EPRI | ELECTRIC POWER RESEARCH INSTITUTE

Smart Grid Roadmap Guidebook

2012 TECHNICAL REPORT

Smart Grid Roadmap Guidebook

EPRI Project Manager
D. Von Dollen

ELECTRIC POWER RESEARCH INSTITUTE

3420 Hillview Avenue
Palo Alto, CA 94304-1338
USA

PO Box 10412
Palo Alto, CA 94303-0813
USA

800.313.3774
650.855.2121

askepri@epri.com

www.epri.com

1025470
Final Report, July 2012

DISCLAIMER OF WARRANTIES AND LIMITATION OF LIABILITIES

THE FOLLOWING ORGANIZATION, UNDER CONTRACT TO EPRI, PREPARED THIS REPORT:

EnerNex LLC

NOTE

For further information about EPRI, call the EPRI Customer Assistance Center at 800.313.3774 or e-mail askepri@epri.com.

Acknowledgments

The following organization, under contract to the Electric Power Research Institute (EPRI), prepared this report:

EnerNex LLC
620 Mabry Hood Road Suite 300
Knoxville, TN 37932

Principal Investigators
R. Farquharson
B. Russ
E. Gunther

This report describes research sponsored by EPRI.

EPRI acknowledges the contribution of the following:

D. Houseman
J. Bucciero
P. De Martini
K. Stefferud
J. Laundergan
G. Davis

The authors of this technical report also wish to gratefully acknowledge the participation of the following (in alphabetical order):

California Energy Commission (PIER Program)
California ISO
Duke Energy
First Energy
Salt River Project
Southern Company
Tennessee Valley Authority

This publication is a corporate document that should be cited in the literature in the following manner:

Smart Grid Roadmap Guidebook. EPRI, Palo Alto, CA: 2012. 1025470.

Product Description

This technical report summarizes the results of the Smart Grid roadmaps developed by the Electric Power Research Institute (EPRI) from 2007 to 2011. The report's major themes are the lessons learned and the methodologies used to develop the roadmaps. Also included are a summary of the roadmaps, key points from follow-up interviews, distilled technology recommendations from the roadmaps, the purpose and benefit of developing a roadmap, the role of standards, and an updated version of the Communications Technology Assessment.

Background

EPRI's goal with roadmaps and the Smart Grid Roadmap Methodology is to help a company transition from understanding what the Smart Grid is generically to achieving the most effective timing and adoption of Smart Grid technology in a way that uniquely maximizes the benefits and minimizes risks for the utility or independent system operator (ISO). The roadmap is essentially a technology portfolio optimization plan.

Objectives

It can be difficult to justify taking the time to develop a strategy and plan technology investments for the short, medium, and long term. In addition, getting engagement, consensus, and organizational support for a plan across different departments and businesses—from the senior to operational levels—can be extremely difficult. However, for any plan to succeed, cross-functional support is very important. Similarly, building a winning economic business case requires capturing the benefits accrued from a technology investment across the whole company.

In addition to the lessons learned and the methodologies used to develop the roadmaps, this report includes the benefits gained by several of the company's roadmap programs and the role of leadership in enabling that to happen.

Approach

The report was developed as a synthesis of the already developed roadmap documents and augmented by follow-up interviews with several of the companies as well as industry experts, including a former utility executive with a strong record of success in leading technology investments at a utility.

Results

The key outcomes of this report are the Smart Grid Roadmap Methodology (SGRM) and the lessons learned.

Applications, Value, and Use

The report is intended to serve as a useful reference for companies that have already developed a Smart Grid roadmap and may help to justify further effort to use and update the roadmap. In addition, the report is intended to explain the process used and the lessons learned to companies considering a roadmap effort with or without EPRI's assistance.

Keywords

Adoption
Applications
Architecture
Business case
Communications
Roadmaps
Security
Standards

EPRI Smart Grid Glossary of Terms

ACRONYM	DESCRIPTION
AB	Assembly bill. A state law passed by the legislature.
AGC	Automatic generation control
AHAM	Association of Home Appliance Manufacturers. A trade association based in the U.S. consisting of the home appliance manufacturers.
AMI	Advanced metering infrastructure
ANSI	American National Standards Institute
ASAP-SG	Advanced Security Acceleration Project for Smart Grid. An EPRI project focused on security for the smart grid.
ASHRAE	American Society of Heating, Refrigeration and Air Conditioning Engineers. An international organization with the "mission of advancing heating, ventilation, air conditioning and refrigeration to serve humanity and promote a sustainable world through research, standards writing, publishing and continuing education." (Source: http://www.ashrae.org/aboutus.)
ADR	Automated demand response. Demand response enabled through automation and communications with customer end-use equipment.
ARRA	American Recovery and Reinvestment Act. Legislation passed by the U.S. Congress in 2009 in support of retaining and creating jobs, economic activity and investment in long-term growth.
AVC	Automatic Voltage Regulator
CAES	Compressed air energy storage
CAIDI	Customer Average Interruption Duration Index. A reliability index commonly used in the electric power industry indicating the average outage duration experienced by customers, or average restoration time.
CAISO	California Independent System Operator. The regional transmission and market system operator of the state of California.

ACRONYM	DESCRIPTION
CARB	California Air Resources Board. An organization with the objective "to promote and protect public health, welfare and ecological resources through the effective and efficient reduction of air pollutants while recognizing and considering the effects on the economy of the state." (Source: http://www.arb.ca.gov/html/missio
CBM	Condition based maintenance. An application of sensors, monitoring systems, and processes to support maintenance of equipment in service as the need arises.
Energy Commission	California Energy Commission
CHP	Combined heat and power. Refers to a system in which heat and electricity are generated simultaneously, with the thermal energy used for end-use requirements such as water heating, process heating, or cooling.
CIGRE	CIGRE (International Council on Large Electric Systems) is a permanent non-governmental and non-profit-making International Association based in France with the primary objective to facilitate and develop the exchange of engineering knowledge and information, between engineering personnel and technical specialists in all countries as regards generation and high voltage transmission of electricity.
CIM	Common information model. A standard developed in the electric power industry that has been officially adopted by the IEC and is aimed at enabling application software to exchange information about the configuration and status of an electrical network.
CIP	Critical Infrastructure Protection
CIPS	Critical Infrastructure Protection Standards (CIPS). A set of NERC guidelines for preparedness and response to security concerns involving critical infrastructure of a region.
CIS	Coordinated information system
CMMS	Computerized Maintenance Management System
CPUC	California Public Utilities Commission
CSI	California Solar Initiative
CSWG	Cyber Security Working Group
CVR	Conservation Voltage Regulation.
DA	Distribution Automation

ACRONYM	DESCRIPTION
DAD	Distribution Availability Database
DER	Distributed energy resources. Electric energy sources that typically include distributed generation and storage and may be interconnected with the power system at transmission or distribution level voltages.
DFR	Digital Fault Recorder (or Design for Reliability)
DG	Distributed generation. Active energy sources such as a microturbine, diesel backup generator, or other standby generation that may be interconnected with the power system at transmission or distribution level voltages.
DGA	Dissolved gas analysis
DMS	Distribution management system. A control system to manage distribution power operations through a combination of communications with field equipment and hierarchical control algorithms.
DNP/DNP3	Distributed Network Protocol. A set of communication protocols developed to facilitate communications between data acquisition and control equipment. DNP is primarily used by utilities and between components in process automation systems.
DOE	U.S. Department of Energy
DR	Demand response. A dynamic change in electric load regarded as a valuable service to a system operator, such as customer response to prices, notifications, controls, or other signals designed to coordinate changes in electric power demand.
DSA	Dynamic Stability Assessment
DSM	Demand Side Management
DTRC	Dynamic Thermal Circuit Rating
EE	Energy Efficiency
EHV	Extremely High Voltage
EIA	Energy Information Administration
EMMS	Enterprise Model Management System
EMS	Energy management systems. 1) A centralized communication and control system for the management of power delivery operations or 2) a system for monitoring and controlling end-use equipment within a building.
EPA	Environmental Protection Administration

ACRONYM	DESCRIPTION
EPDC	Enterprise Phasor Data Collector
EPRI	Electric Power Research Institute
ES	Energy Storage
ETO	Emitter turn-off thyristor
EV	Electric Vehicle
EVSE	Smart Electric Vehicle Supply Equipment
FACTS	Flexible AC transmission systems. A power electronic based system and other static equipment that provide control of one or more AC transmission system parameters to enhance controllability and increase power transfer capability.
FERC	Federal Energy Regulatory Commission
GAD	Generation Availability Database
GHG	Greenhouse gas. A gas when in high concentrations in the atmosphere contributes to the greenhouse effect and global warming.
GPS	Global Positioning System
GTO	Gate turn-off thyristor. A type of thyristor with fully controllable switches which can be turned on and off by the GATE lead.
GW	Gigawatt
GWh	Gigawatt-hour
HAN	Home area network
HVAC	Heating, Ventilating, and Air Conditioning equipment
HVDC	High voltage direct current
IEC	The International Electrotechnical Commission. This organization prepares and publishes international standards for all electrical, electronic and related technologies.
IED	Intelligent electronic devices
IEEE	Institute of Electrical and Electronics Engineers. A professional engineering association for electrical, electronic, and other engineers.
IEPR	Integrated Energy Policy Report. A 2007 report that provides an integrated assessment of the major energy trends and issues facing the California's electricity, natural gas, and transportation fuel sectors, and provides guidance on state energy policy.

ACRONYM	DESCRIPTION
ICCP	Inter-Control Center Communication Protocol
ICT	Information Communications Technology
IDS/IPS	Intrusion Detection System/Intrusion Prevention System
IntelliGrid Methodology	EPRI IntelliGrid Methodology – has the objective of assisting power system companies and staff in implementing the ideas of the IntelliGrid Architecture documents. There is a strong focus on principles related to architecture development, project planning, requirements definition and technology capability / selection. Cyber security best practices are also highlighted.
IOU	Investor-owned utility
IP	Internet protocol
IPv6	Internet Protocol Version 6
IRP	Integrated Resource Plan
IS	Interconnection system
ISO	Independent System Operator. A regional system operator responsible for the reliable operation of the bulk electric transmission system in its FERC-approved geographic territory.
ISO/RTO Council	Council composed of 10 independent system operators and regional transmission organizations
kW	Kilowatt. A unit of measurement of power equal to 1000 watts
kWh	Kilowatt hour
LCM	Life Cycle Management
LED	Light-emitting diode
LSE	Load serving entity
LVRT	Low voltage ride-thorough technology
MAIFI	Momentary average interruption frequency index
MPU	Microprocessor Unit
MRTU	Market Redesign Technology Upgrade
MVA	Megavolt ampere
MVAR	Megawatt-VAR
MW	Megawatt
MWh	Megawatt-hour

ACRONYM	DESCRIPTION
NaS	Sodium sulfur battery
NASPI	North American Synchro Phasor Initiative
NERC	North American Electric Reliability Corporation
NGV	Natural gas vehicle. An automobile, truck, or other transport vehicle fueled by natural gas.
NIST	National Institute of Standards and Technology. A federal institute with the objective of promoting "U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life." (Source: http://www.nist.gov/public_affairs/nist_missio
NREL	National Renewable Energy Laboratory. A national laboratory with research and technology development areas that "span from understanding renewable resources for energy, to the conversion of these resources to renewable electricity and fuels, and ultimately to the use of renewable electricity and fuels in homes, commercial buildings, and vehicles." (Source: http://www.nrel.gov/ove
OEM	Original equipment manufacturer
OMS	Outage Management System
OPC/UA	OPC Unified Architecture. The next generation of the OPC standard defined by a layered set of specifications providing a cross-platform framework for accessing real time and historical data.
OpenSG	Open Smart Grid Users Group
OPF	Optimum power flow
OSHA	Occupational Safety and Health Administration
OSI	Open Systems Interconnection. An initiative that developed the OSI Basic Reference Model.
OSI BRM	Open Systems Interconnection Basic Reference Model. Also known as the OSI seven layer model, this is an abstract description for communications and computer network protocol design. It is comprised of seven layers with each layer representing functions providing services to the layer above and receiving services from the layer below.
PAP	NIST Priority Action Plan
PAS	IEC publicly available specification
PCT	Programmable communicating thermostat

ACRONYM	DESCRIPTION
PDC	Phasor data concentrators
PEV	Plug-in electric vehicle
PIER	Public Interest Energy Research
PJM	Pennsylvania Jersey Maryland ISO
PMU	Phasor measurement unit
PQ_	Power quality. A broad term used to describe the measurement of electrical power performance. Variations in voltage, frequency, wave shape (harmonics) and other aspects of power may make the power delivered to equipment less than ideal, creating compatibility problems. Electronic equipment may be especially sensitive to power quality problems.
PSO	Power System Operations
PSS	Power System Stabilizer
PV	Photovoltaic
RBAC	Role-based access control
REC	Renewable energy credit
RD&D	Research, development, and demonstration
RFID	Radio frequency identification
RMR	Reliability must run. A specially designated resource under contract to provide reliability services in a regional electric power system.
ROW	Right of Way
RPS	Renewables portfolio standard
RTU	Remote Terminal Unit
SAIDI	System average interruption duration index
SAIFI	System average interruption frequency index
SCADA	Supervisory control and data acquisition
SEPv2	Smart Energy Profile 2.0, a standard for communications and information exchange extending to and within customer premises for AMI/HAN.
SGAC	Smart Grid Architecture Committee. A NIST-organized committee responsible for developing a conceptual reference model for the smart grid and listing necessary standards for implementing the smart grid vision.

