashion, for example, from the demand side facility, to the distribution feeder, transmission substation, control area, and reliability coordinator. Each automation component of such a system plays a role with appropriate authority to do its job. Constraints, rules, or regulations may be specified to which interface agreements must conform. For example, restrictions may be placed on power quality by a reliability organization so that other electric system devices can function properly. As another example, a trade organization can create an identity registry and self-impose use of the registry to address resource unique identifier issues. How such authority is bestowed is a regulatory, political, and business policy decision. To the greatest extent possible, any constraint or restriction should be reflected in the interface agreement between interacting entities so that internal decisions for how a constraint or restriction is met remains within the boundary of authority of each interacting party.

2.3 *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" [15]. 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 [16], 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 systems of many interacting automation components is the distributed, multi-agent environment. In these networked systems, software agents personify the intelligent, decision-making aspects of an automation 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 automation component integration and upgrade process. By virtue of these automation components striving to be self-contained, they can be more easily "wired" together with other automation components in the system and help mechanize the work of configuring and adapting themselves into a continually changing environment.

2.4 *The Role of Standards*

The intent of the framework is to assist communication and coordination across multiple industry sectors that are relevant to electricity. Because of this, it is agnostic with regard to specific standards that apply at the architecture (model), design, and solution levels. Standards are referenced in this document as examples to clarify or illustrate a conceptual point. The framework does not specify or endorse standards; nevertheless, standards are extremely important tools to improve interoperability.

Standards specifications can come from recognized standards bodies, trade organizations, collaboration groups, or within a commercial organization. Standards can help interoperability because they specify an agreement between interacting parties. As will be seen in the next section, there are several categories where agreement and alignment must be achieved to enable interoperability. Specific standards address only a portion of the agreement necessary to achieve interoperability.

For a standards specification to have impact, it must be available to its potential users. Proprietary standards may only be available to a community that purchases a specific product. Open standards are desirable because they are available to anyone who wants to use them. Beyond availability, openness implies that there is adequate information to ensure equal opportunities to produce compliant automation components from independent suppliers. The EICTA offers the following criteria for openness [17]:

- Control: The evolution of the specification is set in a transparent process open to all interested contributors.
- Completeness: The specification is complete (within its scope) to ensure interoperability.
- Compliance: There is a substantial standard-compliant offering promoted by proponents of the standard.
- Cost: Fair, reasonable, and non-discriminatory access is provided to intellectual property unavoidably used in implementation of the standard.

Open standards can encourage a competitive, multi-supplier environment. Allowing multiple solution suppliers to compete encourages innovation in features and performance, and reduces the likelihood that a system or subsystem will be stranded if a supplier stops supporting an automation component.

However, using a standard, even an open standard, is not a panacea. As technology changes over time, standards go through life cycle phases, both in commercial adoption and technical maturity. Today's up and coming standard is tomorrow's legacy specification. Also, there is no shortage of standards as one looks across the complicated landscape of interface specifications in electric power, manufacturing, buildings automation, and information technology in general. If the context-setting framework is to have longevity and embrace the progressive work in multiple standards communities, it cannot be pinned to any set of standards. With this in mind, the framework encourages the development and use of standards to enhance interoperable product offerings, but it avoids mandating or endorsing the use of any particular standard. Hopefully, the context provided by the framework can facilitate identifying integration pressure points where existing standards from different organization can come together to resolve issues or where new efforts can involve the right set of people and organizations so that a resulting standard can practically meet the needs of its users and thus achieve a critical mass for adoption.

3. 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. The organizational categories emphasize the pragmatic aspects of interoperation. They represent the policy and business drivers for interactions. The informational categories emphasize the semantic aspects of interoperation. They focus on what information is being exchanged and its meaning. The technical categories emphasize the syntax or format of the information. They focus on how information is represented within a message exchange and on the communications medium.

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 [4] 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 as represented in the informational 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. The information models also support business workflows and reflect knowledge of possibilities and constraints on information contained in messages for a specific business context.

