COMMUNICATIONS FOR THE SMART GRID

Mark Adamiak - GE Digital Energy

As the smart grid drives into the main stream of the utility enterprise, it becomes incumbent on the industry to identify an architecture based on what is the smart grid, what are the communication pieces involved, and how do they fit together. The "pieces" are the existing communication standards. The choice of a standard, however, is not a random process. There is an engineering process for the selection of relevant standards and subsequent migration to an Architecture. Such a process was funded by the Electric Power Research Institute and the output of this process is the IntelliGrid architecture [1]. This paper examines the architecture process of identifying the system requirements and the subsequent process of linking the requirements with candidate standards. Finally, the standards already chosen by the NIST as Smart Grid standards are presented.

1. IntelliGrid Enterprise Activities

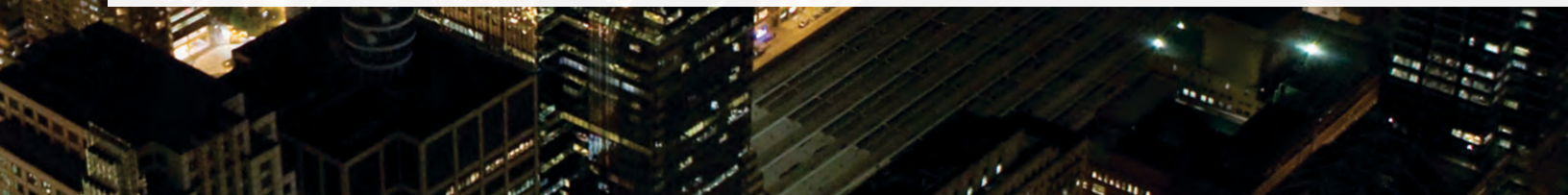
In all cases, an architecture must be based on the functions it is required to perform. In order to identify these functions, a mechanism known as a Use Case was employed. A use case starts with a narrative that describes a specific smart function in the environment of interest. Distillation of the use case identifies data items and their movement through the environment under study. In the energy environment, there are multiple areas of interest.

In order to facilitate categorization of use cases, the energy environment was broken down into 6 primary business functions, namely: Market Operations, Transmission Operations, Distribution Operations, Primary Generation, Distributed Energy Resources, and Customer Services. Over 400 potential use cases were identified and the most demanding of there were elaborated in additional detail to construct a complete high-level set of requirements for the communications infrastructure. The requirements were further categorized as follows:

- Communication configuration requirements, such as one-to-many, mobile, WAN, LAN, etc.
- Quality of service and performance requirements, such as availability, response timing, data accuracy, etc.
- Security requirements, such as authentication, access control, data integrity, confidentiality, non-repudiation, etc.
- Data management requirements, such as large databases, many databases particularly across organizational boundaries, frequent updates, etc.
- Constraints and concerns related to technologies, such as media bandwidth, address space, system compute constraints, legacy interface, etc.
- Network management requirements, such as health and diagnostics of infrastructure and equipment, remote configuration, monitoring and control, etc.

As an example in this paper, the Demand Response use case is reviewed. The IntelliGrid Architecture considered the Demand Response system as part of the Customer Services functional area. While it is clear that Demand Response functionality operates within this domain, it is important to note that Demand Response is not an isolated island of functionality.

The entire premise of the IntelliGrid Architecture is that each of these envisioned applications must interact with other domains and functional areas within the Energy industry. Interoperability between and among other Demand Response systems and other Energy industry applications can be seen as one of the key drivers behind the IntelliGrid Architecture.



Given that a communication channel will exist into the home, commercial, or industrial electrical grid, the IntelliGrid Architecture identified a number of applications that directly touch the Demand Response system.