ACRONYM	DESCRIPTION
SGIP	Smart Grid Interoperability Panel. A broad group of smart grid stakeholders organized by NIST to provide an open process for participation in the coordination, revision, acceleration and harmonization of smart grid standards. Members of the SGIP develop and review use cases, identify requirements, and propose action plans.
SGRM	Smart Grid Roadmap Methodology - has the objective of helping companies address applicable business objectives and mitigate associated drivers by succeeding in the effective adoption and implementation of technologies, applications and standards. Five key steps have been adopted for the SGRM; Vision, Requirements, Assessment, Planning and Roadmap Implementation. Within each step there are three or four recommended tasks. In summary the SGRM will result in a roadmap that is a technology portfolio optimization plan.
SIS	System impact study
SOA	Service oriented architecture
SPS	Special protection systems
STATCOM	Static Synchronous Compensator
SVC	Static var compensator. An electrical device providing fast-acting reactive power compensation on high voltage electric transmission networks as part of a flexible AC transmission system.
TAD	Transmission Availability Database
T&D	Transmission and distribution. The power delivery system or business area.
TC	Technical committee
TCP	Transmission control protocol
TIMM	Transmission Infrastructure Management & Monitoring
TLM	Transmission line matrix
TOGAF	The Open Group Architecture Framework
TVA	Tennessee Valley Authority
TVPPA	Tennessee Valley Public Power Authority

ACRONYM	DESCRIPTION
VAR	Volt-ampere reactive. A unit of reactive power. For a two-wire circuit, the product of the voltage times the current times the sine of the angular phase difference by which the voltage leads or lags the current. VARs and watts combine in a quadrature relationship to form volt-amperes.
VSA	Voltage Stability Assessment
V2G	Vehicle to Grid
V2H	Vehicle to Home
UHV	Ultra High Voltage
WAMACS	Wide area measurement and control system
WAMS	Wide area measurement system
WASA	Wide area situational awareness
WECC	Western Electricity Coordinating Council. A regional forum that promotes electric service reliability in the Western United States and Western Canada.
WG	Working group. A subgroup of a larger community that typically conducts technical work surrounding a given topic.
WIKI	Wiki are websites of interlinked web pages that facilitate easy creation and editing by groups using a web browser and a simplified markup language.
WMS	Work Management System
XML	Extensible Markup Language. A specification for creating custom markup languages to facilitate the sharing of structured data across disparate information systems over the Internet.

Executive Summary

This report has been developed with the intent of documenting the lessons learned and methods used by EPRI in the development of eight Smart Grid roadmaps for seven different companies. The genesis for EPRI's involvement with Smart Grid roadmaps was EPRI's starting of the Consortium for the Electric Infrastructure to support a Digital Society (CEIDS) which was later renamed the IntelliGrid program within EPRI. CEIDS undertook an ambitious project called "the Integrated Electricity and Communications System Architecture" (IECSA). The process used to develop IECSA was found to be applicable to utilities that were developing smart grid implementation strategies. It became clear that the Smart Grid concept was not a "one size fits all" situation. While the high level vision was commonly accepted, the specifics of the vision were different from country to country, state to state and company to company depending upon internal and external drivers. Drivers could be policy drivers or business drivers. It also became clear that the Smart Grid would be created through an evolutionary process that could take years or decades to fully realize. Therefore, each company would:

- Have a unique vision for their Smart Grid
- Have a unique strategy and evolutionary pathway for creating their Smart Grid
- Create their Smart Grid at a pace that would meet their needs as well as the needs to their customers, regulators and legislators.

Therefore it became clear that EPRI needed to develop a new methodology that was flexible yet effective at helping them chose, plan and ultimately deploy technology investments effectively. This is the objective of EPRI's Smart Grid Roadmap efforts.

Smart Grid Roadmap Methodology (SGRM)

The goal of the SGRM is to help companies transition from understanding what the Smart Grid is generically to achieving the most effective timing and adoption of Smart Grid technology in a way that uniquely maximizes the benefits and minimizes risks for the utility or independent system operator (ISO).

Each of the eight roadmaps referenced in this Guidebook were different for a variety of reasons including different business objectives, policy and regulatory requirements, technology & communications infrastructures and objectives for the Roadmaps. Nevertheless the roadmap developments had a lot in common in terms of the overall process.

As the EPRI team implemented the Roadmaps, five key steps have been adopted for the SGRM: Vision, Requirements, Assessment, Planning and Roadmap Implementation. Within each step there are three or four recommended tasks however, depending on the Roadmap objectives, some tasks are optional. Drilling down further, each task is addressed by one or more possible task methodologies. The optimal methodology is selected depending on the client's needs. For example, within the Assessment step there is a task called "Select Focus Technologies". For some Roadmaps the method used for selection involved scoring and ranking the technology by impact and effort/risk. In other cases a more detailed scoring method was used. The SGRM is shown in Figure 1.

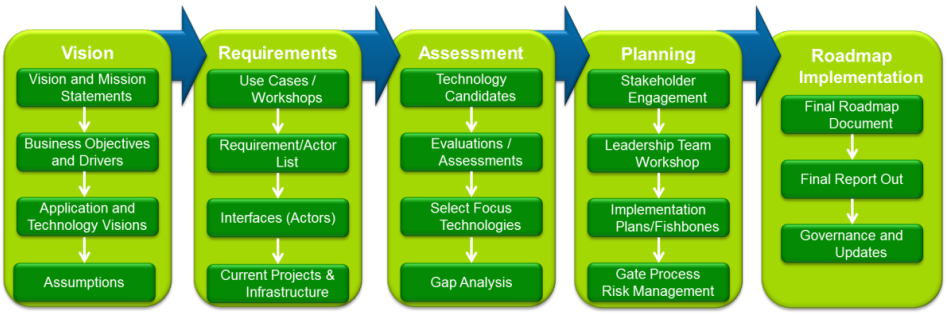


Figure 1
Smart Grid Roadmap Methodology (SGRM)

Benefits Realized

Before we get to the other primary topic of lessons learned, it is important to summarize the benefits that have been realized by the utilities that implemented the SGRM. Not all benefits accrued to all utilities in the same way as each company and each Roadmap is different. The following is a list of benefits realized by at least one company that we worked with:

- Increased collaboration and cooperation between departments
- "Future-proofing" of technology investments – in other words, the Roadmap identified principles and interoperability standards that help protect the value of investments made and minimize the risk of early obsolescence.
- Utility now has greater understanding and approaches for mitigation of risks associated with technology
- Technology life-cycle management can be enhanced
- Following the recommended governance model, led to strong C-level sponsorship and the development of a cross functional Smart Grid leadership team for the company.
- Helped to provide organizational direction and cross-cutting cooperation on the Smart Grid efforts
- Aided in optimizing the planning of technology investments
- Lead to the assignment of a second senior staff member in a lab management capacity to provide greater support for new Smart Grid technology projects and investments
- Many of the recommended initiatives are moving forward within their departments
- The original Roadmap team at the utility has used the same SGRM methods to develop requirements for the new Advanced Metering Infrastructure – Meter Data Management Systems (AMI-MDMS).
- The Roadmap program provided renewed impetus and vision and a way of going forward with a model for what the future might look like

- Out of the original nine technology recommendations, the utility is moving forward to seven programs now and has a project underway to look at the ninth

- Provided a solid starting point for the utility's American Recovery and Reinvestment Act (ARRA) proposals and grant applications

- Enables the utility to discover the potential future impacts of technological change such as Distributed Energy Resource (DER), Electric Vehicles (EV)

- Supports the long term planning needed to achieve overall systems and data integration

- Can be a source of input for regulatory applications and general rate case documents

Vision Communicated

The ability of an enterprise to summarize and communicate the essence of their vision can have a material impact on their ability to achieve that vision. Creating an enterprise wide consensus and momentum is difficult to achieve. As stated above, the goal of the SGRM is to help companies achieve the most effective timing and adoption of Smart Grid technology in a way that uniquely maximizes the benefits and minimizes risks for the utility or Independent System Operator (ISO). With this objective in mind, the graphic in Figure 2 highlights the important role of the other aspects of the organization in achieving the technology adoption objectives namely: the people, the organization and the processes.

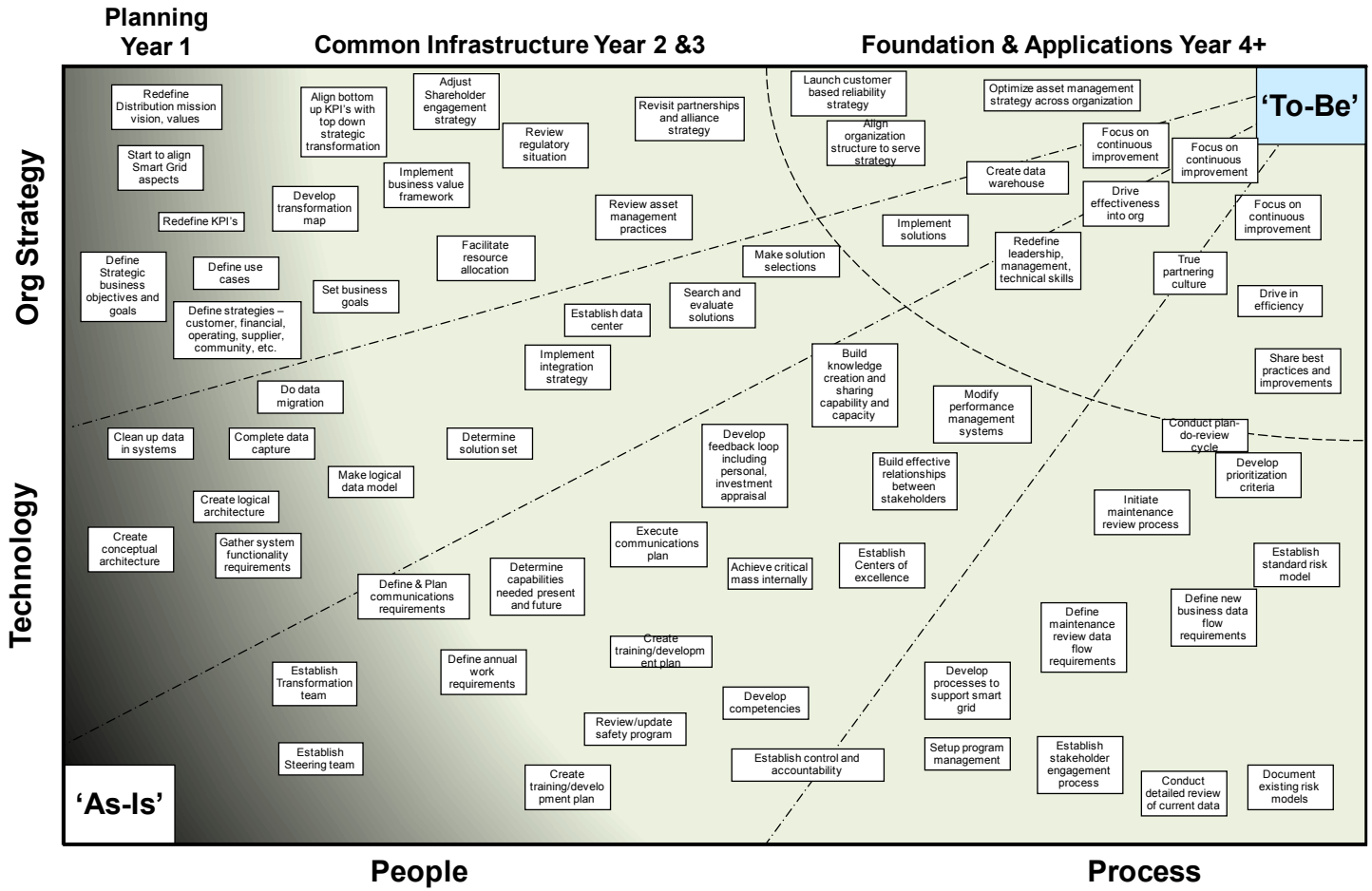


Figure 2
Achieving the Smart Grid Vision

Lessons Learned

As mentioned above, much has been learned. Three over-arching lessons are:

- Leadership and governance is key to success
- The journey (of developing the Roadmap) is at least as valuable as the end product
- The important role of the other aspects of the organization in achieving the technology adoption objectives namely: the people, the organization and the processes. See Figure 2 above.

There have been enough roadmap projects that some common themes have emerged. Some roadmap projects have been more successful than others both in the development of the roadmap and the implementation than others. These lessons are summarized below.

Management

The importance of governance, which we define as engaged oversight, has been confirmed with every roadmap project. The governance should involve both the executive level and the management levels. The value of the involvement of executive or senior management in the roadmap process cannot be over stated. The highest levels of the company should all be involved in establishing the company's technology adoption strategy followed by the initiation and oversight of the roadmap project through to completion. This would ideally include the Board of Directors, and Chief Executive Officer, the Chief Financial Officer, the Chief Engineer, the Chief Information Officer, the applicable Executive VPs and Senior VPs or their equivalents. For the design and construction of a major power plant, those executives would be keenly aware of the status of the project and the cost/benefit summaries, status of regulatory and permitting approval. Grid modernization involves the same magnitude of expenditure and requires the same level of oversight and approval. Without this buy-in, the roadmap report will probably end up in the company library with the other consultant reports that were never implemented.

Steering Committee

In terms of governance, the management level must be engaged as well. Each and every successful project has had a steering committee, chaired by a company executive or senior staff member who was

responsible for the outcome of the project. They provided guidance to the project, reviewed the status of the project and helped keep the whole team involved in the project, so that it stayed on track and with the best possible results. Without the steering committee, projects tend to run longer, have lower attendance at workshops, go over budget and return results that are inferior. Additionally parts of the organization have the ability to say "We were not involved and that is not what we want". Without a steering committee the project manager in the utility is climbing steep hill with a heavy load.

Cross-Functional Teams

Many of the utilities that participated in the Roadmap process began to immediately realize tangible benefits in having active cross-functional teams working together to solve common utility challenges. However, to be most effective, this 'silo-busting' objective must almost always require the critical requirement for organizational buy-in and leadership from top management across all departments.