Interoperability is driven by the need of businesses (or business automation 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 5 depicts these categories of interoperability. The framework pertains to an electricity plus information (E+I) infrastructure. At the organizational layers, the pragmatic drivers revolve around the management of electricity. At the technical layers, the communications networking and syntax issues are information technology oriented. In the middle, we transform information technology into knowledge that supports the organization aspects of the electricity related business.

The work reflected in [3] and [6] 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.

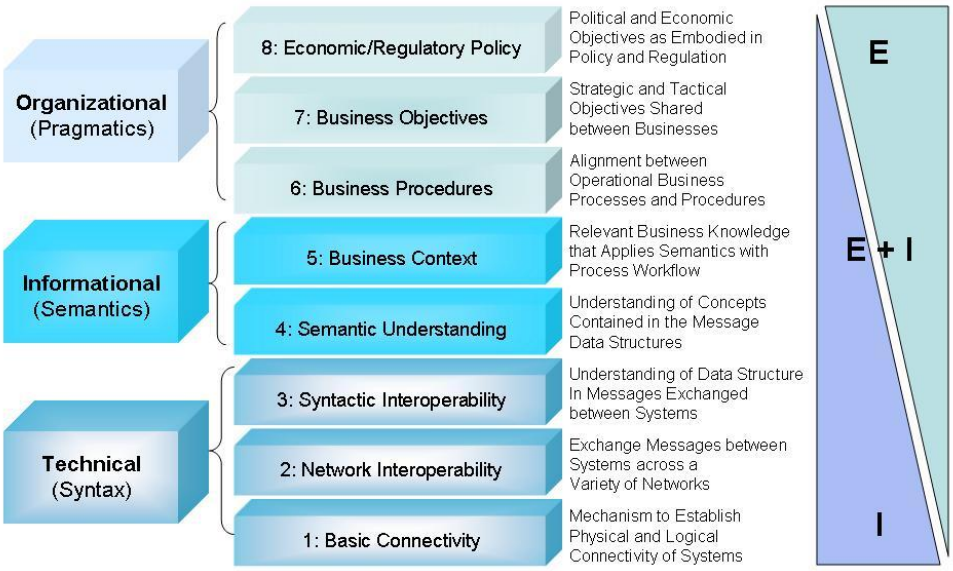

Figure 5: Interoperability Layered Categories

3.1 *Technical Aspects*

3.1.1 Category 1: Basic Connectivity

Mechanism to Establish Physical and Logical Connections of 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.

3.1.2 Category 2: Network Interoperability

Exchange Messages between 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.

The management of the communications network itself may be the responsibility of one of the interacting parties or a third party provider. The aspects of network management that each interacting party must support need alignment; however, the overall management of the communications network itself is not a topic of the framework.

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.

3.1.3 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.

3.2 *Informational Aspects*

3.2.1 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.

3.2.2 Category 5: Business Context

Relevant Business Knowledge that Applies Semantics with Process Workflow

Information models can be very large, describing all aspects of the operations of an organization. Their generality is their strength as they are usually designed to support many different business applications. 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. In addition, the business context includes additional knowledge related to the process interaction. It acts a bridge that transitions the more general semantic understanding with the needs of the specific business procedures. A business context may draw upon information models from different domains (e.g., electric distribution and factory automation systems) as it aggregates the appropriate knowledge to support a business process application.

Since the business context describes how more general information models are applied within a business-process interaction, it may 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 structure and constraints for business workflow and business roles related to the application at hand.

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 are added regarding operation at certain times of the day due to noise-abatement requirements.

UN/CEFACT and the W3C provide examples of work that is bridging semantic understanding with business procedures. The UN/CEFACT ebXML Core Components specification [18], describes business context as a mechanism for qualifying and refining more general semantic building blocks (referred to as a core component in the specification) according to their use

under particular business circumstances. This standard provides a methodology and tools relevant to this category. In addition, 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.

3.3 *Organizational Aspects*

3.3.1 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.

3.3.2 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.

3.3.3 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.

4. Cross-Cutting Issues

Cross-cutting issues are areas 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. These topics are introduced in this formative stage of developing the framework with the realization that each topic needs to be articulated in future developments and captured in detailed technical papers. These topics would then help organize specific work items 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.