The complete list can be found on the IntelliGrid Architecture website, but Customer Domain specific functions are listed here as follows[2]:

1. Automatic Meter Reading (AMR)

- Sub-metering
- Load monitoring
- Sub-contracted metering
- Energy usage display
- Measurement of customer outage minutes/hours
- Auto-pay / Pre-pay metering
- Outage detection and isolation
- Remote connect/disconnect
- Demand profiles

2. Customer Trouble Call Management

3. Real-time Pricing (RTP)

- Day ahead schedule
- Hour ahead emergency condition
- Available by-pass mode
- Automatic in-home load curtailment

4. Load Management

- Direct Load Control under emergency conditions
- DER Watt/VAR dispatch

5. Building/Home Energy Management Services

- Building management
- Building security
- Customer remote access
- Equipment monitoring (e.g. clogged air filters, failed water heater element, etc.)
- Customer energy bidding
- Load analysis
- Home insulation level analysis
- Occupancy based heating and lighting controls

6. Electric Car as Generation Source

7. Weather

- In-home weather forecasts
- Lightning location report
- In-home lightning and severe weather alert

In addition, the customer communications infrastructure will enable other IntelliGrid "cross domain" activities such as:

- Feeder Voltage Optimization
- Downed conductor detection
- Faulted feeder isolation / feeder re-deployment
- Distributed Energy control and isolation
- Distribution based VAR support to transmission
- Distribution SCADA
- Microgrid establishment / control

2. IntelliGrid Demand Response Environments

Each of the myriad interrelated functions defines its own set of detailed functional and non-functional requirements. An architecture is not, however, intended to simply fulfill a patchwork of requirements. The architecture is not simply the union of the lists of detailed requirements for each function. Functions often have conflicting requirements and a good architecture must be flexible enough to accommodate such incongruous anomalies. To realize this, the IntelliGrid Architecture invented what were called "Environments".

An IntelliGrid Architecture Environment is defined as an information environment, where the information exchanges of power system functions have essentially similar architectural requirements, including their configuration requirements, quality of service requirements, security requirements, and data management requirements. These Environments reflect the requirements of the information exchanges, not necessarily the location of the applications or databases (although these may affect the information exchanges and therefore the environment). Since functions can have multiple types of information exchanges, these functions often operate across multiple Environments.

The IntelliGrid Architecture defined twenty one Environments that completely describe the communication requirements for the information exchanges as shown in Figure 1[3]:

Demand Response and all of the ancillary services it provides, enables, or directly touches, operates in several of these environments. A brief synopsis of the relevant environments and typical applications shown in Figure 2[3]:

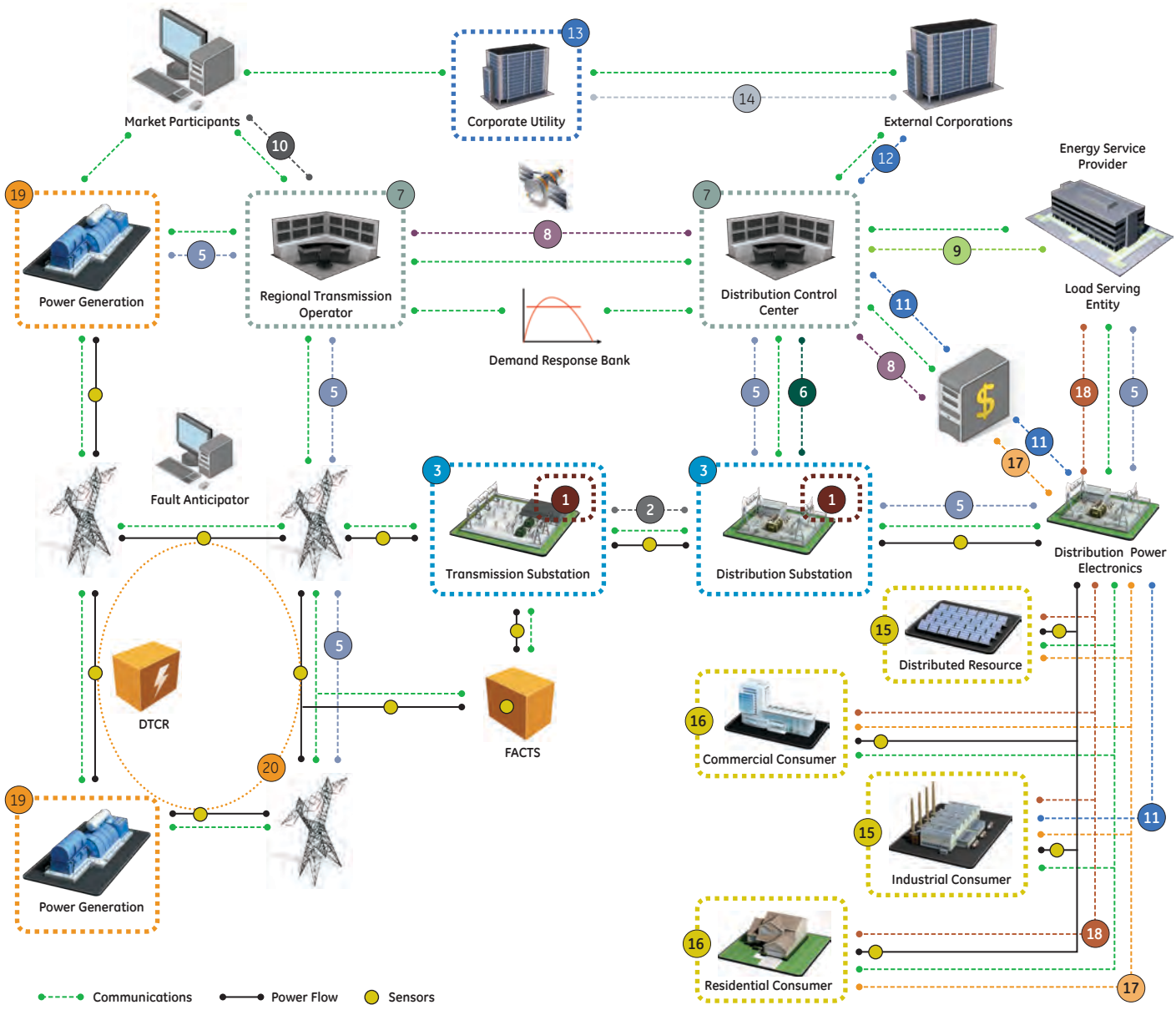
3. IntelliGrid Requirements for Demand Response Implementations