Responsibility

To be successful, roadmap projects need to touch most of the organization. In a typical utility the roadmap touches more than 70 percent of the jobs. Creating a project responsibility matrix and getting buy in from the whole organization is important. Typically a responsibility matrix includes four roles:

1. Responsible – no matter what happens, "the buck stops here." Typically this is the role of the senior executive leading the steering committee and the steering committee.
2. Authorized – these are the people who day-to-day are doing the work.
3. Consulted – these are the people who are expected to be in the meetings, providing input, reviewing documents and commenting. This is an active role in the project and people are expected to make time for this project.
4. Informed – people who will be impacted by the result and so they should know what is going on. However, they are not actively involved in the activity.

In most cases this kind of a matrix lets people know the expectations the project has and how active they are expected to be. Doing this up front and making sure that the people in the roles are keep fully informed means at the end of the project there should be no "Wait, wait, I did not know that was happening" from the organization.

Regulatory

The regulator is a key stakeholder in the roadmap process. They need to be informed and even consulted on what they see as key capabilities that the organization should have as it moves forward.

Review and Updates

A roadmap is never really done, if it is, then it is just a report. Setting a regular review of the roadmap and updating on a regular basis is fundamental to keeping the organization on track. Quarterly reviews on technology changes, regulatory changes, and other items and making updates to the roadmap are important. However a major refresh effort two or three years down the road is usually required.

Benefits Are Not Magic

You don't have a magic wand to make benefits appear on the first day of implementation; in fact benefits typically lag deployment by about a year. Outputs from the roadmap project should be realistic about the lag in benefits. During any major deployment, no one is going to lose a job, in fact in most cases the payroll (including temps, contractors and consultants will rise sharply).

Consumer Involvement

As some prominent utilities found out through negative press coverage and others are also finding out, consumers, both large and small have clear ideas of what they want the grid to be able to do for them. Getting this input early in the process can help calibrate how the public feels about the organization and what needs to be strengthened as part of the modernization effort.

Common Internal and External Drivers:

There are a number of common drivers that underlie the need to modernize the grid. They are:

1. availability / reliability
2. increasing failures or decreasing performance linked to aging assets
3. changing load profiles and consumption
4. demographic changes
5. regulatory compliance
6. emergence of new technologies including DER and EV
7. operational efficiency

8. asset utilization
9. fiscal responsibility
10. real-time situational awareness for both transmission and distribution
11. cyber security
12. workforce readiness
13. intuitive interfaces / simpler training needs
14. comprehensive cost recovery metrics

Not every utility has all of these drivers at the top level. The prioritization of these drivers changes from utility to utility. It is critical that all of the key drivers get reviewed and an agreed to prioritization happens. Spending 70% of the roadmap effort on the 14th most important driver leads to a roadmap that will not be implemented; this is where the steering committee has to make hard choices about priorities.

Technology is a Big Issue

Regardless of the background of the team, the amount of technology involved in a roadmap is tremendous, typically an order of magnitude more than the team thinks when they start the project. It is not unusual to look at more than 200 technology categories over the development of the roadmap.

Technology is a trap for most teams, they have strong technical people and technology is easier to deal with that the messy regulatory issues. Technology should be discussed at the general level (e.g. HAN) until the final stages of the roadmap. Getting too technical and too specific too early will lead to compromises in other areas of the roadmap that the team is not even aware they are making.

If you are not at the point where you are working on the very bottom row of Figure 3 below, you should not be having technology discussions, that go beyond the "we need a two way meter that…".

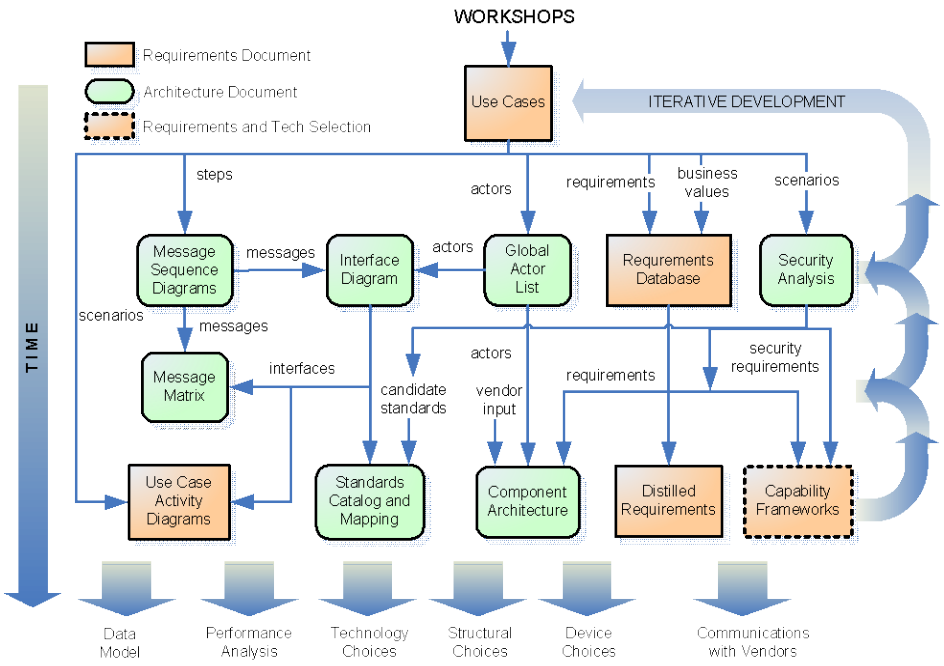


Figure 3
The IntelliGrid Architecture Methodology

Current State Knowledge

Knowing the current state of the organization, its equipment and processes is very important to the use case workshops and how the roadmap is going to impact the organization.

It cannot be stated strongly enough, you need the experts on how it works today in the workshops. That knowledge is critical to determine what the impacts of the changes are and whether they will fit.

Walking into the workshops with detailed knowledge of the current processes and the issues with those current processes is important. Similarly knowing what the issues are with the current equipment in the field is critical to the discussions. This includes root-cause analysis of those issues. Spending an hour debating why the System Average Interruption Duration Index (SAIDI) “is what it is” is not a productive discussion. Doing the homework before the meeting and having this information in hand is critical to the workshop. Ideally the “go to” person in the organization should start the workshop off with some facts about where the topic under discussion stands from a key metrics standpoint. Similarly having any regulatory mandates stated clearly up front also helps to frame the discussion.

In short know what the problems are, how big they are and how much it is costing. Creating a $1 billion dollar fix to a $20 million problem seldom gets the green light from either the regulators or senior management.

Communications Technology Assessment Matrix

Communication is a much bigger part of this project than most; not only communication to people about the project (which is not the theme of this discussion) but also the communications with the equipment in the grid and the people working on the grid.

The creation of a matrix that captures all of the requirements as the project progresses for communications and where the communications needs to happen will facilitate technology assessment later in the project. Some of the key communications areas that are common to a roadmap are:

1. Field and Enterprise Communications Infrastructure and Architecture
2. Customer Systems
3. Grid Operations and Control
4. Renewable and Distributed Energy Resources Integration
5. Grid Planning and Asset Efficiency
6. Workforce Effectiveness

When the technology assessment was done, the key evaluation criteria typically included:

1. Maturity
2. Self-description
3. Security
4. Scalability
5. Manageability
6. Standards
7. Openness
8. Users groups
9. Object modeling
10. Power industry reference implementations and support

For a project manager putting each of these criteria into the evaluation sheet ahead of time as categories is useful to make sure all the requirements are captured in workshops and discussion sessions.

Additional evaluation criteria also have emerged in the roadmaps and are found to be useful for communications:

1. Increase reliability
2. Cost
3. Security/safety compliance (risk mitigation, minimize/avoid negative public relations)
4. Risk of obsolescence
5. Regulatory concerns
6. Customer acceptance
7. System integration
8. Ease of interpreting information
9. Maturity
10. Capability
11. Work force requirements
12. Implementation
13. Training and support

System Integration is HUGE

Not only is it huge but it is a specialized topic. Don't try to wrestle it to the ground in the workshops or in the roadmap. Indication that system "A" needs this kind of information (e.g. Customer) from system "B" is the level that is productive. Anything deeper than that in any workshop or group discussion (unless it is the system integration team) will turn off much of the audience and slow the process down. Remember, save those discussions for when the project reaches the bottom row of the IntelliGrid Architecture Process diagram above.

Don't Just Add

Many teams talk about "additions to the technology, new IT systems, new communications systems, new…"

The problem is there are old systems out there too. The roadmap needs to talk about replacement and transition as well as additions. This can be a hard discussion, since no new system will work exactly like an old system and people are used to how the old system works.

Supporting Items

The roadmap by itself is not enough to succeed. Nor is a business case enough support to make the roadmap succeed in

implementation. There are several other items that need to happen, that the roadmap can be a catalyst for. They include:

1. Organization-wide integration policy
2. Organization-wide security policy
3. Organization-wide privacy policy
4. Asset-management policy

Training and Change Management

Regardless of the technologies chosen or the timelines developed or any other aspect of the roadmap, one item is constant across all of the roadmaps. Training of the existing workforce has to happen for the deployment to be successful and the organization has to change to meet the new technology half way.

It will be people that will make or break the success of the roadmap and its implementation!

Summary

The EPRI Smart Grid Roadmap process has been found to be an effective tool in assisting utilities to move forward in their grid modernization efforts. The Smart Grid vision that these Roadmaps embrace should link electric operations, communications, and automated control systems to create a highly automated, responsive, and resilient power delivery system that should both improve services and empower customers to make informed energy decisions. A Smart Grid with these characteristics would support a wide range of current and evolving energy policy goals, including increased penetration of renewable resources, reduced greenhouse gas emissions, increased energy efficiency, implementation of demand response, increased use of distributed energy resources, maintained and/or enhanced grid reliability, and advanced transportation electrification. Integrated systems introduce more complex cyber security issues, but support a wider range of system options that exhibit lower costs, greater price vs. feature flexibility, and ensure continued improvement in the security of power supply. Therefore, the Smart Grid should place an emphasis on greater protection from cyber security attacks and safeguard customer privacy and worker safety. The Roadmap process has also illuminated some of the challenges associated with Smart Grid development and deployment—such as maintaining and/or increasing reliability in the face of increased grid complexity and managing technologies.

Table of Contents

List of Figures

List of Tables

Section 1: Introduction

In 2000, the EPRI Board of Directors challenged EPRI to launch an Initiative aimed at envisioning and enabling the power delivery system of the future. In response, EPRI established the Consortium for the Electric Infrastructure to support a Digital Society (CEIDS). The future electric delivery system envisioned by CEIDS was a "Smart Grid" that merged monitoring, communications, distributed computing and information technology with the traditional electricity infrastructure to create a system that was more flexible, adaptable and robust. CEIDS launched an ambitious project entitled "the Integrated Electricity and Communications System Architecture" (IECSA) to:

- Flesh out the Smart Grid vision
- Create a high level architecture for the Intelligent Electric Devices (IEDs) and systems that would enable the smart grid
- Develop an initial set of requirements for the infrastructure
- Document the current standards and technology landscape
- Identify the key areas for research and development

Shortly after IECSA was completed in 2003, Southern California Edison approached EPRI about leveraging the work that had been done in IECSA to help them with the development of a specification for their Advanced Metering Infrastructure (AMI). We found that the methodology that was used to create IECSA could also be used by utilities that were planning, designing and implementing Smart Grid applications such as AMI. This methodology was ultimately published by the International Electrotechnical Commission (IEC) in 2008 as Publicly Available Specification 62559 - "IntelliGrid Methodology for Developing Requirements for Energy Systems."

It became clear that the Smart Grid concept was not a "one size fits all" situation. While the high level vision was commonly accepted, the specifics of the vision were different from country to country, state to state and company to company depending upon internal and external drivers. Drivers could be policy drivers or business drivers. It also became clear that the Smart Grid would be created through an evolutionary process that could take years or decades to fully realize. Therefore, each company would:

- Have a unique vision for their Smart Grid
- Have a unique evolutionary pathway for creating their Smart Grid

- Create their Smart Grid at a pace that would meet their needs as well as the needs to their customers, regulators and legislators.

In 2007, Congress passed the Energy Independence and Security Act (EISA 2007). In response to EISA 2007, several utilities launched efforts to develop Smart Grid plans. The people who had the responsibility developing these plans were often overwhelmed. The questions that we were asked at EPRI were "How do you develop a tactical plan to realize a high-level vision for merging IT and communications with the grid?" and "Where do you start?"

The answer that we would give is "you start with the IntelliGrid Methodology."

In 2007, EPRI began working with companies to develop company-specific Smart Grid roadmaps. EPRI was not the only company that was working with utilities to develop roadmaps. IBM, Accenture and KEMA were some of the others developing roadmaps. EPRI's core business is collaborative research and development, not consulting services. EPRI's R&D objective was to develop company-specific Smart Grid roadmaps with a diverse set of utilities and independent system operators (ISOs) to:

- Characterize and document the unique evolutionary pathways that a company would take to realize their Smart Grid vision
- Understand the commonalities in the different pathways
- Understand the differences in the pathways and why those differences exist.

Since 2007, EPRI has worked with the following companies to develop company-specific Smart Grid roadmaps:

- FirstEnergy
- Salt River Project
- Duke Energy
- Southern Company
- California ISO
- Tennessee Valley Authority
- FirstEnergy (refresh)
- Long Island Power Authority

In addition, EPRI has worked with the consumer-owned electric utilities operating within the Tennessee Valley Authority service area under contract with the Tennessee Valley Public Power Association to create a Smart Grid roadmap. EPRI also worked with Pacific Gas & Electric, Southern California Edison and San Diego Gas & Electric to develop the "California Utility Vision and Roadmap for the Smart Grid of Year 2020" under contract with the California Energy Commission.