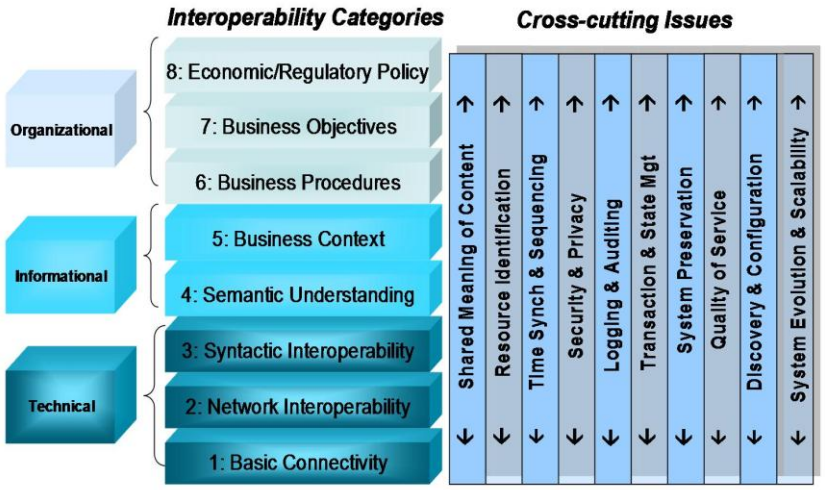

Figure 6: Interoperability Context-Setting Framework Diagram

Figure 6 depicts the cross-cutting issues spanning all categories. Deciding precisely which interoperability categories are relevant to each cross-cutting issue requires more review. Though a matrix of issues for each interoperability category would arguably be desirable, further clarification and analysis of the issues will be necessary.

4.1 *Shared Meaning of Content*

Effective communication at all interoperability categories requires that the vocabularies and associated concepts and definitions used by all parties and automation components be interpreted in context both correctly and with clarity (Principle I04 [5]). 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 automation 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.

For example, a misunderstanding about the meaning of content can arise when one automation component of the system is integrated with multiple automation components from different suppliers. One automation component 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 automation components that need to interact (Principle I03 [5]). Identification schemes are set up within the scope of an automation system or subsystem, but when an automation system talks to a totally separate automation system, 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 mechanism 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. Consider the following examples:

1. Identity 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 interacting system assign names according to their own naming conventions, which typically results in the

use of different names. 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 automation components needs to maintain a common understanding of quality-of-service, time, and sequencing (Principle I05 [5]). 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 [5]). A natural tension exists between the business process needs to interact and the risks of exposing the business process and its information to misuse or abuse. On one extreme, risk is avoided if no interaction takes place, thus defeating the business process. On the other extreme, interactions exposed to open access with critical operational implications are subject to disastrous consequences. A balance must be found that minimizes the exposure to threats while supporting the performance and usability needs of the business process.

The implications of security and privacy do not stop at the boundary between systems. Interface specifications need to address requirements on policy and information stewardship within the related portions of the business process of the interacting parties. Important aspects of this issue reach into the organizational interoperability categories.

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 [5]). 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 [5]). 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 automation 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 [5]).

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 *Quality of Service*

Distributed processes must meet expected interaction performance and reliability requirements. Performance requirements include response latencies and transaction throughput as they relate to the effectiveness of the shared process. Insufficient performance or unreliable interaction discourages users and prevents necessary services from being provided. Once the shared process works in a timely manner, then reliable information exchange becomes critical for continued acceptance (Principle I09 [5]).

Performance and reliability concerns need to be met according to each party's contribution to the business process. Not only must each automation component meet the quality of service expectations within its portion of the process, but the communications network infrastructure also must meet the expectations of it. The responsibility of provisioning and managing the

information exchange network must be clearly understood and the implications of this on the interacting parties need to be specified in their collaboration agreements.

For example, a business process that involves scheduling the next day energy demand for a manufacturing plant may have performance and reliability requirements that can withstand relatively slow transactions and occasional communications failures and retries, while a coordinated electric fault detection and response scenario requires a reliable, low latency communications network with fast processing response within each collaborating automation component.

