WHITE PAPER ON COMMUNICATIONS FOR SMART ENERGY

Contents

1. Introduction

Alex is driving home after a long day at work and is concerned about the blackened sky filled with thundering ominous clouds. This morning, he had glanced at the gloomy forecast on his mobile device and knew it was going to be an interesting ride back. The air is getting humid as winds are picking up speed and light showers are falling on his windshield. He calls home to check up on the family. Indeed, everyone is in the house safe and sound but the home environment temperature has decreased and the entertainment system power outlet has been shut off. This is a precaution he takes when the barometer plunges, just in case power surges from lightning strikes penetrate the premises and damage his sensitive electronics. His Home Automation system is what he depends on nowadays to monitor and control power flow and levels of energy consumption from his appliances, lighting, entertainment and security systems, based on pre-set conditions he's programmed on the Smart Home web portal. Behind the scenes, their Smart Meter is monitoring their energy usage and broadcasting it periodically over an encrypted wireless mesh network to the utility's nearest hub.

As he's about to take an off-ramp and exit the highway, he sees the wind turbine farm in the distance and notices their long blades are turning at a high rate of speed. Winds are now increasing to gust velocity. Just a few miles away from home, the skies deliver on their menacing brew as a lightning bolt shoots across the road and strikes a tree in the distance. He watches in awe as the top half of a large tree falls toward the road and slices through overhead power lines. The resulting flashes of light and sparks dance around the ground, immediately causing a power outage in the vicinity as street lights lose power and homes and business go dark in an instant. Fortunately, no one was in the path of the tree as it lies harmlessly across the road, blocking his way.

Pulling over on the soft shoulder for safety, he calls the hydro company contact center from his cell phone and reports the scene he has just witnessed, providing exact GPS coordinates available from his in-car navigation system. His next call is home to see if all is well. His wife reports that they heard the thunderclap sounds and ground vibrations from the lightning strike close by; lost power briefly but within a matter of minutes, the power was back on, albeit with the air conditioning completely turned off. She checks the In-Home Display, which shows the power was out for only 4 minutes and the utility turned off the air conditioning unit to conserve power and redeploy it to another affected neighborhood. Fortunately, the stored energy from the rooftop solar panels powered the battery backup emergency lights in the house during the outage.

Feeling comforted that everyone is safe; he waits in his hybrid car until the deluge of rain subsides and turns around to head down an alternate road. Just as he's turning left, a hydro company repair truck and lineman crew travel in the direction of the fallen tree to deal with the danger.

This scenario is a glimpse of the possibilities at hand for an advanced power transmission and distribution network. The integration of Smart Grid, Smart Metering and Smart Home, termed Smart Energy, would enable the enhancement and progress of how we work, live and interact with energy as a whole. Underpinning all this is seamless communications across all components of future-state solution architectures. The networking systems in conjunction with the control and communications infrastructure are a key foundational element for enabling the benefits of Smart Energy, and are the main theme of this White Paper.

2. PART 1

2.1 Business Context

In the last few years, most utilities around the world have heard the drumbeats of radical change demanded by society to deal with non-renewable energy sources, global warming and continued growth of energy demand in the face of tighter supplies. This has forced them to update their long-term strategies and seek out innovative ideas and solutions to deal with their most pressing concerns. The 2009 Platts/Capgemini Utilities Executive Study (http://www.us.capgemini.com/plattsstudy) found that the five most critical issues facing the energy industry today are regulation, the environment, infrastructure, finance, and workforce management. Furthermore, over the next two years, executives plan to increase spending on government/regulatory affairs, risk management, building new transmission and information technology. In addition, over the next 5 to 10 years, the respondents expect the industry's use of technology and conservation/energy efficiency advocacy to increase substantially. Of particular concern as it relates to this article is that utility executives continue to view the need for new and upgraded infrastructure and two-way communications as the most critical issue impacting the current and future state of the industry.