Based upon the above Environments, the IntelliGrid Architecture proposes a base set of high level requirements for Demand Response Systems that will also aid in achieving interoperability with other systems sharing the same infrastructure. These requirements are categorized as follows [3]:

Configuration Requirements

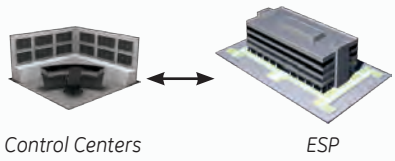
- Support interactions between a few "clients" and many "servers"
- Support peer to peer interactions
- Support interactions across widely distributed sites
- Support the frequent change of configuration and/or location of end devices or sites
- Support multi-cast or broadcast capabilities
- Support interactions within a contained environment (e.g. substation or control center)

IntelliGrid Architecture

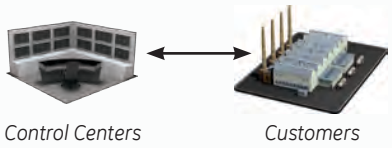


1	Deterministic Rapid Response Intra-Substation	8	Inter-Control Center	15	DER Monitoring and Control
2	Deterministic Rapid Response Inter-Site	9	Control Centers/ESPs	16	Intra-Customer Site
3	Critical Operations Intra-Substation	10	RTOs / Market Participants	17	Intra-Cusomer Sites
4	Inter-Field Equiment	11	Control Center / Customer Equipment	18	Customer / ESP
5	Critical Operations DAC	12	Control Center / Corporations	19	HV Generation Plant
6	Non-Critical Operations DAC:	13	Intra-Corporation	20	Field Equipment Maintenance
7	Intra-Control Center	14	Inter-Corporation	21	Special

Figure 1.
The IntelliGrid Architecture defines 21 Environments that span the entire Electric Energy Enterprise



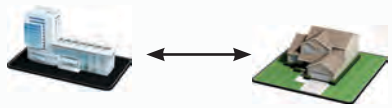
Environment 9: Control Centers to ESPs embodies the requirements for communications between utility control centers and Energy Service Providers or "aggregators". Typical applications in this environment include Real-time pricing negotiations, aggregated customer metering and settlements as well as data mining for later use in market operations. This is characterized as a business-to-business (B2B) environment having very strict requirements for security and a contractual level of timeliness and record keeping (and audit trails).