4.9 *Discovery and Configuration*

An important aspect of systems composed of collaborating partners is how they become configured so the automation components interact properly once made operational. In the large, complex electric system, automation components enter and leave the overall system on a continual basis so that the system itself is constantly evolving. To simplify the integration or revision of automation components in a collaborative environment, more automated techniques are emerging to discover automation components. Once discovered, other tools can describe how the automation component is connected into the system (the topology) and how to interact with an automation component so that the transacting parties are configured for proper operation (Principles B02, U01, I06 [5]).

Discovery and configuration can apply at the interacting automation component level where interrogation interfaces can be supported to find out characteristics of the automation 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 an automation component's existence or demise and reserving things such as names or obtaining a unique identifier.

Discovery and configuration issues also concern how an automation component is connected into the system. Such connections can be electrical connections, such as a building to a distribution feeder or they might involve other topologies, such as financial connections with banks and insurance companies. The need to understand such topological information depends upon the business process requirements.

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 [9] is an e-business technical specification under the Organization for the Advancement of Structured Information Standards (OASIS) that supports the definition of collaboration agreements. These agrements describe how to interact to configure and interoperate with an automation component. They also have 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 and Scalability*

As described in the section on system preservation, a collaborating automation component within the overall system must not operate to the degradation of the system. As automation 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 automation 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 automation 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 [5]).

In addition, as the system evolves, it must be have the capability to scale over time to meet anticipated growth projections. Successful business interactions often fuel further growth. Automation interfaces should be capable of scaling up and delivering on their quality of service commitments as the number of anticipated interactions increases with no impact to performance, reliability, and interoperability

For example, a collaboration agreement with an automation 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. Examples of Applying the Framework

Appendix A provides a set of example scenarios that highlight the use of the framework, particularly the categories of interoperability. More work is needed to articulate the cross-cutting issues and provide clarifying scenario descriptions.

Three scenarios are provided: one on a residential demand response interface between a residence and the electricity provider, another on a commercial building demand response interface, and one on a congestion management scenario. Many more scenarios can and should be added as users' share their experiences with applying the framework.

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. A mechanism to correct, to update, and to clarify this framework and its derivative material is necessary.

For the time being, the GWAC shall maintain the framework as reflected in this document; however, 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.The GWAC is sponsoring an interoperability forum in the fall of 2007. An objective of this meeting is to engage the electric system community to develop a plan and organization for maintaining the framework and related material over time. Items to address in developing the governance for this material include the following:

- Establish a governance organization and populate it
- Establish a revision control process
- Establish a document posting policy
- Consider web-based mechanisms to capture proposed changes such as a controlled wiki
- Establish metrics to measure successes and shortcomings of the interoperability context-setting framework material and drive improvement. Note, the metric definitions must support practical measurement mechanisms.

As mentioned in the *Introduction*, we are in a foundation setting phase of a process to bring awareness to interoperability issues and eventually establish an interoperability culture. The framework and companion material may take on new forms as this process matures.

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, Richard Schomberg, Don Watkins, and Steve Widergren.

8. References

[1] Neumann, S. "Position Paper for the GridWise Interoperability Workshop," April, 2007. (http://www.gridwiseac.org/pdfs/interop_papers_0407/papers/neumann.pdf)

[2] GridWise™ Architecture Council, "Interoperability Path Forward Whitepaper," November 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] 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.

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

[6] 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.

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

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

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

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

[11] "ISO/IEC Information Technology – Home Electronic System – Guidelines for Product Interoperability – Part 1: Introduction," ISO/IEC Standard 18012.

[12] GridWise™ Interoperability Workshop April 11-12, 2007 Proceedings Summary, May 2007. (www.gridwiseac.org)

[13] 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.

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

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

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

[17] European Industry Association, Information Systems Communication Technologies Consumer Electronics, "EICTA Interoperability White Paper," 21 June 2004.
[18] UN/CEFACT, "Core Components Technical Specification – Part 8 of the ebXML Framework", Version 2.01, 15 Nov 2003.
[19] Levy, R., "A Vision of Demand Response – 2015," PIER Interim Report, prepared for the California Energy Commission, CEC-500-2006-001, January 2006.