For example, during interviews with utility executives regarding these concerns, some were quoted as saying the following statements:

- "We've got an aging infrastructure out there; we've got reliability concerns based on the state of that equipment. It's old, it's analog equipment. It's reliable, but it's not the type of automated, highly computerized systems that we have seen developed in a lot of other industries, whether it's in telecommunications, banking, or other things like that. So there is going to be a lot of attention paid to that and a lot of investment made in delivering that power to the customers."
- "Smart Grid. To me, that's still kind of a nebulous term. There are a lot of pieces to it. But I think that's going to be an area of increased investment, as well, to squeak more efficiency out of the system, as well as to potentially come up with some additional ways to make the customer's demand side more efficient. But we need technology development and supplier capabilities in all those areas. . . . Most of those technologies are reasonably developed. It's just a matter of deciding which investments are prudent and then putting them in place, and kind of tracking the data and using it effectively. "
- "Probably the new and emerging area of technology is going to be on the customer side. The combination of smart meters and robust communication networks, I think, offers the same opportunity as, say, in the 1980s looking at a PC. We have no idea how many applications can be driven. But if you connect the dishwasher with the utility control room, the opportunities to

manage the system are exponentially improved. Ten years from now you'll look at today's technologies with smart meters and the ability to remotely turn on and off a customer, read daily reads, etc., we'll look back at it as if it's a joke. It'll seem so crude."

- "We have a need for more Smart Grid type information. One of those sorts of self-healing situations. Typically you will put three of them in an area and they communicate with each other, and when there is a fault the three communicate with each other and determine where the fault is at. Then they restore as much as they can and isolate where the problem is at. I see more of a need for things like that."
- "I've just been very disappointed that while these systems have been out there....there's just been too much of this proprietary software, proprietary systems, no standards that have been developed that you can use or that the industry has chosen to use that will give utilities flexibility. I've got this system and this utility has got that system. They can't talk to each other. It's like everybody is out here on an island with all these different systems. Even within the utility you've got a SCADA (supervisory control and data acquisition system), you've got an outage management system, you may have an AMI system, you may have a GIS [geographic information system], and customer service, a CIS [computer information system], and all of these are not interfaced and don't work very well together. We've done a lot and we've come a long way. But there are a lot of challenges out there to get the systems within a utility all communicating and talking together."

Governments throughout the world are also powerful stakeholders in the modernization of power grids and have set direction and vision to the utilities on behalf of their constituents. Three primary directives are energy conservation, distributed generation, and the "greening" of the electricity business, which implies investment in new sectors and 'green' job creation.

2.2 Business Objectives

Capgemini's experience with leading global utilities has uncovered many Smart Energy business objectives. The business strategies, scenarios, requirements and objectives are typically derived using intense workshop sessions facilitated in one of our Accelerated Solutions Environments (ASE). The resulting themes driving utilities' visions and plans can be highlighted with the following key business objectives, which are but a subset of the full and evolving Smart Energy business landscape:

1. Integration of new distribution generation sources into the existing grid
   - With the increase in smaller and more distributed generation such as windmills, solar, biomass, gas turbine, etc, there is a need to implement Smart Grid concepts which will absorb these new sources of generation and support continued reliable and safe operation of the existing distribution system. Distributed generation must be integrated in a manner that maximizes up time by automating isolation and reconnection events; maintaining power quality by monitoring and supplementing voltage requirements; minimizing costs while maximizing the availability of supply.
2. Improving the reliability and operations of the electrical distribution network

- The electrical distribution system requires increased automation in varying degrees to provide for better near-real time monitoring and control, automatic restoration and optimized operations to reduce overall utility costs and improve customer satisfaction.

3. Optimizing electrical outage restoration
    - Customer outages need to be minimized through a combination of station/lines automation, integration of various enterprise systems; greater field information collection and quicker more efficient fault restoration by enhancing field force mobilization. In parallel customers require notification of outage status through a variety of media in their homes.
4. Customer Enablement
    - Through the deployment of Smart Meters in the home, customers will eventually be migrated to Time-Of-Use billing. Tools, devices and information should be made available to customers to provide them better control and allow them the opportunity to better manage their electrical consumption. Some of the types of interfaces and media proposed are:
        i. Two-way communicating programmable thermostats and in-home displays
        ii. Web presentment of information and central management or customer control of devices
5. Worker Safety
    - Safety is always a prime directive of a utility especially given the dangerous nature of electricity in general. Its handling must always be done with upmost caution, proven processes and best available technologies.
    - Utilizing two-way communications, utility workers will be monitored in the field in near real-time for incidents that impact their safety or the public's, and their location will be known. Messaging should include information required to deal with outage scenarios and dispatch the appropriate support based on the incident arising.
6. Asset Security
    - Increased and improved utility asset monitoring and security is required, leveraging streaming data provided by video cameras and perimeter sensors located at distribution feeder stations and other strategic sites. A high-speed and high bandwidth network will be needed, with intelligence capability that analyzes the incoming feeds and escalates to monitoring centers for dispatch.