In developing the company-specific Smart Grid roadmaps, an extension of the IntelliGrid Methodology has been developed; the Smart Grid Roadmap Methodology (SGRM). EPRI has worked with hundreds of individuals of large investor owned utilities, small cooperatives, municipal utilities, government agencies and ISOs. The EPRI project team has gained tremendous insight into what makes a roadmap a "living document" that guides a company in its investments and implementations and investments rather than being just a piece of "shelfware".

The objectives of this report are to:

- Document EPRI's methodology for developing Smart Grid roadmaps
- Share insights, lessons learned and best practices from EPRI's experience in developing company-specific Smart Grid roadmaps

Additional Experiences with the IntelliGrid Methodology

Preceding and apart from the roadmap work, there have been several IntelliGrid general technology transfer projects and workshops where the general concepts of the IntelliGrid Methodology were introduced including the use case based requirements methodology. These workshops and applications of the IntelliGrid Methodology helped refine the process eventually used for roadmap development. These utilities and workshops included:

- Southern California Edison – 2004 to 2009
- PSE-O - February 2004
- EDF - February 2004
- LIPA - August 2004, January 2007
- ConEd - August 2004, December 2005
- SRP - November 2004
- TXU - November 2004
- BPA - February 2005
- Sempra - March 2005
- Alliant Energy - April 2005
- NYPA - June 2005
- CEC - July 2005
- PNM - October 2007
- Consumers - November 2007

NIST and the Smart Grid Interoperability Panel (SGIP)

EPRI and EnerNex utilized the IntelliGrid use case based requirements methodology to assist NIST with the 2009 workshops implemented to help NIST carry out their EISA 2007 responsibilities. The continued the use of the

process after the instantiation of the SGiP has resulted in an ever increasing library of uses cases captured in the EPRI IntelliGrid format and made available in the public domain through the SGiP, DoE Smart Grid Information Clearinghouse, EPRI and other repositories.

What is the Difference between the EPRI IntelliGrid Methodology and the Smart Grid Roadmap Methodology?

The EPRI IntelliGrid Methodology – has the objective of assisting power system companies and staff in implementing the ideas of the IntelliGrid Architecture documents. There is a strong focus on principles related to architecture development, project planning, requirements definition (with use cases) and technology capability / selection. Cyber security best practices are also highlighted.

The Smart Grid Roadmap Methodology (SGRM) - has the objective of helping companies address applicable business objectives and mitigate associated drivers by succeeding in the effective adoption and implementation of technologies, applications and standards. Five key steps have been adopted for the SGRM; Vision, Requirements, Assessment, Planning and Roadmap Implementation. Within each step there are three or four recommended tasks. In summary the SGRM will result in a roadmap that is a technology portfolio optimization plan.

Section 2: Defining Smart Transmission, Distribution and Customer Engagement

Sometimes called "the world's largest machine," the US electricity system encompasses more than 5,000 large central station generating stations connected together by 157,000 miles of high-voltage transmission lines and millions of miles of distribution wires. Yet, except for its gargantuan size, today's centralized system hasn't changed fundamentally since its inception well over a century ago. While there have been continual technological advances, it hasn't undergone the digital transformation that characterizes most industries, and the grid remains largely a one-way system of providing electricity to businesses and households on demand. Those demands have continued to rise, with the percentage of total US energy consumption devoted to electricity at 10% in 1940 and 25% in 1970. Today it is 40% and still growing, with plug-in electric vehicles about to hit the mass market. If power were an infinite resource without "negative externalities" like environmental consequences, if transmission lines were easy to site wherever needed, and if consumers had money to burn, the system could continue on the same trajectory for a long time to come. But, that path appears increasingly unsustainable, and several converging trends point to a new direction for America's energy future, one that poses new challenges and new opportunities for consumers, utilities, and regulators.

As the electrification of our economy and the number of electrical devices we use to support a modern lifestyle grow each year, the electricity infrastructure we take for granted is aging. Increasing numbers of critical components in the electric power generation and delivery system remain in service well beyond their design life and are being stretched to the limits of their capacity. While overall electricity demand grew by more than 25% since 1990, construction of transmission facilities fell by 30% in that period. The resulting congestion has increased market electricity prices and raised line losses from 5% of electricity transmitted in the 1970s to 10% today. The threat of system failures – and their potential cost to consumers and the economy -- is on the rise.

The average age of power plants is more than 30 years; however, economic constraints and environmental concerns limit the construction of large new central station generators. Construction and equipment costs continue to climb, and a study by the Brattle Group estimates a total cost of at least $1.5 trillion

dollars over the next 20 years to provided needed upgrades, new power plants, and expansion of capacity, including $880 billion in transmission and distribution investment.

At the same time, concern about carbon dioxide and other emissions contributing to global climate change is producing public demands for alternatives to fossil-fueled electricity. Electricity production creates almost 40% of the nation's output of "greenhouse gases" -- twice as much as produced by the transportation sector. Policy in many states has begun to shift towards promoting renewable energy resources, which have been expanding rapidly in recent years. The installed capacity of wind power and solar power in the US grew by 40% in 2009 alone. The growth of state Renewable Portfolio Standards over time can be anticipated to keep these resources at the forefront of new energy development, as Illinois and many other states strive to use clean energy to improve the environment and create jobs. While non-hydro renewable energy currently supplies less than 4% of US electricity needs, US-DOE projects potential for more than 20% of US electricity to be generated using these sources within the next twenty years. However, wind and solar power are variable and distributed resources; bringing them to market and integrating them into the resource mix at high penetration levels is a challenging task.

What is a Smart Grid?

Smart Grid is a high-level concept for "modernizing" the electric power system to support the anticipated needs of society. The concept received a great deal of visibility by its inclusion in the Energy Independence and Security Act of 2007 (EISA 2007). EISA 2007 was an act of Congress which laid out the energy policy for the United States.

Title XIII in EISA 2007 states that:

> "It is the policy of the United States to support the modernization of the Nation's electricity transmission and distribution system to maintain a reliable and secure electricity infrastructure that can meet future demand growth and to achieve each of the following, which together characterizes a Smart Grid:
>
> 1. Increased use of digital information and controls technology to improve reliability, security, and efficiency of the electric grid.
> 2. Dynamic optimization of grid operations and resources, with full cyber-security.
> 3. Deployment and integration of distributed resources and generation, including renewable resources.
> 4. Development and incorporation of demand response, demand-side resources, and energy-efficiency resources.
> 5. Deployment of "smart" technologies (real-time, automated, interactive technologies that optimize the physical operation of

appliances and consumer devices) for metering, communications concerning grid operations and status, and distribution automation.

6. Integration of "smart" appliances and consumer devices.
7. Deployment and integration of advanced electricity storage and peak-shaving technologies, including plug-in electric and hybrid electric vehicles, and thermal-storage air conditioning.
8. Provision to consumers of timely information and control options.
9. Development of standards for communication and interoperability of appliances and equipment connected to the electric grid, including the infrastructure serving the grid.
10. Identification and lowering of unreasonable or unnecessary barriers to adoption of smart grid technologies, practices, and services."

At the highest level, a Smart Grid infuses Information and Communications Technologies with the existing electric power infrastructure (grid) to improve the efficiency and performance of the grid and provide electricity consumers with more information, options and control of their service.

A Smart Grid can be thought of as a collection of new technologies that are integrated into the existing electricity infrastructure that enable new or enhanced capabilities.

For example, Smart Grid Technologies can include:

- Communications networks
- Sensors
- Data processing and management
- Phasor Measurement Units and other intelligent electronic devices
- Smart meters and related applications
- Software applications such analytics
- Communications protocols

Electricity Infrastructure can include:

- Transmission lines
- Substations
- Transformers
- Distribution lines
- Generation
- Distributed generation
- Loads

New or enhanced Capabilities can include:

- Dynamic line rating
- Situational awareness
- Demand response
- Automated fault location, isolation and recovery
- Automated voltage management
- Smart metering
- Usage information to consumers
- Condition-based maintenance

How Does A Smart Grid Get Built?

Electric utilities are responsible for building and maintaining the electricity infrastructure and for providing electricity service to consumers. Investor owned utilities generally operate under the "Regulatory Compact". The Regulatory Compact is a covenant between the authority of state governments, represented by public utility commissions, the Federal Energy Regulatory Commission (FERC) and in some cases local government and investor owned utility companies. In exchange for the obligation to provide service to all customers in that territory, investor owned electric utilities are given a territorial monopoly on service and allowed to earn a limited profit. State regulators set prices at rates that reflect the cost of building power plants and putting up the wires. Profits have reflected the cost of capital.

The Edison Electric Institute forecasts that the U.S. electric utility industry will spend approximately $80 to $85 billion per year on capital investments over the next several years. This is approximately twice the capital expenditure made by the industry in 2004. Capital investments are typically made to meet load growth and to maintain reliability. Capital investments are balanced by the desire to maintain affordable electricity rates for consumers.

However, the costs for smart grid deployment are substantial, the barriers are significant, and the benefits will not accrue to all customers equally. For example, the cost to deploy Smart Meters in California is in excess of $5 billion. In assessing smart grid, each state must take into account a host of local issues including, regional and local economics, energy sources, energy market structure, consumer preferences, and impacts of geography and demographics. Affordability to consumers and fair treatment of those with special needs is always a key issue for regulators and is essential to public acceptance of any changes in utility service or policies. A successful approach to grid modernization must consider these issues and factor them into how utility investments are proposed, approved, and funded. Mechanisms for determining costs and benefits - and who bears the costs and realizes the benefits - must be developed and implemented consistently. All of these are vital aspects addressed by a sound

roadmap development effort using the EPRI IntelliGrid Roadmap process and framework.

Electric utilities, in close cooperation with their regulators, are the organizations that will build a Smart Grid. Since Smart Grid investments are made to provide new or enhanced capabilities, they tend to be in addition to the capital investments that are made to meet load growth and maintain reliability. Deployments of Smart Grid technologies can also have a profound impact on the day-to day business of the utility. The questions that utilities and regulators are asking are "do we need to invest in the Smart Grid?" and, if so, "which Smart Grid technologies and capabilities should we deploy?"

Drivers for Change

Frankly, if everything in the electric power sector stayed the same, there would be little need to build a Smart Grid. However, there are several factors that are compelling utilities to adopt the new or enhanced capabilities that Smart Grid technologies enable. These drivers include:

- The Drive for Greater Energy Independence and Decarbonization has lead several nations and states to establish policies to reduce carbon dioxide emissions, increase the amount of renewable generation and promote energy efficiency. As an example, Figure 2.1 shows several of the energy and environmental policies enacted by California that influence the State's Smart Grid.
  - Assembly Bill 32 (AB 32, the California Global Warming Solutions Act) establishes a comprehensive program of regulatory and market mechanisms to achieve real, quantifiable, cost-effective reductions of greenhouse gases (GHG). AB 32 makes the Air Resources Board (ARB) responsible for monitoring and reducing GHG emissions.
  - Executive order S-3-05 calls for a greenhouse gas reduction goal of 1990 levels by 2020 (30% reduction from projected levels by 2020, 15% reduction from current levels), with a target of 80% below 1990 emissions levels by 2050.

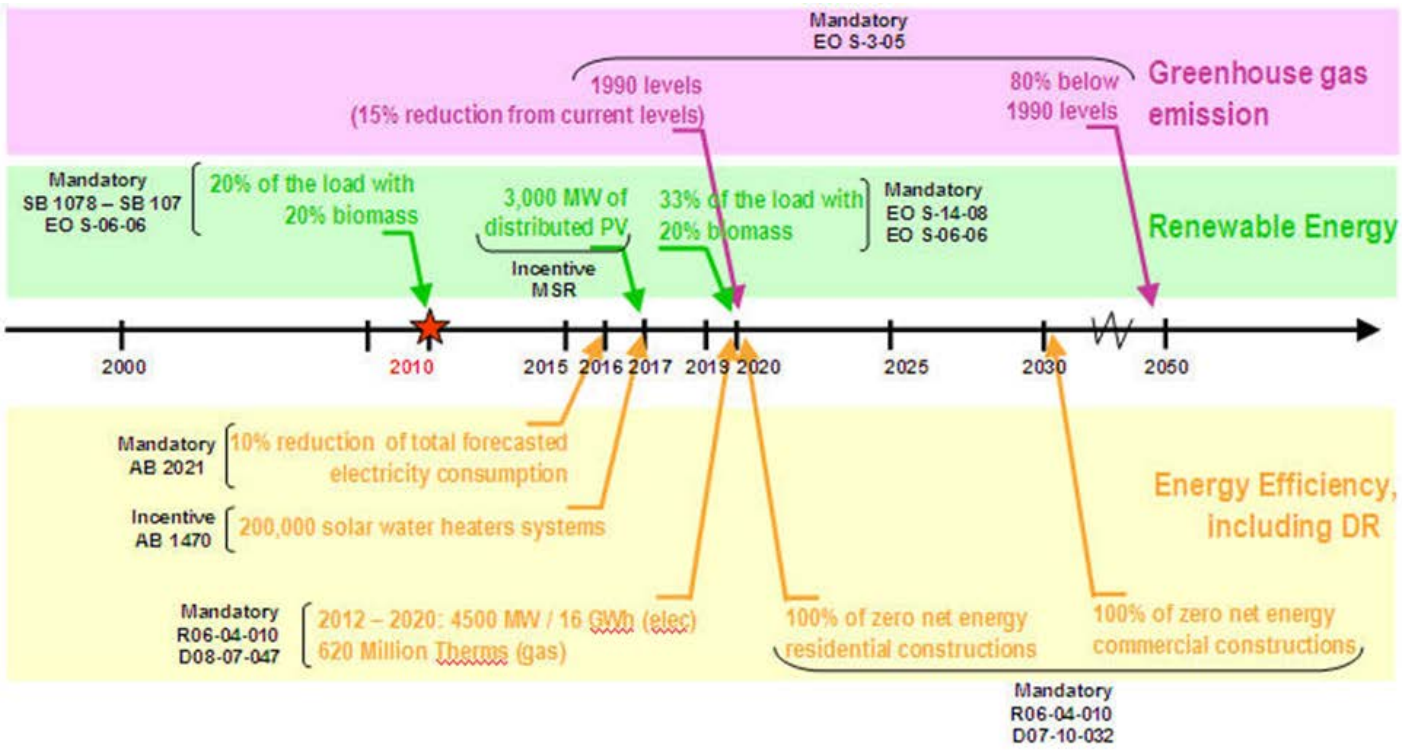


Figure 2-1
California Policies that establish Targets for Reduction in Greenhouse Gas Emissions, Increase in Renewable Energy and Improved Energy Efficiency that influence the State's Smart Grid

California Policy: Renewable Portfolio Standard

- Executive Order S-14-08 requires California's retail sellers of electricity to serve 20% of their load with renewable energy by 2010, and 33% of their load with renewable energy by 2020.
- Executive Order S-06-06 promotes the use of bioenergy, and calls for the state to meet a 20% target for the use of biomass for electricity generation within the established state goals for renewable generation for 2010 and 2020.