Appendix A: Example Scenarios

A.1 Residential Demand Response

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 residential demand response programs, and advanced metering infrastructure in the state of California. This example is adapted from a scenario developed by Mr. Roger Levy for the California Energy Commission (CEC) concerning programmable controlled thermostats [19].

A.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 residential energy management system. 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 the energy manager controller 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 controller light up showing that it has established communications with the utility. He waves what looks like a special barcode from the package near the controller, 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 preferences in the controller to normally keep the condo at 72 degrees, and after helping her move her belongings, leaves to let her get herself organized.

What they didn't see:

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

Residential Energy Management Legislated. By law, the controller is required to contain a communications interface so that it can react to emergency load curtailments initiated by the California Independent System Operator (ISO). The law in question requires that the controllers be included in all new buildings. The legislation does not specify the interfaces to be used. Instead, the interfaces are agreed upon by the power utilities, controller suppliers, heating, ventilation, and air conditioning (HVAC) and other residential equipment industries and are published separately. The Energy Commission implements this legislation as one measure that helps 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 legislation. Therefore, the utility ensured that the condo builder was supplied with ZigBee expansion cards for all its energy management controllers. The utility's meters all included ZigBee transceivers because the 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 controller at a local home renovation store. However, the ZigBee cards fit perfectly because the controller 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 controller 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 from the controller is a secure web service using SOAP messaging within the IP and carried over the AMI network. 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.

A.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 energy management controller and checks the hallway. Sure enough, a blue LED is flashing on the controller, indicating a CPP is coming. The temperature is still at 72 degrees.

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

told her having the controller adjust her energy usage 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 controller 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 controller does this for her automatically based on whether she overrides the controller comfort 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 controller through her meter was one of a limited set of messages agreed upon by the controller suppliers and the utilities in response to the 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 legislation requires that the reliability and emergency events communicate that energy be reduced by certain levels and provides a critical peak price to the energy management controller for its consideration and action. Such a signal allows other demand resources in the premise to contribute to the reduction signal. Interoperability principle B01 encourages interactions that avoid specifying implementations of the collaborating party as long as the agreed-upon product or service is satisfied. In this the case, non-HVAC equipment, such as water heaters, refrigerators, and pool pumps, are also be aggregated with the HVAC equipment by the energy management controller for the premise. The industry encoded these requirements in the definition of the messages.

A.1.3 An Emergency Occurs

Later in the day, Meg is playing cards with some friends when the controller 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. My air conditioning will turn 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 automation 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 their controllers backing off 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 controller 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 controller suppliers agreed how the controller should behave when it received each of the messages. For instance, the controller 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 controller will ignore emergency events that would shut off appliances such as air conditioning because it has been programmed to do so due to her medical exemption. However, Meg's neighbors will not be so fortunate. Their controllers 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 controller suppliers to agree to yet another level of semantics—a common coding for what the LEDs on the outside of the controllers mean.

Business Context: Meg's utility has actually agreed on not just a model for energy management controller interface, but on an information model for the utility industry, known as the CIM. The controller model uses a subset of the CIM in message definitions and the only messages the controller 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.

A.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.

Residential Demand Response		
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 policy ensuring that new homeowners will have interoperable energy management controllers. - Policy specifies that controllers 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 demand response (DR) 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 interfaces will be standardized. - Suppliers market compliant controllers 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 advanced tariffs and controllers using the same AMI network, reducing costs. - Utility uses mailed-out packages and the communications network to automate registration for demand-response programs.