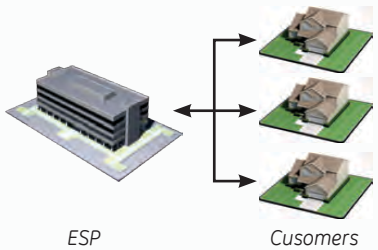
Environment 11: Control Center to Customers encompasses the requirements for what has traditionally been termed commercial or industrial metering and includes the requirements for any data exchange that goes directly between control centers and customer sites. Typical applications include metering of large customers, control of distributed energy resources, and load curtailment. This is characterized as a B2B environment but involving operational rather than financial data.

Environment 15: DER Monitoring and Control encompasses the communication requirements between distributed energy resources and the organizations that must monitor and operate them. Typical applications include an ESP aggregating data from or operating multiple small generators including renewable power, small hydro, co-generation or any other mini-grid. This may also include demand response and adjustment of power quality. This environment is characterized by the fact that it is vital that these message exchanges are not tampered with, monitored, or interfered with by unauthorized persons.

Environment 16: Intra-Customer Site defines requirements for communications that are local to customer sites (residential, commercial, or industrial). Typical applications include a customer printing processes online or offline in response to RTP, a customer locally managing a distributed energy resources in response to external factors (environment, price, regulations, etc.). Additionally this also includes building and home automation systems. This environment is characterized by critical data with local scope and limited impact on the overall power grid. Data is real-time potentially peer-to-peer with application specific security.



Environment 17: Inter-Customer Sites captures requirements for communications between customer sites (residential, commercial, or industrial). This is a relatively new environment that is not widely deployed yet but would include typical applications such as coordination of customer loads (e.g. A/C or refrigeration compressor startup) and mini-grid management. It is characterized by high security requirements because data crosses organizational boundaries.



Environment 18: Customer to ESP. This environment encompasses the communication, distributed processing, security, and data management requirements for applications that exist between ESPs, typically the distribution level energy utility, and the end-use point-of-sale energy customers like residential homeowners and apartment dwellers. Typical applications include automatic (or manual) meter reading, monitoring and control of DER, demand response and RTP. It is characterized by extremely large volumes of data with frequent con-figuration and topology changes to the communications network. Commands are often broad-cast due to the large number of end users but address space must be massively scalable.

Figure 2.
A brief synopsis of the relevant environments and typical applications

Quality of Service Requirements

- Provide medium speed messaging on the order of 10 seconds
- Support contractual timeliness (data must be available at a specific time or within a specific window of time)
- Support medium availability of information flows of 99.0+% (~3.5 days/year outage)

Security Requirements

- Provide Identity Establishment Service (you are who you say you are)
- Provide Authorization Service for Access Control (resolving a policy-based access control decision to ensure authorized entities have appropriate access rights and authorized access is not denied)
- Provide Information Integrity Service (data has not been subject to unauthorized changes or these unauthorized changes are detected)
- Provide Confidentiality Service (only authorized access to information, protection against eavesdropping)
- Provide Inter-Domain Security Service (support security requirements across organizational boundaries)
- Provide Non-repudiation Service (cannot deny that interaction took place)
- Provide Security Assurance Service (determine the level of security provided by another environment)
- Provide Audit Service (responsible for producing records, which track security relevant events)
- Provide Security Policy Service (concerned with the management of security policies)
- Provide Path and Routing Quality of Security (being able to determine a secure communication path)
- Provide Firewall Transversal
- Provide Privacy Service (the ability to ensure person information is not disclosed)
- Provide User Profile and User Management (combination of several other security services)
- Provide Security Protocol mapping (the ability to convert from one protocol to another)
- Provide Security Discovery (the ability to determine what security services are available for use)

Network and System Management Requirements

- Provide Network Management (management of media, transport, and communication nodes)
- Provide System Management (management of end devices and applications)
- Support extensive data validation procedures

Data Management Requirements

- Support the management of large volumes of data flows
- Support extensive data validation procedures
- Support keeping data consistent and synchronized across systems and/or databases
- Support timely access to data by multiple different users
- Support frequent changes in types of data exchanged
- Support management of data whose types can vary significantly in different implementations
- Support specific standardized or de facto object models of data
- Provide discovery service (discovering available services and their characteristics)
- Provide conversion and protocol mapping
- Support the management of data across organizational boundaries

4. IntelliGrid Design Principles [4]

In order to design an architecture, one must have "guiding principles" as to how to identify the pieces of the architecture and how they are to be put together. The IntelliGrid architecture identifies several such principles described below.