California Policy: Distributed Energy Resources

- Million Solar Roofs Program: the goal of this program is to install 3,000 MW of distributed solar photovoltaic (PV) electricity generation in California by the end of 2016.
- Combined heat and power (CHP): the California Air Resource Board in its Scoping Plan sets a target of an additional 4,000 MW of installed CHP capacity by 2020, enough to displace approximately 30,000 GWh of demand from other power generation sources.

California Policy: Energy Efficiency

- AB 1470 –Solar Water Heating and Efficiency Act: Authorized a ten year, $250-million incentive program for solar water heaters with a goal of promoting the installation of 200,000 systems in California by 2017
- AB 2021 – Public utilities: energy efficiency: Sets a statewide goal of reducing total forecasted electricity consumption by 10% over the next 10 years (starting 2006).
- Rulemaking 06-04-010 Decision 08-07-047: First, this decision sets interim energy efficiency savings goals for 2012 through 2020 for electricity and natural gas on a total market gross basis. For 2012 through 2020, total energy savings are expected to reach over 4,500 megawatts, the equivalent of nine major power plants. Further, the decision expects savings of over 16,000 gigawatt-hours of electricity and 620 million therms over that period. The decision also confirms existing energy savings goals for 2009 through 2011 that shall be gross goals, not net of free riders (D.04-09-060 goals over the 2009-2011 period: 7516 GWh, 1584 MW and 162 million therms).
- Rulemaking 06-04-010 Decision 07-10-032: All new residential construction in California will be zero net energy by 2020. All new commercial construction in California will be zero net energy by 2030.
- California Air Resources Board (CARB) Scoping plan: the plan would set new targets for statewide annual energy demand reductions of 32,000 gigawatt hours and 800 million therms from business as usual – enough to power more than 5 million homes, or replace the need to build about ten new large power plants (500 megawatts each). These targets represent a higher goal than existing efficiency targets established by CPUC for the investor-owned utilities due to the inclusion of innovative strategies above traditional utility programs.

- Difficulty Siting New Transmission Lines

  Obtaining new rights of way is extremely difficult in many parts of the United States. Most new transmission lines face local opposition. Although opponents often invoke environmental or health issues, they are usually motivated by other concerns: land use, property values, aesthetics, potential impacts on nearby recreational areas or wildlife habitat, etc.

  An example of the difficulty in siting new transmission is the construction of the Wyoming-Jacksons Ferry 765 kV transmission line by Appalachian Power. The 90-mile line that connects power stations in Wyoming County, WV, and Jacksons Ferry, VA was completed in 2006. Ultimately, the $306 million project took 13 years to permit and just under three years to construct.

- Retirement of Generating Plants

  Many generating plants in the U.S. are reaching the end of their lives. More stringent EPA environmental regulations have impacted generating resources and production costs creating downward pressure on coal plants. Large-scale changes in the generation fleet significantly impact power flow on the transmission system which can result in some lines being overloaded and others being underutilized. Reliability and safety can be impacted by changes to the available reserve generation capacity. Short term operating reserve margins will increase in response. Planners may need to increase long-term reserve margins. Access to the most cost-effective generation could be restricted. The loss of base load fossil powered plants limits dynamic reactive control tools and reduces frequency response.

- Aging Infrastructure

  It is not unusual for assets with a 40 year asset life to stay in service for 50 or even 60 years. As an example, one utility has reported that 25 percent of overhead conductors, 25 percent of overhead groundwires and 35 percent of tower structures have surpassed 75 percent of their expected service life. Sixty seven percent of power transformers, 46 percent of breakers and 30 percent of relays are likewise 75 percent or more through their expected service life.

  However, age is not the only determinant of asset's health. In the case of a transformer, running the transformer at under 50 percent of its manufacturer's recommended load (nameplate) means it will last almost forever, on the other hand running it at over 130 percent of its recommended load can reduce the life of the transformer from roughly 40 years to roughly 8 years.

  Older equipment can have higher failure rates that could impact the reliability of the grid. Increased inspection and monitoring is required to sustain system reliability and safety. Maintenance activity is increasing and will be reactive in nature in the absence of improved system awareness.

- Aging workforce

  More than 50 percent of the utility workforce in the U.S. is age 45 or older. The U.S. Bureau of Labor statistics indicates that 30 percent or more of the existing utility workforce is or will be eligible for retirement in the next five years.

  The North American utility industry is experiencing pressures trying to maintain cost effective, reliable, safe and compliant service in the face of a rapidly aging workforce. Losing experienced workers to retirement and competing in the marketplace for more technically adept replacements increases costs and threatens reliability and safety.

- Electric Vehicle Integration

  It is anticipated that the number of plug-in electric vehicles (PEV) will increase in the future. Large concentrations of PEV could strain the existing infrastructure. One EV parked at a typical household in a middle class neighborhood could double the monthly demand for electricity. At parking garages, a single charger for an EV can draw as much electricity as the whole parking garage infrastructure did previously. In areas where the grid was built in the 1946 to 1960 time period, the local infrastructure may be strained by a small number of electric vehicles trying to charge.

- Changing Consumer Expectations

  Consumers have come to expect instant response from their electric supply - from flipping on the light switch to turning on the TV or computers. Even the slight delay in turning on the compact fluorescent (CFL) bulbs seems intolerable at times. Consumers want their electric supply to be cost-effective, and they want the convenience to use electricity when they want to do their tasks. While these consumer expectations will likely remain for a long time to come, the Smart Grid helps the electric utilities meet these consumer demands at the most effective cost throughout the day, while reducing the peak demand for electricity in a convenient non-intrusive manner. The Smart Grid will help consumers become more aware of their energy uses, and give them a means to control their energy costs.

- Economic Development

  The smart grid can help foster economic growth by improving the reliability and reducing cost of electricity service in order to spur new investment and job growth in a region. An example of this is the New York Energy Highway, a public private partnership that will provide more reliable, lower cost power for New York's homes and business, protect and create jobs, spur new investment in New York State, generate economic growth and safeguard the environment.

  The smart grid is also an industry in itself which presents governments with an opportunity to invest and support initiatives that foster a) innovation (both technological and intellectual) and b) economic development through skills development and job growth.

Challenges for the Electricity Infrastructure Resulting from the Drivers

The Drivers listed above present several challenges for the electric infrastructure. These challenges include:

- Integrating renewable resources into the transmission system

  There are numerous issues that will need to be resolved with integrating bulk renewable generation into the existing utility transmission system such as managing intermittent generation ramp rates, avoiding congestion and maintaining adequate system protection.

  Additional transmission infrastructure will be required to move the power from areas where renewable resources are concentrated to the load centers. Also, transmission systems must reduce the overall variability by aggregating and averaging local variable generation over large geographic areas.

  System planning must expand beyond traditional service territories to work regionally and inter-regionally.

  Capacity planning will need to cover not only maximum load scenarios but also low load scenarios and shoulder-load scenarios that may present higher reliability risks than in the past. It will also be necessary to increase the flexibility of the power system to respond to more variability and uncertainty. The potential exists for this flexibility to come from both conventional generation and new sources such as controlled smart charging of electric vehicles, energy storage, and additional system coordination.

  Wind and solar are the currently preferred renewable sources to mitigate carbon dioxide production. Wind and solar tend to be variable in their production and that means that either demand has to vary to match the production, or storage needs to be added to the grid, customers need to be removed from the grid, or additional non-variable generation needs to be added to the production mix.

- Integrating large amounts of distributed generation on the distribution system

  The growth of renewables has changed the way the grid has to operate. The grid is designed to allow power to safely flow from central generation to the consumer. To reduce issues with lightning and other surges, the grid is designed to prevent most power from flowing from the consumer back toward central generation. Getting the grid ready to allow two way power flow means changing this protection system and sometimes the supporting equipment that is installed in the grid.

  Distributed generation has a tendency to be installed unevenly across the grid, causing additional issues that have to be dealt with, like uneven voltage increases, harmonics and changes in the power factor. All of these changes

have to be anticipated and dealt with as part of the new grid design. Because the renewable generation is typically variable in nature, turning on when the sun is up or the wind is blowing at the right speed, these issues come and go as the generation runs or does not run. Depending on their capacity (size), operational characteristics, and the nature of the electric system to which they are connected, these resources will need to be paired with energy storage and control technologies.

- Developing effective approaches for reducing consumption at peak times

  If everyone consumed the same amount of electricity at all times, all of the assets in the grid would run at peak efficiency at all times. Unfortunately this is not true. Peak demand can be two, three, four or more times the average demand. A typical asset has to be sized to handle peak, not average demand. Since 1970 the difference between peak and average demand has been growing faster than overall demand. That means that assets have to be larger and they are used in a less efficient manner. Ensuring grid capacity levels can support customer demand is a major part of system adequacy. With peak power growing quickly, many circuits in the grid are rapidly approaching or exceeding their design limits.

  Because of the difference between peak and non-peak usage, shifting some of the peak energy demand from peak to off peak can significantly increase the life of the circuit and associated assets and at the same time increase system adequacy and efficiency.

- Reducing transmission and system losses

  Transmission efficiency is defined as providing more power from generator to end-user without increasing asset infrastructure. Efficiency improves the cost effectiveness of the transmission grid by deferring capital investment. Transmission efficiency reduces congestion and can, therefore, improve the design life of aging assets that are adversely impacted by an overloaded grid.

  Today, transmission losses account for between 2 and 4 percent of the total electricity generated in the United States. While the percentages may appear relatively low, the total amount of energy involved is considerable, equating to between 83 million MWh and 166 million MWh lost each year based on a total US annual generation of 4,157 million MWh.

  In the modernized grid, utilities will harness improvements in microprocessor relay data gathering technology to improve transmission system efficiency. Where relay data is gathered routinely, maintenance staff can run useful analytics to save time and money. For example, accumulating the I^2t value for each circuit breaker over time allows an algorithm to be developed that triggers preventative breaker maintenance at a prescribed value. This same information could be provided to operators to make them aware that circuit breakers are due for repair and so be incorporated into contingency planning. Monitoring contact timing values identifies breakers that operate slowly and require maintenance. Maintenance tasks tend to be

simple lubrication and exercising the breaker. Without preventive maintenance more failed breakers need replacing since the slow opening causes excessive arcing and heating.

- Developing effective approaches for promoting consumer energy efficiency and conservation

  The Smart Grid represents a change to our fundamental and most consistent relationship with our approach to electricity consumption. The Smart Grid has the potential to give us much more control over our own electricity usage, enables us to have the greatest control over the price we pay for electricity, and allows us to change our energy use in response to price signals and other operational controls. The Smart Grid represents a significant change in the way we think about and use electricity, as well as interact with our electricity supplier.

  Consumer energy efficiency and conservation will likely best come through establishing rational expectations and developing an understanding of what is realistic to expect from the Smart Grid. This approach will help the pricing of electricity become more comprehensible while allowing the consumer much more flexibility in determining how to participate. The communications and transparency of the process and pricing must support and help the consumer witness how the Smart Grid works to encourage them to accept it. In addition, the utilities must be consistent in their message to present the reality of the solutions available to the consumer while educating them on how the Smart Grid can help promote their energy efficiency and conservation strategy.

New and Enhanced Capabilities Needed to Respond to Drivers and Challenges

- Enhanced Situational Awareness

  Situational awareness means understanding the current environment and being able to accurately anticipate future problems to respond effectively. In a future, more complex grid environment, operators not only need to know how close they are to the edge with greater precision than ever before, but also how quickly they are moving in any particular direction.

  Currently, control centers use Supervisory Control and Data Acquisition (SCADA) technology to feed data from transmission substation Remote Terminal Unit RTUs into an engine that estimates the state of the power system once every few minutes. Increasing situational awareness in a modernized grid involves creating enhanced visibility into the grid and access to more effective decision support tools.

- Enhanced Visibility

  In a modernized grid, integrated advanced sensors and robust communications provide greater visibility into the power system state. A larger population of more precise sensors enhances visibility.

Many utilities have already deployed synchrophasor technology to enhance power system visibility over the past decade and will increase its use of synchrophasor data for both on-line and off-line applications by 2020.

Numerous applications use Phasor Measurement Unit (PMU) data. Oscillation monitoring, event location, and extra high voltage (EHV) state are three primary examples. Power system oscillations cause equipment damage, reduced stability margins and other operating problems. Event location expedites outage restoration by quickly identifying probable outages. System EHV state is quickly determined when increased system status information is available, resulting in faster convergence between the Energy Management System (EMS) and the actual system state.