Residential Demand Response		
Interoperability Category	**Tools, Systems, Key Actors**	**Examples of interoperation across organizational boundaries where agreements must be reached**
		- Utility issues warnings of upcoming pricing events ahead of the event in compliance with regulatory policy and for enhanced customer service. - Customers (or their controllers) 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. - Controllers 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 cannot. - policy requires that the process use both energy reduction levels and prices.
INFORMATIONAL		
Business Context Awareness of the business knowledge related to a specific interaction	Electric Utilities System Suppliers	- Controller object classes are part of the IEC 61968 distribution CIM, but residential controllers only need to worry about DR-specific objects, not about load models or market operations. - Object classes defined for each controller message. - Controller messages supporting procedures: clock set, price event, reliability event, emergency event, cancel event, display 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. - Controllers could standardize on meaning of LEDs in the future.
TECHNICAL		
Syntactic Interoperability Understanding of data structure of messages exchanged between systems	System Suppliers Consultants Standards Organizations	- SOAP XML messages over IP.
Network Interoperability	System Suppliers Consultants	- Wide area wireless mesh network to meter. Currently, only interoperable within utility; may change in future.

Residential Demand Response		
Interoperability Category	**Tools, Systems, Key Actors**	**Examples of interoperation across organizational boundaries where agreements must be reached**
Mechanism to exchange messages between multiple systems across a variety of networks	Standards Organizations	- IP, IPsec - Security measures prevent messages from being hacked. - Meter acts as router for the controller messages.
Basic Connectivity Mechanism to establish physical and logical connections between systems	System Suppliers Consultants Standards Organizations	- 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.

A.2 Commercial Building Demand Response

In this scenario, a critical peak pricing (CPP) event is communicated via web services to the energy management controller of a commercial customer, using standard message syntax.[3]

The facility owner signed a contract that places electric use on real time rates, but also includes agreement to bring on backup generation during CPP events. When the CPP signal arrives at the energy management controller web services interface, the controller examines facility use schedules and proceeds to schedule equipment/lighting shut-downs, generator warm-up, and temperature setback of select building thermostats to correspond with the start of the CPP event. Knowing that the CPP will begin in the early afternoon, the EMCS schedules some pre-cooling in some building spaces, and lowers cooling water temperatures exiting the chillers by 1 degree to stay within allowable tolerances. Half an hour preceding the event, the EMCS starts warm-up of generators and staged shutdown procedures for some building equipment. At the start time of the CPP event, the facility has completely shut down one of three chillers, has shut down all unnecessary motor loads (such as the fountain pumps and escalators), and reduced ventilation to minimum health quality requirements. The backup generator is also feeding load to the grid.

The energy management controller has access to various sub-meters throughout facility buildings to monitor facility electric use. The utility reads the main meter, and receives confirmation of facility CPP response via web services from the controller.

Standard services within BACnet™ allow for efficient dissemination of load reduction commands throughout the facility. Agreement among utility stakeholders and commercial customers on XML message contents allows any utility to send CPP messages to any commercial BACnet web services compatible building and have that message be understood and acted upon.

BACnet security protects messages while on the facility network. Web services security protects message security in transit to the utility.

Facility owners have vendor tools for building demand response (DR) plans and actions. They also may buy products certified to be compatible for demand response applications in BACnet.

Commercial Building Demand Response		
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	Fed and state gov't Local gov't, PUCs	• Gov't bodies set policy for utility rate offerings. E.g., FERC encourages ISOs to build up markets for DR. NE ISO responds with real time market. • State gov'ts mandate DR goals. E.g., PA

[3] Adapted from material contributed by David Holmberg of the National Institute of Standards.