One of the most important system integration principles in IntelliGrid is the concept of Technology Independent Architecture (TIA). TIA is technology neutral or technology agnostic. It can insure successful integration of the various utility enterprise applications without requiring changes to the application's internal operation. It can also achieve high level of interoperability and interworkability with the built-in intelligence of auto-configuration and self discovery. Figure 3 illustrates the TIA framework.

Three key information-modeling elements in TIA framework are,

- Common Services – These are atomic building blocks frequently required by the utility applications. IntelliGrid further breaks the common services down to four categories, namely "system and network management services", "data management and exchange services", "common platform services" and "common security services".

- Common Information Models – These are common data that are exchanged between services and applications. This includes the suggested data format, data attributes and their relationships.

- Generic Interfaces – Generic Interfaces are used as the mechanism for exchanging Common Information Model data between services. Generic Interfaces correspond to how data is exchanged. It specifies a set of standard verbs such as "get", "set", "report", which allows different applications to communicate with each other.

These common information-modeling elements are the key to achieving higher-level interoperability of power system distributed information systems.

Common Services

Common Services are commonly defined functionality derived by identifying the crosscutting distributed information requirements. Common Services allow components to be treated as black boxes. This facilitates greater flexibility, as components are less dependent on how each works internally.

However, the use of Common Services does not by itself substantially reduce the complexity of dealing with different platforms such as Java, .Net or Web Services. Also, Common Services do not necessarily deal with the discontinuity of the meaning of data. Lastly, Common Services do not deal with the discontinuity caused by different data access mechanisms such as "read/write data" or "subscribe to data".

To overcome semantic heterogeneity a common information model is used as the common language that all services use to communicate. To overcome platform heterogeneity, the generic interface is required. The generic interface can be implemented on any platform. While the different implementations of the generic interface are not interoperable, "off the shelf", the mapping from one platform specific implementation to another is simple and well known.

Common Information Models

In order to precisely describe the meaning of a set of terms, engineers often create an information model. An information model describes a collection of related real world objects. An information model describes objects in terms of classes, attributes and relationships and provides unique names and definitions to each object.

The EPRI/IEC Common Information Model (CIM) describes data typically used in the power system. The CIM contains object types such as substations, breakers, and work orders as well as other data typically found in an EMS, SCADA, DMS, or work, and asset management system. More recently, the CIM is being extended to include transmission reservation and energy scheduling information. In general, the benefit of creating an information model include:

- Models give context to data improving understanding and productivity.

- Models enable automation of setup and maintenance tasks.