In addition to PMUs, sensors monitoring the health of critical components such as transformers and circuit breakers will be increasingly deployed. This data will serve multiple purposes including enhancing power system visibility and asset management.

As new technologies are deployed to enable greater visibility into the transmission grid state, the information and communication technology (ICT) infrastructure becomes increasingly critical. Modern grid technologies demand more analytical horsepower and data-handling capabilities. Some data is harvested in real time and some is stored in a historian database. Data is made available to end users and end-use applications with the desired levels of accuracy, security, and speed.

An ICT infrastructure allows diverse datasets to be quickly and accurately transmitted across an entire network. Users customize their data and information needs. Emerging end-use applications facilitate the work of planners and operators. Two-way communication between data sources enables remote management of demand response, energy storage, and plug-in electric vehicles.

- Decision Support

  In a modernized grid, decision support tools manage and organize large data flows from transmission and equipment sensors to automate processes such as system restoration and reactive power management in real time. Decision support tools identify exceptions in large data flows to monitor performance and compliance as well as to manage risk and resource adequacy. Using standard methods and approaches to implement decisions provides the operator with rigor and continuity in project planning and execution. The following decision support capabilities are enabled in the modernized grid:

  - Better control-center tools and techniques improve the operator's situational awareness and decision-making
  - Simulation and modeling are used frequently to perform off-line studies and real-time contingency analysis

- Grid planners and operators have the ability to seamlessly transfer real-time Energy Management System (EMS) data to off-line simulation study tools for studies and to transfer results back to an EMS environment for display
- Fast simulation techniques facilitate prompt real-time contingency analysis
- Automated processes validate component simulation models (such as generator-excitation system models) by comparing routinely available field data with simulation results
- Operators restore systems following major blackouts using tools to identify an optimal system restoration path from the multiple paths available during restoration
- Grid operators identify potential voltage instability areas and the corresponding dynamic and static reactive power requirements in these areas in real time to avoid instability
- Automated voltage-control strategies are in place to address potential voltage-collapse situations using various voltage-control devices such as generator automatic voltage regulators (AVRs), capacitors, shunt reactors, static var controllers (SVCs), FACTS devices, and power system stabilizers (PSSs)
- For each potential voltage-security or collapse scenario identified from off-line studies, PMU data is used to calculate MW or MVAR margins available in real time before a voltage collapse occurs. Real-time tools, including mitigation strategies, guide operators through security situations
- Automated tools replicate system events using power flow and system dynamics simulation programs. The tools include interfaces to read real-time data across wide areas. This facilitates timely event investigation for root causes, solutions, and what-if scenarios

- Voltage Management

  Voltage management will improve the power factor of the power flow, and in the process reduce line losses, increase the utilization factor for the grid assets, and reduce the peak loading of assets. Moreover, such improvements will also enhance efficient operation of customer loads by reducing customer system losses and thus contributing to the overall peak demand reduction.

  The implementation of grid efficiency, voltage reduction and voltage regulation approaches and solutions will require more monitoring and data collection from the grid in order to increase the knowledge and understanding of its current operating state. In order to transform the data generated into actionable information that can be directly used by operators, data management and processing systems are needed as well as optimization algorithms. Finally, the advancement of materials such as composites, superconductors, next generation semiconductors, and Flexible Alternative Current Transmission Systems (FACTS) devices will also provide highly efficient and flexible solutions to improve overall grid efficiency and performance.

- Asset Monitoring and Performance-Based Maintenance – Substations

  A modern grid will enhance the value derived from grid assets through asset condition monitoring, leading to condition-based maintenance. Asset condition monitoring will be enabled by the installation and use of different sensor technologies in order to collect data relevant to the state of assets through an adaptive communication infrastructure. The new generation of embedded and automated field devices, such as smart transformers and communicating fault indicators among others, will integrate the monitoring and data collection capability. Advanced data analytics functions such as tracking and monitoring algorithms, expert systems, predictive analysis, and enhanced visualization tools will enable transformation of field data into useful information to be used in asset management and performance optimization processes.

Some of the asset-monitoring systems are listed below

ASSET	MONITORING SYSTEM
Transformer	• Cooling system • On-line LTC monitoring • On-line DGA • On-line moisture in oil monitoring • On-line winding temperatures and hot-spot detection • On-line bushing monitoring • On-line frequency response analysis • Geomagnetically induced current monitoring
Circuit Breaker	• Pole separation timing monitoring
Gas Insulated Substation (GIS) Bus	• On-line SF6 density monitoring • UHF partial discharges
Disconnects and Terminal Equipment	• On-line temperature monitoring

- Asset Monitoring and Performance-Based Maintenance – Lines

  In much the same way as asset monitoring of substation equipment, a modern grid will enhance the value derived from transmission line assets through asset condition monitoring, leading to condition-based maintenance. Asset condition monitoring will be enabled by the installation and use of different sensor technologies and computer applications to collect and analyze the data relevant to the state of the transmission assets through an adaptive communication infrastructure. The new generation of embedded and automated field devices, along with advanced network application software technology will integrate the monitoring, data collection, and

analysis capabilities. Advanced data analytics functions such as tracking and monitoring algorithms, expert systems, predictive analysis, and enhanced visualization tools will enable transformation of field data into useful information to be used in asset management and performance optimization processes.

- Dynamic Rating of Substation Equipment and Lines

  Based on the loading, operating, and environmental conditions, the ratings for various substation and transmission line equipment can be adjusted dynamically to provide for greater throughout of power as needed to meet the changing system conditions. Typically, the operating limits of the field equipment are manually set based on operating conditions emulated during the planning stage for implementation. These limits are typically conservative settings to protect the equipment while allowing for classical loading levels. As more accurate information becomes available for the substation and transmission line equipment under various operating conditions, these operating limits can be adjusted dynamically to allow for higher loading levels of operation during specific system conditions of peak loading or environmental conditions that would permit greater loading levels to occur. These settings can also be adjusted dynamically to limit the transfer capability of the equipment, if needed.

- Phasor Measurement Applications

  As phasor measurement units (PMUs) are implemented throughout the electric grid, additional information will become available on a more frequent basis to more accurately determine the state of the electric system. The PMUs provide more frequent measurements of voltages and phase angles throughout the electric grid that will help advanced applications predict and report any unusual conditions occurring on the grid in real-time and allow the system operators to recognize and respond to changing system conditions before a system cascading event can occur. The North American SynchroPhasor Initiative (NASPI) was transitioned to NERC in 2007 to help coordinate industry activities and to facilitate a synchronized data measurement network in North America with associated analysis and monitoring tools for enhanced reliability.

- Demand Response

  Demand response involves the active management of consumer loads on a day-to-day basis to balance electricity supply and demand. Some of the approaches to demand response include:

  - Direct load control (DLC) – Provides the utility the ability to reach into a customer location and turn off one or more devices. The most successful DLC programs turn off items that the customer would not notice, like the hot water heater on a hot day, instead of the item they are using at the time, like air conditioners. Florida Power and Light has the largest residential DLC program today.

- Demand Limiting (DL) – Demand limiting provides a threshold of demand that the customer has to stay under. This means that the customer has to maintain their overall load (use of energy) below the demand limiter that is typically built into the meter. ENEL in Italy built demand limiters into the smart meters they installed at 27 million households.
- Price Response (PR) – Customers are given a price for electricity for an upcoming period of time and they decide whether to pay more or reduce the amount of electricity they use. Price response includes Time of use (TOU) pricing, real-time pricing (RTP), critical peak pricing (CPP) and other pricing programs.

Demand response can minimize the need to build costly new generation and delivery infrastructure. The various demand response programs will tend to be optimized for operational value and targeted at specific customer segments that are most able to respond. Communications and load management technologies will be available to help maximize demand response convenience and cost-effectiveness.

- Electric Vehicle Charging Infrastructure

It is not enough to have plug-in electric vehicles (PEV). To be able to operate them, an infrastructure similar to the gas station infrastructure that exists for gasoline and diesel vehicles needs to come into existence. Further, most PEVs take hours, not minutes to recharge. This infrastructure has several parts the need to be thought through. The Society of Automotive Engineers (SAE) has developed standards for global charging plugs and charging rates. This set of standards starts with J1772 and run though J2847 which outlines how PEVs will communicate with charge stations and other devices. These standards provide the physical connection infrastructure and the communications infrastructure between the vehicle and the rest of the world. They do not deal with payment methods, charge station installation rules, number of charge stations, or other items that will impact the way the grid and PEVs interact.

Charging infrastructure will at least initially control when a PEV can charge and what the price will be. The initial set of PEV's are not smart enough to understand electricity pricing or to understand that it should not charge right now. As the next generation of PEV's are released, the need for charge stations to be the control point will probably be reduced. Grid operators today do not see enough PEVs to make them a factor in load planning, or make it an issue to stop them from charging even at peak. As the number of PEVs on the road increase, this too will change. The charging infrastructure needs to be designed to support this control need, as well as the ability to pass a price to the PEV or the PEV owner.

- Enhanced usage information to consumers

Today most customers only interact with the grid by paying their bill. To encourage customer participation it is important to provide them information

on when and how much they are consuming, an incentive to participate, and provide them with the times and reasons to participate.

Customers have for more than 100 years only received information, in the form of their bill, which arrives so long after their use of electricity that they seldom can remember what they were doing that caused the use. Additionally they have not been offered incentives to change the way they use electricity, nor have they ever been educated about the true cost of electricity. Over the history of the grid, utilities have been required to manage the price, supply and risks for the customer and to provide them with a bill that averages these items over the billing period.

Today, it is possible to provide customers with detailed information from meters or other measurement instruments, and timing information from forecasting systems. This information can empower the customer to decide how and when to interact with the utility via variable tariffs, take advantage of rebates and/or other programs made available to them.

- Consumer Energy Management Tools

  A modern grid will provide consumers with better information, choices and control of their electricity service.

  - Value-added web tools to help customers understand their energy usage on a day-after and historical basis (e.g., trend analysis, benchmarking)
  - Authorized third-parties have access to customer data in machine-readable format and can help customers manage their energy usage
  - Customers will have the ability to obtain and install devices that automatically trade-off energy cost, comfort, and environmental impact based on user preferences; devices also provide remote control capabilities (via Web)

  The typical first step in providing consumers with energy management tools is to install a smart meter. A next step could be to provide consumers with pricing information which may be delivered via the meter and its home area network card, or through another path like a cellular phone. In addition to pricing information may be demand limit information or demand limit commands, direct load control commands to specific devices in the home or business, and forecasting information to help customers plan (e.g. "Tomorrow will be a hot day and electricity prices will be high").

  Smart appliances and smart entertainment systems are starting to become commercially available. The Consumer Electronics Association (CEA) and the Association of Home Appliance Manufacturers (AHAM) are both working with the Smart Energy Profile (SEP) to provide devices that can understand and respond to information provided by the utility or a third party demand response aggregators. In two years AHAM expects to move the functionality down into the top 20 percent of their appliances, then two years later into their mainstream appliances (top 70 percent) and finally into their budget appliances two years later. So in countries that adopt the SEP as the messaging standard, in 2020, all income segments should be able to buy

and use smart appliances. In the average deployment of AMI, the time period from decision to proceed to final meter being installed is six-to-eight years. A decision to proceed today with AMI would be matched by appliance availability in most deployments. SEP can be deployed without an AMI system, if an alternate channel for communications is selected (e.g. mobile phone, internet, fixed line phones, etc), smart appliances need information on DSM programs and timing, which can be delivered in many ways. AMI can be used to provide a common infrastructure with a secure communication channel, should that be desired, but it is not required.

Other customer systems can include simple timer globes that change color depending on the time of day and programs that change the price of electricity at the same time each day. These systems can be very simply made and have been proven to be effective in reminding people that the price of electricity has just changed. In France the Tempo and BLUE programs have used time of use rates with almost 3 million customers for years. Customers have been able to buy a pricing reminder that changes colors for several years and those homes that have them do a better job of reducing their peak demand, and with that reduction their overall electricity bill.

Smart Grid Standards

Standards play an essential role in enabling a more seamless integration of new and diverse technologies to implement Smart Grid capabilities and features across the enterprise architecture. The National Institute of Standards and Technology (NIST) has been the focal point of the standards development process for the Smart Grid. NIST was charged by the US Congress in the Energy Independence and Security Act (EISA) of 2007 to coordinate the development of a standards framework to achieve interoperability of Smart Grid devices and systems. The Smart Grid Interoperability Panel (SGIP) was also formed by NIST as a result of the EISA 2007 legislation. The SGIP is a public/private partnership tasked with working with the various Standards Development Organizations (SDOs) to coordinate standards development and acceptance by industry for the Smart Grid. A number of international SDOs, such as IEEE, IEC, UCAi, and EPRI, are participating with the SGIP to define the Smart Grid requirements and develop the related standards to be followed by the industry. The SGIP has produced and maintains a Catalog of Standards and best practices that are considered relevant to the development and implementation of the Smart Grid.

In the post-9/11 age, grid security -- both cyber security and physical security -- is also a growing concern for system operators and planners, as well as customers. Congress has indicated that they will get increasingly involved in defining very specific mandatory measures that must be taken to protect critical electric infrastructure such as HR5026 - the Grid Reliability and Infrastructure Defense (GRID) Act. This Act together with the technical best practices being developed by NIST, DOE, and others must be considered and built into any new system being considered for deployment as part of a smarter grid.