Figure 2: Smart Energy Business Objectives

What are the strategies utilities must undertake to enable progress towards this vision? First and foremost, the low-voltage distribution grid system requires extensive modernization. Currently, primitive communications exist that only allow one-way control of distribution equipment and devices such as Reclosers, Switches and Voltage Regulators. Remote control of these devices and high-speed communications to centralized distribution management systems are required to enable the Smart Grid. Conversely, the high-voltage transmission grid system has traditionally been engineered with greater intelligence and flexibility than the distribution grid. Transmission Energy Management Systems (EMS) have been in place for decades, relying on communication protocols such as SCADA running on serial or low-speed digital communication links.

An advanced distribution management system requires prudent technological convergence of high and low-voltage systems, providing seamless and efficient operational control across all utility assets. An architectural framework outlining appropriate Smart Grid, Smart Meter, Smart Home principles, standards and possible roadmaps for the requisite communications technologies, systems and infrastructure is needed. As utility planners reach out to the vendor and system integrator community, they are faced with a myriad of options and choices. It is the purpose of this White Paper to outline an approach, present a structure, discuss communication technology trends and offer strategies to support the utilities in their quest in achieving real benefits and transforming their business towards Smart Energy.

3. PART II

3.1 Applying the IAF Approach to Smart Energy Objectives

The overall approach towards complex issues in business, information, systems, infrastructure and its interdependencies is called architecture. Most large Smart Energy initiatives that Capgemini embarks on with its clients are comprised of two major integrated elements, a Distribution Management System (DMS) and Intelligent End Devices (IED). These elements need to be absorbed into a complex solution of technologies, systems, IT integration, electrical networks and devices, and communication networks requiring extensive cyber and physical security. The scope of these undertakings is typically delivered through more than 10 project work streams. A solution architecture team provides primary direction and co-ordination of the work streams from an end-to-end solution perspective. They apply Capgemini's Integrated Architecture Framework (IAF) to set the foundation for the project. IAF is a framework that shows the dependencies and relationships between six Aspect Areas of issues that must be analyzed and solved. These Aspect Areas are:

1. Business
    - What business services and processes are required to support the mission?
    - How do these services need to be organized?
2. Information
    - What information and knowledge is needed to support the business services and processes defined in the business architecture?
    - How does this information and knowledge need to be organized and distributed to most effectively support the business?
3. Information Systems
    - What automated systems are needed to support the business services and processes?
    - How should these systems be best organized?
4. Technology infrastructure
    - What is the structure of hardware, systems software and networks required to support the information systems services?
5. Security
    - What is required to mitigate known risks to the architecture implementation?
    - Which specialized services and components are needed to deliver the required security?
6. Governance
    - Addresses the manageability and quality of the architecture implementation

IAF is a communication framework as well as an analysis framework. It helps to structure and manage complexity within an industry such as Utilities. Each Aspect Area can be described at different levels of contemplation, termed Abstraction Layers:

a. Contextual Layer (Discovery)
b. Conceptual Layer (Visioning)
c. Logical Layer (Future State)
d. Physical Layer (Mobilization)

IAF uses Aspect Areas and Abstraction Layers to separate different types of architectural deliverables (artifacts) into a structure that allows different stakeholders to get at what they need whilst retaining end-to-end traceability.

An illustration of IAF is thus represented as follows:

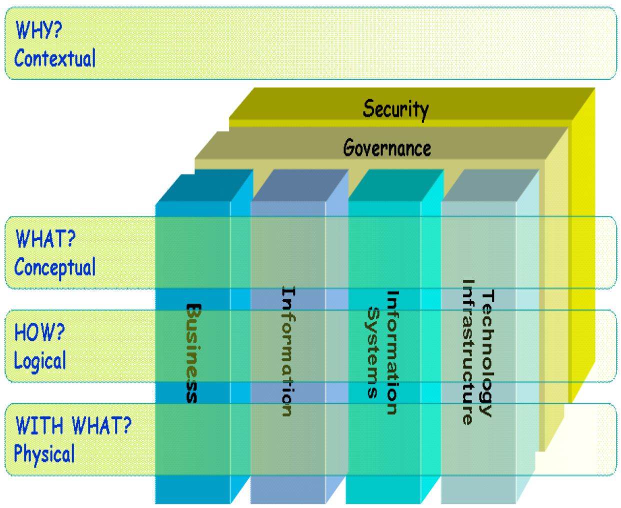


Figure 1: IAF Framework

From a control, communications and networks perspective, it is instructive to understand where and what the 'Line of Sight' is within the Framework, and position various strategic elements appropriately. In Part I, the utility Business Aspect Area was discussed at a high-level in the Contextual and Conceptual layer.

At this point, let's review briefly the Information, Information Systems and Technology Infrastructure aspect of the model as it applies to utilities. What shapes the type of information required of Smart Energy solutions; their sources, event frequency, destination, organizational and customer needs? Which applications are needed to process the data; what are their response time, criticality and availability requirements so that ultimately, seamless and invisible end-to-end communication systems and infrastructure, melding wireless and wired networks are architected, engineered and constructed to meet the needs of the business.

3.2 Information

The impetus for communications relies on motivation and need. To assert communications exists implies a source and destination. Understanding a communication message assumes a common language and quality medium of transmission. Successful response to a message means expected behavior was achieved temporally.

These basic tenets drive enterprise and communication architecture decisions. Using the six utility business objectives outlined previously, let us analyze a process to deconstruct and identify the essential informational elements and requirements needed to drive the right decisions for Smart Energy communications infrastructure.

3.3 Distribution Generation Integration, Improved Reliability and Operations, Optimizing Outage Restoration

The first three business objectives, Distribution Generation Integration, Improved Reliability and Operations and Optimizing Outage Restoration have similar informational requirements primarily because they are derived from the same common equipment, IEDs and legacy RTUs.

Connection of Distribution Generation (DG) supply sources to utility distribution system feeders impacts electrical behavior:

- Steady-state and transient voltage profiles and
- Current distribution along the feeder

These impacts must be controlled. To accomplish this, the design of the power equipment, protection, control and metering systems used at the DG facility interconnection must meet specific requirements:

- Control and telecommunications facilities are required at the DG facilities connected to the utility's transmission and distribution system for provision of protection and real time operating data
- The quantities and device statuses are to be provisioned, monitored and controlled for continuous transmission to utility's control center

General requirements for substation automation in support for all three business objectives from a control and communications perspectives are:

- All or some of the following Intelligent End Devices (IED) require remote monitoring and/or control:
    - Circuit Fault Locators
    - Smart Capacitors
    - Smart Line Monitoring Devices
    - Smart Reclosers
    - Smart Switches
    - Smart Voltage Regulators
    - Equipment Monitoring (Oil, Pressure, Moisture, Temperature, Acoustic)
    - Storage
    - Station RTU
    - Smart Meters
- Substation real-time data information from IEDs follow the IEC 61850 or DNP3 standard;
- These standards can be described as:
    - An object model of the information available from the different primary equipment and from the substation automation functions
    - A communication specification between the IEDs of the substation automation system

- A set of protocols that can run over TCP/IP networks supporting point-to-point or multicast communications
- A set of protocols that can also run over substation LANs using high speed switched Ethernet to obtain the necessary response times of < 4 ms for protective relaying

The Optimization Outage Restoration business objective has additional informational components related to the utility's workforce response to outage situations. These components require a different set of communication requirements primarily driven from workforce management, incident and trouble management processes. These processes rely on datasets pertaining to location-based information drawn from GIS systems and location-based services such as GPS. Outage events rely on these data to accurately pinpoint source of issues and equipment at fault. Workforce management information depends on static and real-time personnel data such as availability, skills, current location using AVL (Automatic Vehicle Locator), workgroup, etc. so that incident management processes can optimally identify and dispatch the most appropriate resources to deal with outages requiring manual intervention.

Another element to consider is the targeted service levels contracted between the utility and its customers. These agreements determine the level of investment in equipment and resources required to deal with outages in a timely manner.