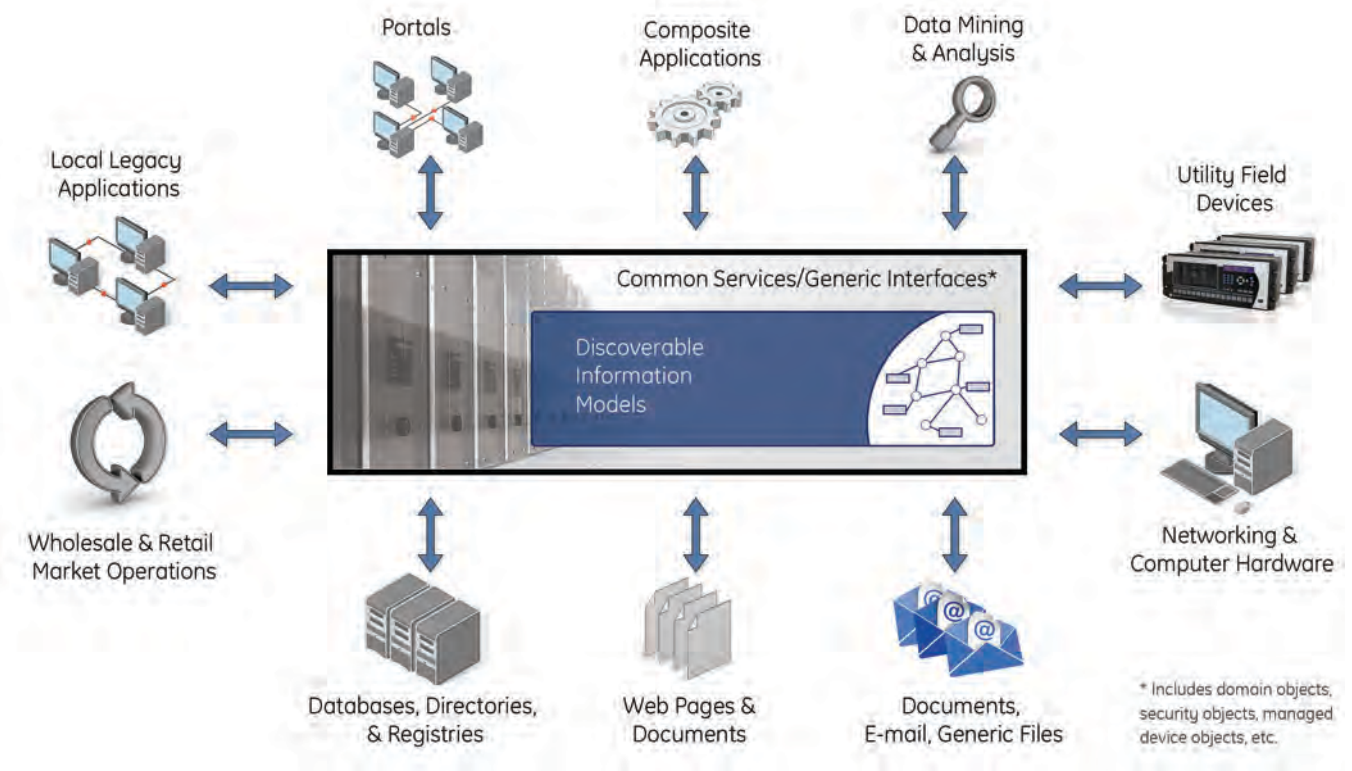


Figure 3.
Technology Independent Architecture - The guiding principle of the IntelliGrid Architecture shows that Common Services, Common Information Models, and Generic Interfaces enable scalable interoperability in a heterogeneous technology environment.

Generic Interfaces

The mechanism used to exchange data is determined by an application's interface. However, the native interface provided by an application is typically limited. For example, typically existing interfaces:

- Do not expose data within the context of a common inter-application data model.
- Do not provide a means to discover what business object instances are serviced by a particular component instance other than a rudimentary listing of legacy IDs (tags) that cannot be viewed within the context of an inter-application data model such as a power system network model.

REMEMBER THAT DEVELOPING AN INDUSTRY-LEVEL ARCHITECTURE IS A PROCESS – NOT AN END POINT

Without a means to discover what data an application processes, plug and play is nearly impossible to achieve. To address these impediments to plug and play and the need for a common exchange mechanism, "Generic Interface" is introduced to specify how data are exchanged. The phrase "Generic Interface" is an umbrella term for four interfaces types:

- An interface for mapping names to ID's and visa versa.
- A request/reply oriented interface that supports browsing and querying randomly associated structured data – including schema (class) and instance information.
- A publish/subscribe oriented interface that supports hierarchical browsing of schema and instance information. This interface would typically be used as an API for publishing/subscribing to XML formatted messages.
- Applications use the generic interfaces to connect to each other directly or to an integration framework such as a message bus or data warehouse. A technology neutral interface allows applications to be designed independently of the capabilities of the underlying infrastructure.

Generic interfaces provide the following key functionality required for creation of a plug and play infrastructure:

- Interfaces are generic and are independent of any application category and integration technology. This facilitates reusability of applications supporting these interfaces.
- Interfaces support schema announcement/discovery – The schemas are discoverable so that component configuration can be done programmatically at run time. Programmatically exposing the schema of application data eliminates a great deal of manual configuration.
- Interfaces support business object namespace presentation – Each component describes the business object instances that it supports within the context of a common namespace shared among all applications such as a power system network model like the EPRI Common Information Model (CIM). It is not enough to merely expose the application data schema, one must also expose what specific breakers, transformers, etc., that an application operates on. This also eliminates manual configuration as well as provides a means for a power system engineer to understand how enterprise data is organized and accessed.