Cyber Security is particularly critical to the success and reliability of the Smart Grid. To address the issues related to cyber security, NIST established the SGIP Cyber Security Working Group (CSWG). One of the centerpieces of the NIST activities has been the development of the NIST Interagency Report 7628, Guidelines for Smart Grid Cyber Security, the first draft of which was issued in August 2010. It is currently under revision for re-issue to the industry in late 2012. The CSWG has also moved on to focus on specific security-related topics such as risk management processes, key management within the Smart Grid, development of a Smart Grid security architecture, Advanced Metering Infrastructure (AMI) security, testing and certification, and privacy within the Smart Grid.

The North American Electric Reliability Corporation (NERC) is also a standards development organization that is focused on the reliable operation of the bulk electric system and has developed standards related to cyber security. Version 4 of the Critical Infrastructure Protection (CIP) Cyber Security standards was recently approved by the Federal Energy Regulatory Commission (FERC) and is set to be effective in April 2014. These standards while focused on the reliability of the bulk electric system are closely connected to the security of the Smart Grid. In addition to the various standards setting organizations, there are also a number of industry groups that are promoting the use of standards in the development of the Smart Grid's capabilities. One of the most prominent of these organizations is the Utility Communications Architecture International Users Group (UCAIug).

Section 3: The Role and Purpose of a Roadmap

The goal of the Smart Grid Roadmap Methodology (SGRM) is to help a company transition from understanding what the Smart Grid is generically to achieving the most effective timing and adoption of Smart Grid technology in a way that uniquely maximizes the benefits and minimizes risks for the utility or ISO. More specifically, the purpose of a Smart Grid Roadmap is to help a utility address the business objectives and mitigate the drivers by succeeding in the effective adoption and implementation of technologies, applications and standards. In summary the roadmap is a technology portfolio optimization plan.

The SGRM includes the five key steps of ; Vision, Requirements, Assessment, Planning and Roadmap Implementation. Within each step there are three or four recommended tasks. These steps and tasks are described in detail in Chapter 4.

The Big Picture and the Roadmap

It is also instructive to know the place of a Roadmap and the SGRM in the context of the bigger picture for the utility. The SGRM ideally commences after the overall corporate technology strategy is in place and the C-level sponsorship (ideally cross-functional) is in place. It is assumed that this strategy addresses key regulatory and policy mandates applicable to the utility. After the Roadmap is complete, the next steps may include: conceptual architecture, logical architecture, updated cost benefit analysis, continued progression of the technology stage gate process (see Chapter 5 for an example), technology testing and pilot implementations, component architecture, project planning and deployment. Figure 3-1 shows the contribution of the Smart Grid roadmap in overall technology adoption for many utilities. For reference there are a number of good EPRI reference reports available to assist with these next steps. For example these two reports are useful references for cost benefit analysis[12].

---

[1] *Methodological Approach for Estimating the Benefits and Costs of Smart Grid Demonstration Projects*. EPRI, Palo Alto, CA: 2010. 1020342.

[2] *Estimating the Costs and Benefits of the Smart Grid: A Preliminary Estimate of the Investment Requirements and the Resultant Benefits of a Fully Functioning Smart Grid*. EPRI, Palo Alto, CA: 2011. 1022519.

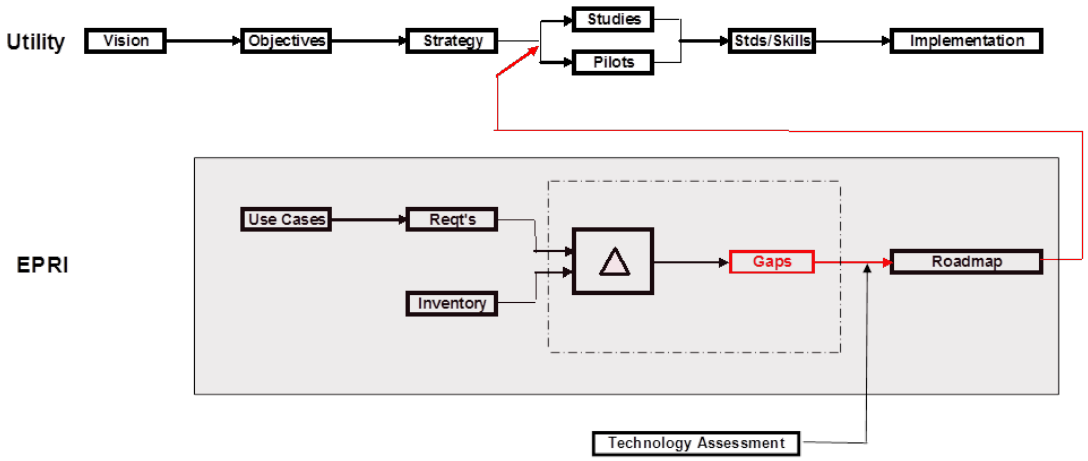


Figure 3-1
The Smart Grid Roadmap and Overall Technology Adoption Process

The Technology Adoption Strategy

Given that the role of the Roadmap is tied to the business objectives which will be partially defined based on the company's technology adoption strategy, this strategy is a key determinant in how (or even whether) a roadmap is developed. This strategy is established at the C-level. For example, in terms of the "S" curve, what is the utility's policy or practice in the pace of technology adoption (innovator, early adopter, early majority, late majority or laggard)? This decision is important and really guides the overall strategy. Figure 3-2 shows the challenge involved in picking the right time to invest in a given technology.

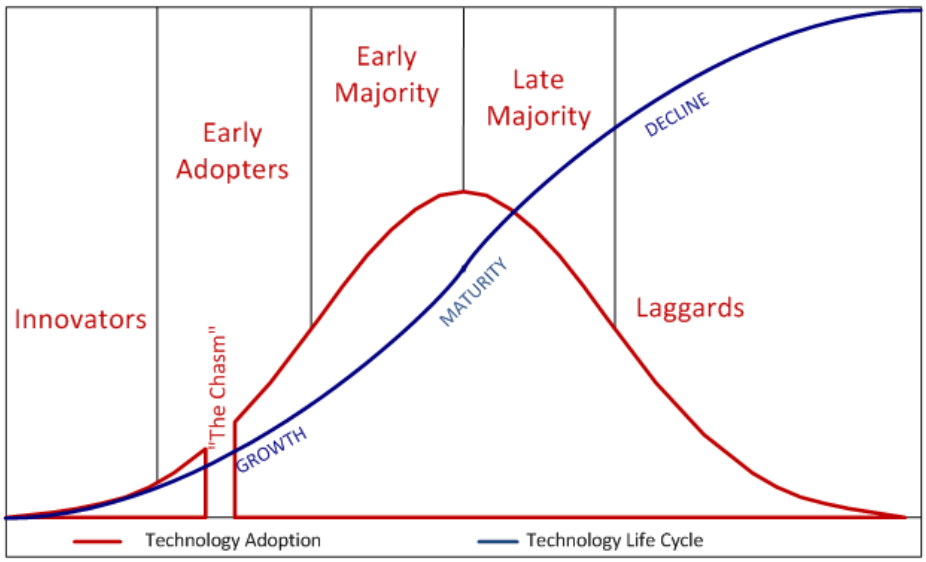


Figure 3-2
The Technology Life Cycle vs Technology Adoption Policy

Overall, technology adoption includes the following key elements

- Selecting new technologies through a procurement process requires robust vendor qualification and technology evaluation methods and metrics for proposal assessment.
- Full use of the external engagement, technology development, and system design is best suited to new or so-called "greenfield" procurements due to their comprehensive nature.
- Smaller implementations or incremental improvements to existing systems or technologies, or "brownfield" procurements, may need only certain aspects of these procurement tools.
- Systems design involves development of business and functional requirements, reference architecture, and trade-off analysis to develop a cost-benefit analysis.
- To assess the impact on existing infrastructure, legacy systems need to be evaluated for potential obsolescence or integration compatibility.
- The ability of an organization to adapt will be influenced by the level of initial expertise, the culture around organizational changes, and appropriate training on new systems.
- Implementation strategy may depend on the size and complexity of the system implementation with multiple approaches possible, including R&D, trials, pilots, partial rollouts, or full adoption.
- A maturity model scoring system can clearly translate utility priorities into vendor qualification criteria.
- Testing candidate systems prior to purchase ensures that business and technical requirements can be met.

The Value of Roadmapping

At its core, roadmapping is simply good planning. Business, technology and regulatory interaction related decisions are made as a fundamental part of the plan. The process itself leads to the creation of cross-silo teams that can more effectively identify the potential for realizing utility wide value and minimizing business risk through efficient implementation of corporate strategy. We can make the following additional observations on the value of roadmapping:

- A roadmap links regulatory policy, corporate business strategy, and customer needs with vendor, technology, and standards adoption decisions. Roadmapping allows a team to clearly relate planned features and system performance metrics in terms of value for the customer.
- As its name implies, roadmaps explicitly incorporate a time ordered string of events and actions. Roadmapping helps ensure that the team has access to technologies, personnel, best practices and other capabilities at the time they are needed to carry out the overall strategy.

- Roadmaps generally identify gaps in a company's technology evolution and adoption plan and organizational change management plan. These gaps become apparent quickly and can be addressed in a timely fashion.
- Roadmapping allows a disciplined approach to driver identification and prioritizing capital expenditures based on those drivers. At every step of the roadmap process focus is maintained on the basics of customer needs, regulatory compliance, institutional capability and technology investment. Cross-functional teams are lead to discover and implement the most important things first thus allocating time and resources in the most efficient manner possible.
- Roadmaps help set realistic targets for what can be accomplished in your organization given existing infrastructure, personnel, ability to adapt to and adopt new technology, and the regulatory environment. Realistic targets help build buy-in to the roadmap and underlying strategy and allow all stakeholders to see the positive results of the process.
- Roadmapping is an effective communication tool internal to the organization as well as externally for consumers, regulators, and vendors. Internally, a roadmap allows the team to clearly and consistently articulate the overall direction of the organization on many levels. It allows the team to send clear signals to the vendor community as to what technology is needed when hence reducing the risk of both vendors and the utility. Consumers and regulators also benefit by including them in the "value loop" – allowing this critical stakeholder community to comment early and often thereby reducing the risk associated with consumer disconnect and pushback that we have seen in other utilities in their grid modernization programs.
- Roadmaps also allow the team to see when a detour is required to act on external events and other unforeseen circumstances. Part of the process involves identifying risks along the way so the events that might require a change in direction are not a complete surprise.

The utility industry has developed a spirit of collaboration over the past decade that includes the sharing of use cases, best practices and now roadmaps. This approach is facilitating a much more efficient use of industry resources to address a wide range of issues that many utilities have in common. Common requirements result in multiple choices of vendors supplying the needed technology and allowing multiple parties to share the technology adoption risk. Identifying common elements of roadmaps across utilities offers further opportunities to manage risk, prevent reinventing the wheel, and gain more leverage over development plans in the vendor community.

The Primary Uses of a Roadmap

The following are the primary uses for a roadmap:

- Optimize the planning of technology investments
- Identification of important technology, standards and application areas not yet addressed

- Provide organizational direction and cross-cutting cooperation on the Smart Grid efforts
- Identify technical requirements for specific technologies, applications and standards
- Increase collaboration and cooperation between departments
- Energize the organization
- Identify business values, rules or specific risks associated with a technology
- Risk mitigation (see below for more detail)
- Identify key enablers for specific technology adoption
- Highlight immediate actions that may be required related to technology planning and adoption such as capability assessments, lab testing, other
- Develop and justify short term budget requirements
- Provide useful inputs to the next phases of business case development and architecture design.
- Technology life cycle management can be enhanced
- Identify "trigger scenarios" in advance for initiating the next step in the planning or stage gate technology deployment process
- Provide a template for evaluating projects already underway
- Define assumptions and sensitivities related to technology changes or investments
- Provide a starting place of requirements for reference when developing procurement specifications
- Identify specific issues, challenges and any impacts of delays related to specific technologies
- Enables the utility to discover the potential future impacts of technological change such as DER, EV
- Support the long term planning needed to achieve overall systems and data integration
- Can be a source of input for regulatory applications and general rate case documents

Other Uses for the Roadmap

A roadmap can also be used to:

- Organize technology investment options according to the directions established by the business objectives
- Run scenario planning as part of an overall strategic direction setting process
- Foster and encourage innovation

- Provide guidance and reference material related to standards development and other industry activities

Risk Mitigation

An important role for the Roadmap is the mitigation of risk. Business risk mitigation can be enhanced by identifying early, the potential impacts of technology change such as the adoption of distributed energy resources and electric vehicles. Technology risks exist in the adoption and deployment where the SGRM provides essential methodologies and principles such as the development of cross-functional requirements and recommends the use of interoperable standards to minimize obsolescence risk. The risk assessment matrix in Figure 3-3 below can form the basis for differing mitigation strategies. For example, a material investment in an immature technology will require a far more rigorous requirements development and technology assessment effort than a low volume implementation of a mature technology.

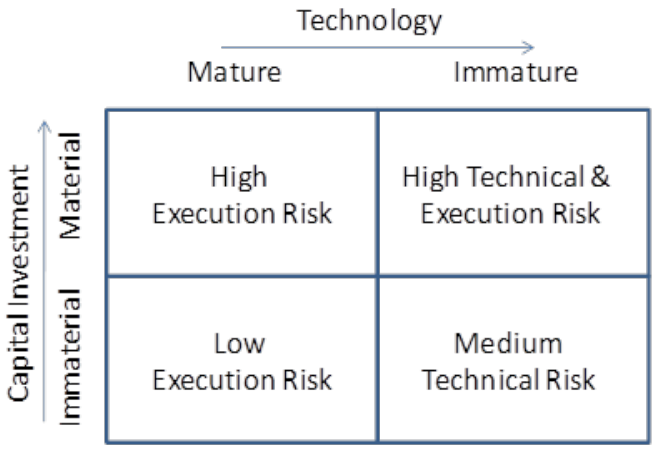


Figure 3-3
Risk Assessment Matrix

Section 4: EPRI Smart Grid Roadmap Methodology

This section provides a summary of the EPRI Smart Grid Roadmap Methodology (SGRM). Each of the eight Roadmaps referenced in this Guidebook were different for a variety of reasons including different; business objectives, policy and regulatory requirements, technology & communications infrastructures and objectives for the Roadmaps. Nevertheless the roadmap developments had a lot in common in terms of the overall process.