3.4 Customer Enablement

Customer Enablement provides the tools and devices such that customers will have the means to better understand and control their energy usage and consumption and allow increased automation within their home or commercial buildings. There are many sources of information possible that can affect this objective such as placement of electronic sensors within an environment that can sense, measure, convert or calculate readings and results for such things as temperature, humidity, pressure and energy usage, etc. Examples include automated pool pump and water heater controllers, in-home power cost monitors and thermostats to name but a few. The communications with sensors is directed to a gateway hub that receives the telemetry and either processes the data locally or forwards it to an upstream server. The web presentment of the customer information is also a key requirement, which should be available from any type of browser-enabled computers.

3.5 Worker Safety

Staff location and state can be monitored in near-real-time, and assistance can be dispatched as required using GPS information. There are three approaches to using GPS. Coordinates can be captured in the field on work order open and maintained throughout the work order lifecycle, implying transactional communications between a GPS-enabled PC Tablet and a workforce management system. Also, field worker safety can be enhanced by enforcing field business processes and workflow to ensure safe protocols are observed and followed thru the mobile presentment of forms and instructions.

The second approach to using GPS is incorporating the notion of a GPS-enabled wearable device onto a utility workers tool belt or parts of their garment. This is effective in situation where workers are working alone or in remote areas distant from basic emergency services or regular communication infrastructure. This solution is termed Lone Worker.

The third approach to using GPS is to embed its capability within utility trucks, i.e.(Automated Vehicle Locator (AVL). This solution provides back office employees visibility and a breadcrumb trail of all vehicles in the fleet as they are dispatched on work orders.

3.6 Asset Security

Utility generation, transmission and distribution sites have been targeted in the past for trespassing, vandalism, sabotage and copper theft. Based on threat risk assessments, various sites may already be equipped with Closed Circuit Television (CCTV) and intrusion detection systems to communicate alarms and images to central command for incident response. Many other physical security services are available such as IP cameras, perimeter and motion sensors, public address and voice evacuation systems, alarm monitoring and intruder alarm, access control and time attendance, facial recognition and biometric systems, audio video intercom, under vehicle surveillance and parking control and management. The need for improved security is ever increasing and a robust communications infrastructure is required to support more sophisticated requirements.

CCTV images can be viewed or stored locally or remotely. For remote management, the transmission of large files across a wide area network is necessary, with the possibility of moving stored image files across different sites. A typical CCTV camera with resolution of 640x480 pixels and 10 frames per second (10 frame/s) in MJPEG mode requires about 3 Mb/s bandwidth. IP audio communications require a network that provides minimal latency for voice packets, less than 90 Ms. Any security sensor data traffic should have high priority over non-critical data so that a converged communications infrastructure can delineate between traffic classes and route appropriately. Encryption is a must, redundancy and survivability an important criteria.

From a communication systems and network perspective, the architecture needs to support these business objectives that have, in some cases vastly different or competing informational requirements, in a holistic fashion. The vision should be to collapse existing independent and specialized networks onto a common integrated and converged network infrastructure that can support business and operations to the greatest extent possible, with cost-effective results.

3.7 Information Systems

The application capabilities needed to support Smart Energy can be grouped by functionalities requiring communications infrastructure. They can be characterized by a set of common attributes that will assist in identifying and selecting the most appropriate network characteristics to meet the performance and response time requirements. The attributes are:

- Delay [Maximum, Jitter]
- Bit Rate (Bandwidth) [Data size, Frequency, Minimum, Maximum]
- Reliability [Outage, Loss %]
- Link Connectivity [Point-to-point, Point-to-multipoint, Multipoint-to-multipoint]
- Security [Accountability, Assurance, Availability, Confidentiality, Data integrity]

Application categories encompassing these attributes can be structured as follows:

  - Latency-critical
  - Latency-urgent
  - high data volume
  - low data volume

The application space for Smart Grid and Smart Meter includes over 100 functions, too many to list here (Reference: NIST PAP-01 Smart Grid Application Requirements, app_matrix_pap.xls). However, suffice it to say that each of these application functions' communication attributes needs to be understood and documented. At this time, the National Institute of Standards and Technologies (NIST) has undertaken an analysis under the auspices of Priority Action Plan no.1 to address this need, with results expected mid-2010.