Commercial Building Demand Response		
Interoperability Category	**Tools, Systems, Key Actors**	**Examples of interoperation across organizational boundaries where agreements must be reached**
policy and regulation	Organizations (LEEDS, ASHRAE) ISO	requires all gov't facilities to cut load, participate in load shedding plans, and implement DR strategies. • GSA specs BACnet in federal facilities • Independent orgs like LEEDS (Leadership in Energy and Environmental Design) and ASHRAE make efforts toward sustainable buildings that can do DR. Lobby gov't bodies. Work on standards.
Business Objectives Strategic and tactical objectives shared between businesses Strategic objective: Save energy and money with RTP service and customer DR, DG Tactical objective: communicate utility needs to customers who can act. Specifically: communicate RTP to the Large Commercial facility owner	Utilities Market Facility mgrs BOMA Building control system vendors ASHRAE	• Utility community works with building community through a collaborative committee to understand needs of commercial building owners and potential DR response of buildings. • Building control system vendors work to develop BACnet standard to allow DR response to utility signals and a standard device-level load reponse interface. • BOMA (Building Owners & Managers Association) promotes real-time price (RTP) and other DR programs and the benefit to building owners to participate and how to do that. • RTP to large commercial customers is really a subset of a wide array of DR customer programs. • Utilities plan their rate structures to include RTP rates for commercial customers and standard implementation. • Utility standards body sets up a process for maintenance of the customer RTP web services standard with BACnet liaison. • Articles in facility management publications explain different utility services and why RTP is best choice to roll out first to serve needs of utilities and large commercial customers.
Business Procedures Alignment between Objectives, Operational Business Processes, and Procedures Stakeholder community	Utility community Facility Management community Stakeholders on	• Stakeholders agree that: o A utility-customer contract is in place that specifies: account IDs, passwords/keys, rate class, web server address, etc. o Utility distributes RTP data using a web service interface with encryption. o RTP message data includes RTP hourly

Commercial Building Demand Response		
Interoperability Category	**Tools, Systems, Key Actors**	**Examples of interoperation across organizational boundaries where agreements must be reached**
members need to realign business with objectives. Stakeholders need to be clear on objectives, and act on them.	path from generator to customer	schedule (with specified units and formats), plus account info and timestamps. • Building community and utility community meet to understand mutual business process. For example: o Utility wants account and price data information to remain confidential, therefore encryption is required. o Hourly rates with day ahead estimates gives building owners sufficient time to plan DR. o Utility requires response to ensure customer non-repudiation. • Compliance determination process,
INFORMATIONAL		
Business Context Awareness of the business knowledge related to a specific interaction Both sides of the interoperability coin need to understand the context of RTP communications to large facility customers.	Stakeholder organizations on building and utility sides Standards bodies Gridwise	• Building community and utility community agree on what RTP messages should be. For example: o Utility sends price data that includes today and tomorrow's hourly rates with prices fixed one hour ahead and future prices estimated, total of 48 hours of prices. o RTP message account information includes utility ID and rate program ID and customer ID and customer password, along with timestamp, all for authentication o Response repeats back RTP data and timestamp. • Technical folks flesh out the specific message details (fields, types, units, structures) consistent with general semantics.
Semantic Understanding Understanding of concepts contained in the message data structures Both sides of the interoperability coin need to	Stakeholder organizations on building and utility sides	• BACnet committee and IEC TC57 committee work out information model changes CIM and BACnet objects for addressing load reduction applications. • There may be non-BACnet devices on the network that need gateways to understand load reduction information.

Commercial Building Demand Response		
Interoperability Category	**Tools, Systems, Key Actors**	**Examples of interoperation across organizational boundaries where agreements must be reached**
understand the meaning of concepts: • What is RTP? • What is contained in "account information" (e.g., what is an appropriate Account_ID)?		
TECHNICAL		

Syntactic Interoperability
 	
Understanding of data structure of messages exchanged between systems
	BACnet XML and Utility Interaction working groups.
	
	IEC TC57 standards body
		• Web services interface to utility agreement:
		  ○ SOAP messages
		  ○ XML details

Network Interoperability Mechanism to exchange messages between multiple systems across a variety of networks	Technical committees to iron out architectural details within business directives	• TCP • IP • IPSec
Basic Connectivity Mechanism to establish physical and logical connections between systems	Technical committees	• Ethernet—10 MBPS • WiFi

A.3 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 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	RTO/ISOs	- Use OWL to federate and extend IEC 61970 CIM with

Congestion Management Market		
Interoperability Category	**Tools, Systems, Key Actors**	**Examples of interoperation across organizational boundaries where agreements must be reached**
Awareness of the business knowledge related to a specific interaction	Market Participants System Suppliers Consultants	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 structure of messages exchanged between systems	System Suppliers Consultants Standards Organizations	- OASIS ebXML message syntax - W3C SOAP message syntax - OASIS UDDI registry and discovery syntax - W3C XML
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