5. IntelliGrid Recommended Implementation Technologies

There are too many recommendations to capture in this project summary, but common themes can be identified as follows[1]:

- Harmonize the existing common services, information models, and interfaces, as well as create new standards where they are needed, so the power industry speaks a common communications language of 'nouns' and 'verbs' that can be translated into different technologies. This is a key requirement for the higher levels of system integration now emerging across the energy industry
- Integrate security, systems, network management, and technical development (i.e. new technologies), which have too often been considered separate tasks.
- Unify technologies between power system automation networks, corporate networks, and inter-business networks, again by linking them to common information models, services, and interfaces.
- Remember that developing an industry-level architecture is a process – not an end point. Requirements and enabling technologies are constantly changing. Although the guiding principles should remain constant, individual solutions will change over time.

Based on the identified design principles, IntelliGrid makes a link from design guidelines to recommended technologies that best embody the stated principles and meet the identified requirements. IntelliGrid makes a point of recognizing that many needed technologies may not exist and encourages the identification and subsequent standardization of such technologies.

The list below is a first level summary of the "primary" recommended technologies for the identified environments. The list is organized by functional layer. For the complete list of applicable technologies, please refer to the IntelliGrid.info website[3]:

Data Exchange:

- IEC61850 – Communication Networks and Systems in Substations
  - Data Models
  - Abstract Services
  - Substation Configuration Language
- ANSI C12.19 Metering Tables

- AEIC Guidelines for Implementation of ANSI C12.19
- IEC61970 Part 3 Common Information Model (CIM)
- IEC61970 Part 4 Generic Interface Definition
- IEC61968 SIDM System Interfaces for Distribution Management
- IEC60870-6 Inter Control Center Protocol
- IEC62325 on Framework for Energy Market Communications
- NERC e-tagging
- NAESB OASIS for Market Transactions
- IEC62056 – Data Exchange for Meter Reading, Tariff, and Load Control
- Universal Description, Discovery, and Integration (UDDI)
- Simple Object Access Protocol (SOAP)
- EbXML
- XML Metadata Interchange (XMI)
- Meta Object Facility (MOF)
- Globally Unique Identifiers (GUID)
- S/NTP (Simple/Network Time Protocol)
- ANSI/ISO/IEC 9075 – Structured Query Language (SQL)

Security:

- ISO/IEC 10164-8:1993 Security Audit Trail Function - Information technology - Open Systems Interconnection - Systems Management - Security,
- ISO/IEC 18014-1:2002 Time-Stamping Services - Information technology - Security Techniques - Part 1: Framework - Security, Data Management
- ISO/IEC 10181-7:1996 Security Audit and Alarms Framework - Information technology - Open Systems Interconnection -- Security Frameworks for Open Systems - Security,
- FIPS PUB 112 Password Usage - Security,
- FIPS PUB 113 Computer Data Authentication - Security,
- RFC 1510 The Kerberos Network Authentication Service (v5)
- RFC 2196 Site Security Handbook - Security,
- RFC 2401 Security Architecture for the Internet Protocol - Security,
- RFC 2527 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework - Security,

THERE ARE MANY LONG-TERM BENEFITS TO THE ENERGY INDUSTRY THAT WILL BE REALIZED THROUGH IMPLEMENTATION OF THE INTELLIGRID PRINCIPLES AND RECOMMENDED TECHNOLOGIES

Transport:

- TCP / Internet Protocol IPV4 / IPV6

Network Management:

- Simple Network Management Protocol (SNMP)

Physical/Data Link:

- IEEE 802.x (LAN, WAN, WiFi, WiMax, Ethernet)
- SONET
- ATM

6. NIST Selected Smart Grid Standards – Rev 1.0

As part of the Energy Independence and Security Act of 2007, the North American Institute of Standards and Technology (NIST) was mandated by Congress to coordinate a "framework of protocols and model standards to achieve interoperability of the Smart Grid". As part of this mandate, NIST has recently released the first set of "accepted" standards for use in Smart Grid communications [5].