Information systems (IS) software packages containing Smart Grid and Smart Meter application functionalities are developed by specialized industry vendors. These systems are classified as Grid Management systems and are identified under the following names:

- Outage Management System - OMS (Transmission and/or Distribution)
- Energy Management System – EMS (Transmission)
- Distribution Management System – DMS (Distribution)

IS supporting Customer Enablement applications are many and varied. For utilities in general, these packages require customization to meet unique requirements. They are known as:

- Customer Information Systems
- Customer Relationship Management (CRM) Systems
- Customer Facing Solutions (Web portals, messaging / mobile device platforms)

IS supporting Worker Safety applications are classified as Infrastructure Management systems and can include the following:

- Workforce Management Systems
- Work Scheduling System
- Mobile Dispatch System
- AVL System
- Lone Worker System

Underpinning these applications are GIS and Asset Management Systems (AMS).

IS supporting Asset Security are provided by specialized security vendors and are known as Physical or Cyber Security systems.

Ultimately, the informational elements related to communications and controls described in section 3.6 are used by the Information Systems mentioned in this section. An end-to-end network view that satisfies the necessary communication attributes of the application functionality, from the event sources to their eventual application level destination, is required to effectively engineer the best available primary or redundant communication routes.

3.8 Technology Infrastructure

The communications technology infrastructure requirements for the utility industry are probably one of the most stringent across all sectors. Given the criticality of electricity to society, homes and businesses, having a pulse on what is happening in the field and the home is absolutely essential. This implies very high availability and redundancy, with the objective of maintaining continuous uptime (99.999% or higher). The challenge of this requirement is further enhanced by the environmental and geographical factors associated with maintaining generation, transmission and distribution networks. Most common communications infrastructure is intended to serve populated areas; be it urban or rural. Utility infrastructure is generally deployed a distance away from the population base and hence, specialized or custom builds extending out from service provider central offices or built directly by the utility itself is necessary. This places pressure on capital expenditures and constrains the type of networks that can be deployed in certain pockets of the network topology.

Furthermore, the Intelligent End Devices, sensors, nodes, computers, cameras, phones, etc deployed to service each of the six business objectives described in section 3.3, 3.4, 3.5 and 3.6 significantly influences the type of network infrastructure required to support them. Factors affecting these decisions include:

- Mobility
- Location
- Security
- Availability
- Extreme environments

All utilities have unique communication network profiles dictated by their history, geographical footprint, and physical factors such as relief, elevation, foliage, geology. In addition, business strategies have also shaped what facilities have been built, bought or leased from third-party providers. Because of these considerations, generalities and assumptions on what is the 'best' network architecture should not be assumed. Suffice it to say that a network satisfying a utility's Smart Energy strategy most likely uses the following network elements:

- Wireless infrastructure
    - For IEDs, mobile workers, smart meters, remote sites, remote workers, sites with no embedded wireline infrastructure
- Wireline infrastructure
    - For high-speed backbone, digital broadband and analog access to generation, transmission or distribution centers where available and cost-effective
    - For enabling high-availability and redundancy in core network segments or access to data and operations centers

Part III of this White Paper will explore the types, characteristics and services of wireless and wireline networks; propose those that best meet the Smart Energy communication attributes for application level functions; discuss state of standards pertaining to these networks and submit a few network strategies for certain communication network profiles that may be applicable to utilities.

4. PART III

4.1 Communications Networks for Smart Energy

Content development in-progress

- Given that the Smart Grid will not only be a system of systems, but also a network of information networks, a thorough analysis of network and communications requirements for each subnetwork is needed. This analysis should differentiate among the requirements pertinent to different Smart Grid applications, actors, and domains.
- For Smart Grid applications that have specific quality-of-service requirements (such as minimum access delay, maximum packet loss or minimum bandwidth constraints), other technologies, such as Multi Protocol Label Switching (MPLS), can be used for the provisioning of dedicated resources.
- Encourage the use of IPv6 for new systems to be developed and deployed. IPv6 was specifically developed to solve the address space issue and to provide enhancements for the IP network.
- Given the heterogeneity and the large number of devices and systems that will be interconnected within the Smart Grid, multiple IP protocol suites may be needed to satisfy a wide range of network requirements. In addition, protocols and guidelines must be developed for the initiation of Smart Grid applications and the establishment and management of Smart Grid connections, in addition to the packetization of Smart Grid application-specific data traffic over IP

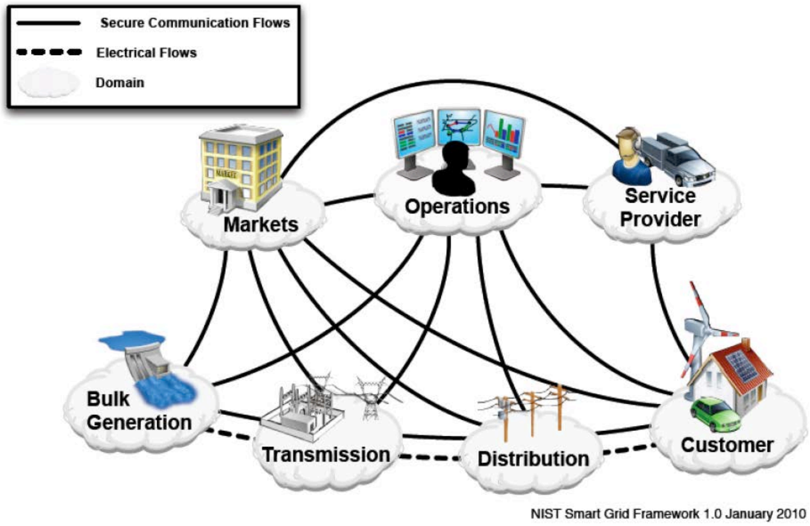
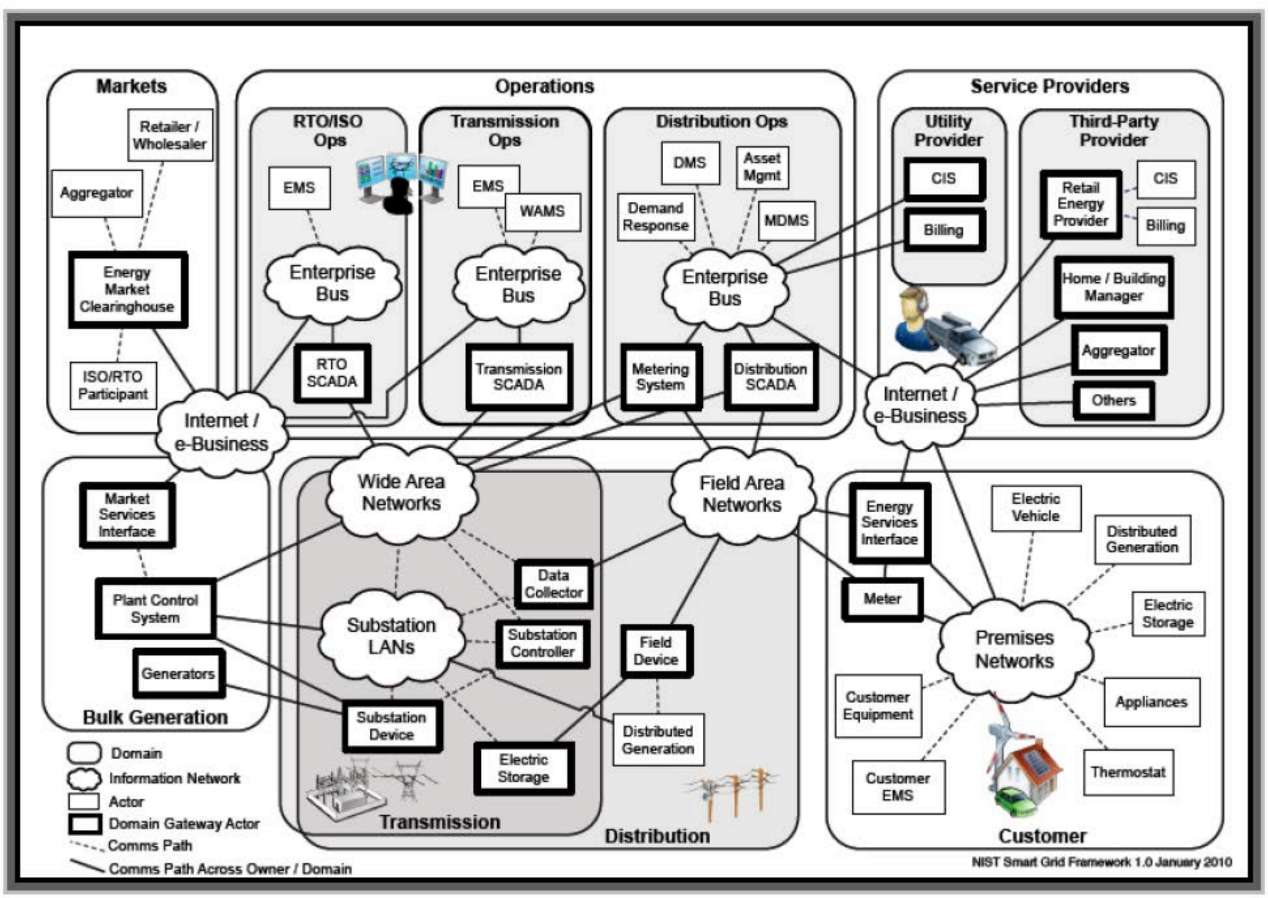