It is to be noted that this is a work in progress and is not exclusionary. The list of these standards follows closely to the recommendations made by the IntelliGrid document. The list of selected standards is as follows:

- AMI-SEC System Security Requirements
- ANSI C12.19/MC1219 – Revenue Metering
- BACnet ANSI ASHRAE 135-2008/ISO 16484-5 – Building Automation
- DNP3 - Substation and feeder device automation
- IEC 60870-6 / TASE.2 - Inter-control center communications
- IEC 61850 - Utility automation and protection
- IEC 61968/61970 - Application level energy management system interfaces
- IEC 62351 Parts 1-8 - Information security for power system control operations
- IEEE C37.118 - Phasor measurement unit (PMU) communications
- IEEE 1547 - Physical and electrical interconnections between utility and distributed generation (DG)
- IEEE 1686-2007 - Security for intelligent electronic devices (IEDs)
- NERC CIP 002-009 - Cyber security standards for the bulk power system

- NIST Special Publication (SP) 800-53, NIST SP 800-82 - Cyber security standards and guidelines for federal information systems, including those for the bulk power system
- Open Automated Demand Response (Open ADR) - Price responsive and direct load control
- OpenHAN - Home Area Network device communication, measurement, and control
- ZigBee/HomePlug Smart Energy Profile - Home Area Network (HAN) Device Communications and Information Model

This list will continue to grow as new standards are identified and as new standards are developed to meet the identified gaps in the existing standards.

7. Conclusion

The IntelliGrid Architecture provides a foundation for the operation of the Smart Grid and offers an optimized approach to build future visions. There are many long-term benefits to the energy industry that will be realized through implementation of the IntelliGrid principles and recommended technologies.

Clearly the IntelliGrid Architecture has profound ramifications for a broad range of advanced power systems applications. Careful planning of an open and standards-based system design will support integration of advanced systems thus realizing the IntelliGrid vision for the Smart Grid of the future.

8. References

[1] Peter Sanza, Joe Hughes, et. al.; "IntelliGrid Architecture Volume I 'User Guidelines and Recommendations' Final Report", 2004, Electricity Innovation Institute (E2I) Consortium for Electric Infrastructure to Support a Digital Society (CEIDS); www.IntelliGrid.info.

[2] Peter Sanza, Joe Hughes, et. al.; "IntelliGrid Architecture Volume II Appendix F 'Task 1 Enterprise Activities' Final Report", 2004, Electricity Innovation Institute (E2I) Consortium for Electric Infrastructure to Support a Digital Society (CEIDS); www.IntelliGrid.info.

[3] Peter Sanza, Joe Hughes, et. al.; "IntelliGrid Architecture Volume IV Appendix E 'Environments' Final Report", 2004, Electricity Innovation Institute (E2I) Consortium for Electric Infrastructure to Support a Digital Society (CEIDS); www.IntelliGrid.info.

[4] Peter Sanza, Joe Hughes, et. al.; "IntelliGrid Architecture Volume IV 'Technical Analysis' Final Report", 2004, Electricity Innovation Institute (E2I) Consortium for Electric Infrastructure to Support a Digital Society (CEIDS); www.IntelliGrid.info.

[5] NIST Recognized Standards for inclusion in the Smart Grid Interoperability Standards Framework – Release 1.0; www.nist.gov/smartgrid/standards.html

Mark Adamiak

Mark Adamiak is the Director of Advanced Technologies for GE Digital Energy and is responsible for identifying and developing new technology for GE's protection and control business. Mark received his Bachelor of Science and Master of Engineering degrees from Cornell University in Electrical Engineering and an MS-EE degree from the Polytechnic Institute of New York. Mark started his career with American Electric Power (AEP) in the System Protection and Control section where his assignments included R&D in Digital Protection and Control, relay and fault analysis, and system responsibility for Power Line Carrier and Fault Recorders. In 1990, Mark joined General Electric where his activities have ranged from advanced development, product planning, application engineering, and system integration. Mr. Adamiak has been involved in the development of both the UCA and IEC61850 communication protocols, the latter of which has been selected as a NIST Smart Grid protocol. Mark is a Fellow of the IEEE, a member of HKN, past Chairman of the IEEE Relay Communication Sub Committee, a member of the US team on IEC TC57 - Working Group 10 on Utility Communication, the US Regular Member for the CIGRE Protection & Control study committee, a registered Professional Engineer in the State of Ohio and a GE Edison award winner for 2008.