Figure 3-2. **Conceptual Reference Diagram for Smart Grid Information Networks.**



4.2 Types of Networks

Wireline

- A
- B
- C

Wireless

- D
- E
- F

4.3 Standards

Content development in-progress

Network Standards

Networks	Core (Wired)	Core (Wireless)	Emerging (Wired)	Emerging (Wireless)
Internet	IETF RFC 2460 (IPv6); IETF RFC 791 (IPv4); ICMP; IPSec	IETF RFC 2460 (IPv6); IETF RFC 791 (IPv4); ICMP; IPSec		
Substation LANs	Ethernet (IEEE 802.3); Serial communications (SCSM)	RF – 800/900 Mhz WPAN (IEEE 802.15.4)		WiMax (IEEE 802.16)
Home/ Commercial/ Industrial Premises Networks (HAN, WPAN)	Ethernet (IEEE 802.3); DOCSIS 3.0;	WiFi (IEEE 802.11a, b, g, n) WPAN (IEEE 802.15.4)	G.Hn HomePNA	WPAN Mesh (IEEE 802.15.5) ZigBee Smart Energy 2.0 HomePlug GP (IEEE 1901) Z-Wave mesh (900Mhz)
Field Area Networks (AMI)	N/A	WPAN (IEEE 802.15.4)		WPAN Mesh (IEEE 802.15.5) IETF 6LoWPAN
Metro Area Networks (MAN)	Ethernet (IEEE 802.3); SONET;	WiMax (IEEE 802.16)		
Wide Area Networks (WAN)	IETF MPLS, IPVPN; PON (Passive Optical Fiber); BPL (Power Line Comm); IP over DVB; PSTN (TDM / SS7) Optical Ethernet (IEEE 802.3);	3G: CDMA2000; UMTS/W-CDMA; GSM EDGE; HSPA; HSPA+ Satellite: IPoS v2.0 BGAN (INMARSAT) IMPACT (Telesat) - NA		4G: LTE

Communication Network Standards

Networks	Core	Emerging
Internet (Transport)	TCP; UDP; RSVP;	NIST PAP-01 to define
Substation LANs	DNP3; MMS/UCA 2.0 (Utility Comms Arch); IEC 60870-6 / TASE.2: ICCP IEC 61850-6; GOOSE (P-to-P)	
Home/ Commercial/ Industrial Premises Networks **(HAN, WPAN)**	BACnet (ANSI/ASHRAE 135-2008/ISO 16484-5); LonWorks 2.0 (ISO/IEC 14908-1) Modbus RTU; DALI (Lighting protocol)	Obix (OASIS std)
Field Area Networks (AMI)	ANSI C12.22 (declining)	
Metro Area Networks (MAN)	ANSI C12.22 (declining) IEC 60870-6 / TASE.2: ICCP	
Wide Area Networks **(WAN)**	ANSI C12.22 (declining) IEC 60870-6 / TASE.2: ICCP	

4.4 Issues

- Each AMI communication vendor develops a unique interface card for each meter (in close cooperation with the meter vendor). This one-at-a-time, custom approach presents a high barrier of entry for new meter vendors. That's good for meter vendors perhaps, but not for the utility customers. Put bluntly, utilities will not see lower meter prices until there is more competition. The UtilityAMI organization has noted this as a high priority with significant value to utilities.

4.5 Strategies

Content development in-progress

4.6 Roadmaps

Content development in-progress