It can be said that the term "Roadmap" is as much over-used as the term "Smart Grid". When a term is over-used it loses clarity of meaning to the point of being a useless term. The other challenge is that there are many categories of roadmaps including:

- Strategic
- Technology
- Business
- Regional or Statewide
- Regulatory / Policy
- Vendor / product
- Implementation / deployment
- Standards (The NIST Standards Framework and Roadmap is an example of this)
- R&D (note the CA 2020 Roadmap is an example of this)

So what category are the EPRI Roadmaps? In developing the SGRM, we have found that a hybrid of the strategic, technology, business and implementation roadmap categories is optimal.

As the EPRI team implemented the Roadmaps, five key steps have been adopted for the SGRM; Vision, Requirements, Assessment, Planning and Roadmap Implementation. Within each step there are three or four recommended tasks however, depending on the Roadmap objectives, some tasks are optional. Drilling down further, each task is addressed by one or more possible task methodologies. The optimal methodology is selected depending on the client's

needs. For example, within the Assessment step there is a task called "Select Focus Technologies". For some Roadmaps the method used for selection involved scoring and ranking the technology by a relatively simple (and more subjective) method of impact and effort/risk. In other cases a more detailed scoring method was used. The SGRM is shown in Figure 4-1.

In identifying the task methodologies, the SGRM borrows from a number of other references sources such as the EPRI IntelliGrid Methodology [3] which has also been published by the IEC[4]. An excellent case study on the successful implementation of the IntelliGrid Methodology is included in this document[5]. A helpful additional resource that was written as a follow up to the original IntelliGrid Methodology document is an EPRI white paper that provides further guidance on standards on technology adoption[6]

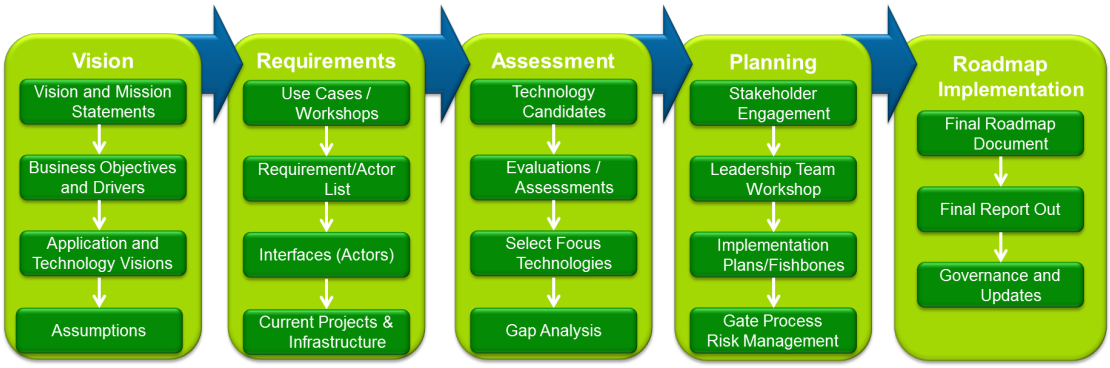


Figure 4-1
EPRI Smart Grid Roadmap Methodology (SGRM)

[3] EPRI Report: "IntelliGrid Architecture Application Guide: Metering and Consumer Systems"; Report 1013610, December 2006

[4] IEC PAS 62559 - " IntelliGrid Methodology for Developing Requirements for Energy Systems" - http://webstore.iec.ch/preview/info_iecpas62559%7Bed1.0%7Den.pdf

[5] "Designing the Future", Smart Grid Newsletter Case Study - Nov 2006 - http://www.smartgridnews.com/pdf/SGNCaseStudySCE.pdf

[6] EPRI White Paper: "A Utility Standards and Technology Adoption Roadmap"; October 2011

Vision

The Vision step starts with developing the company's Smart Grid Vision and Mission Statements. This is followed by obtaining or documenting the business objectives and drivers that relate to technology planning and deployment. Once the business imperatives are identified the next task is to make the initial selection of the applications and technology visions that will address them. This list of applications is used as an input for the selection of use cases in the next step. An application chosen at this stage may be a higher level application utilizing one or more technologies, standards and lower level applications. An example application at this step might be distribution automation selected to address a business objective of improving overall service to customers. Another approach may be the development of proposed technology vision statements that are more detailed and include a goal for stage of implementation and schedule.

Vision and Mission Statements

The Vision Statement

The purpose of a Smart Grid vision statement is to succinctly summarize the utility/ISO's goal to both leverage the existing and adopt new technologies and standards to address the applicable business objectives and drivers. Therefore the process of defining a vision statement begins with identifying and evaluating the essential business objectives and drivers that can be addressed by technology investments.

A vision statement is a summary of "what" the utility/ISO intends to accomplish and why.

The value of a vision statement lies in how it can serve to communicate widely within the organization the importance of the Smart Grid related initiatives to the success of the business. Well written vision statements can serve as the "elevator pitch" to help build identity and engagement across different departments of the utility/ISO. In terms of Roadmap development, a vision statement is useful in helping to ensure that the directions established in the Roadmap are consistent with the vision and objectives of the business.

The following are examples of vision statements:

- A power delivery infrastructure that enables integration of advances in communications, computing, and electronics to optimize system reliability, contain costs, and accommodate the delivery of services to meet the future needs of our customers.
- Energy delivery system automation will enhance and automate the control and restoration and provide real time situational awareness of the health, configuration, and utilization of the transmission, substation, and distribution infrastructure which will maximize availability of the energy delivery system to our customers.

- Smart Grid technologies, such as PMUs, energy storage and smart meters, applied from the transmission system to the consumers will enable the utility to operate the grid reliably, securely and efficiently and facilitate effective, open markets that engage and empower consumers while meeting the State's policy targets to integrate renewable resources, reduce greenhouse gas emissions, and secure energy independence.

The Mission Statement

The Smart Grid mission statement has a different purpose, mainly to provide a summary of the essential "how" the vision statement will be accomplished.

The value of a mission statement is similar to a vision statement in that it can serve as the "elevator pitch" to help build understanding and engagement across different departments of the utility/ISO. In terms of Roadmap development, a mission statement is useful in helping to ensure that the approaches or "hows" established in the Roadmap are consistent with those of the business.

The following are examples of mission statements:

- Plan and deploy a well-coordinated, inter-operable, cost-effective corporate infrastructure that will enable the development, integration and application of new technologies throughout the company that provide secure, high quality, cost-effective, reliable services both internally and externally.
- Leverage technology to proactively minimize the impact of, and with a long-term goal to eliminate, customer service interruptions associated with unplanned energy delivery equipment outages and to plan, maintain, and operate the system to achieve optimal levels of performance.

Developing the Vision and Mission Statements

Steps in the process of developing a vision and mission statement include:

- Ideally driven from the CEO or Executive/Senior VP level
- Alternatively it is necessary to engage them, at least for review and approval
- Must support the overall corporate vision
- Gather key artifacts such as regulatory requirements; government policy; corporate policy; stated corporate objectives; reliability, operating, maintenance and efficiency issues; economic opportunities, risk assessments and other potential future threats to the business.
- Rank the key elements according to opportunity, risk (impact times probability) to the business, the applicability of technology and standards to address
- Address the business objectives related to technology (see examples below)
- Address the drivers: internal, external, guiding principles (see examples below)
- Consider changes in capabilities if needed

- Include the intended time frame
- Describe the destination

Vision and mission statements are just one of the SGRM tasks used to help a utility address the business objectives and mitigate the drivers by succeeding in the effective adoption and implementation of technologies, applications and standards. Some utilities have elected to skip this task. The absence of these statements does not necessarily mean that the technology adoption will be hindered. Conversely, an effective statement can contribute only so much, so the time and effort allocated to developing the statements needs to be carefully managed.

Business Objectives and Drivers

A clear understanding of the business objectives and drivers is essential at this point in the Roadmap development. Any plan leading to investments in technologies needs to be grounded in the needs of the business. As with the task of developing a vision statement, we begin this task by gathering key artifacts such as regulatory requirements; government policy; corporate policy; stated corporate objectives; reliability, operating, maintenance and efficiency issues; economic opportunities, risk assessments and other potential future opportunities and threats to the business. Note that rate cases typically contain mandates and goals and strategies. These are the things that the company will be held accountable for. Most general rate cases include a policy section that actually lays out the technology strategy and two years in advance for a 5 year period. In terms of state and other regulatory policies and mandates, the California policies outlined in Chapter 3 provide good example. Finally compliance with NERC standards is required and can justify significant investments in some cases.

Business Objectives

Business objectives should include both key objectives that the business has for the technology investments and the objectives that are specific to the Roadmap itself.

Examples of business objectives related to technology investments are:

- Increase grid reliability, and efficiency and situational awareness
- Facilitate resource integration including renewable resources and distributed energy resources
- Implement and maintain physical and cyber security
- Faster and more informed operational and business decisions
- Reduced operations and maintenance costs
- Enhanced service to our customers and the ability to offer value-added services
- Widely deployed demand response to reduce peak demand

- Distribution grid management for system protection and restoration
- Condition based maintenance of key assets
- PEV integration to meet customer needs
- Reduce greenhouse gas emissions
- Meet or exceed all regulatory and policy mandates
- Safety

Business Drivers – Internal, External and Guiding Principles

To develop more detail around the business objectives and support mapping to applications, use cases and recommended technologies it is helpful to identify these imperatives in the form of drivers with internal and external sources. These drivers can then be easily mapped to technology visions, use cases and technology investment recommendations for future traceability. Example internal and external drivers are provided below. More detailed examples of drivers are provided in Chapter 2.

Guiding principles are the over-arching fundamental positions that the company has highlighted to support the effective adoption and implementation of technologies, applications and standards. Example Guiding Principles are also included below.

Example Internal Drivers:

- Availability / reliability
- Operational efficiency
- Asset utilization
- Aging assets
- Optimizing capital costs
- Real time grid situational awareness
- Cyber security
- Workforce preparation and readiness
- Cost recovery

Example External Drivers:

- NERC/FERC compliance
- Other state and federal policy and regulations
- Renewable Portfolio Standards.
- Consumer privacy
- Customer interface
- Peak demand reduction / energy efficiency

- NIST standards activities
- Environmental requirements
- Carbon reduction
- Integration of distributed energy resources such as residential solar, energy storage
- Energy efficiency
- Electric vehicles
- FCC spectrum options
- Power quality
- PJM market initiative
- Consumer acceptance and expectation

Example Guiding Principles:

- Business value (including cost recovery) – clearly established business value proposition for each project that supports the Smart Grid roadmap process that includes delineated cost recovery mechanisms
- Cyber security & compliance - incorporate best practices to deliver upon the capabilities of a Smart Grid, while establishing a highly secure architecture that meets all regulatory mandates.
- Architecture definition and best practices - continue to define and implement an open architecture infrastructure and framework based on industry standards and best practices. This will provide the foundation all future application integration and will protect these investments as technology changes.
- Standards selection and adoption – assess and adopt industry standards that support smart grid technology adoption and business drivers
- Effective data management, integration and interoperability – properly implement existing established standards that focus on the enterprise service bus, common information model and other interoperability standards.
- Technology selection - select architectures, technologies and standards to position the company to adopt and integrate new technologies in the future with optimal time and effort.
- Industry initiatives - consult industry best practices such as the NIST SGIP Working Groups and the GridWise Architecture Council and become involved in key industry initiatives to ensure the utility is in the best position to make informed technology decisions.
- Enterprise wide integration - ensure cross functional requirements are identified and system integration with all relevant applications is planned upfront for new technology investments.
- Leverage - to the maximum extent possible, leverage existing technology investments by integration.

- Workforce management – effective training, change management and application of the workforce as the transition to the future vision takes place.
- Ease of use – intuitive interfaces that require minimal training, easy to follow business processes that lead the user, self-evident applications.

Application and Technology Vision Statements

The initial set of high level applications chosen to address the priority business objectives. These applications are normally defined at a high level without stating specific references to technologies or standards. The application and technology vision statements are defined in the context of the business objective(s) or driver(s) to be addressed and must be able to be mapped to at least one business objective or driver. These statements will be used in the Requirements Step that follows to aid in the selection of use cases. Examples of application and technology vision statements are:

- We will deploy a range of standards based technologies to facilitate the integration of distributed energy resources on our distribution network.
- Establish secure, two-way, real-time communications links to all customers to support customer engagement and interaction.
- Implement a digital communications link to each critical transmission substation that allows secure communications to multiple substation devices on the same physical communications link.
- We will provide local and wide area grid awareness, intelligence and decision making capability to effectively conduct grid operations necessary to optimize power delivery performance in terms of reliability, power quality, and economy.

Assumptions

In some cases, documenting assumptions is a useful way of communicating to the rest of the organization, the basis on which the Roadmap is developed, the effort and support needed for a good Roadmap result and the key elements necessary for successful longer term technology adoption and deployment. Example assumptions can include cross functional participation, management support, guiding principles are followed.

Requirements

The Requirements Step starts with use cases including use case workshops. Once the use case titles and narrative are developed and the workshops have been held and documented, the next task is to derive the requirements and primary actors. As part of the workshops, it is recommended that the interactions between the primary actors be identified. This allows the documenting of the Actor Interfaces in the form of a bubble diagram. The final task for the Requirements Step is to identify the current projects and existing infrastructure. The IntelliGrid Requirements and Architecture development process is shown in Figure 4-2.

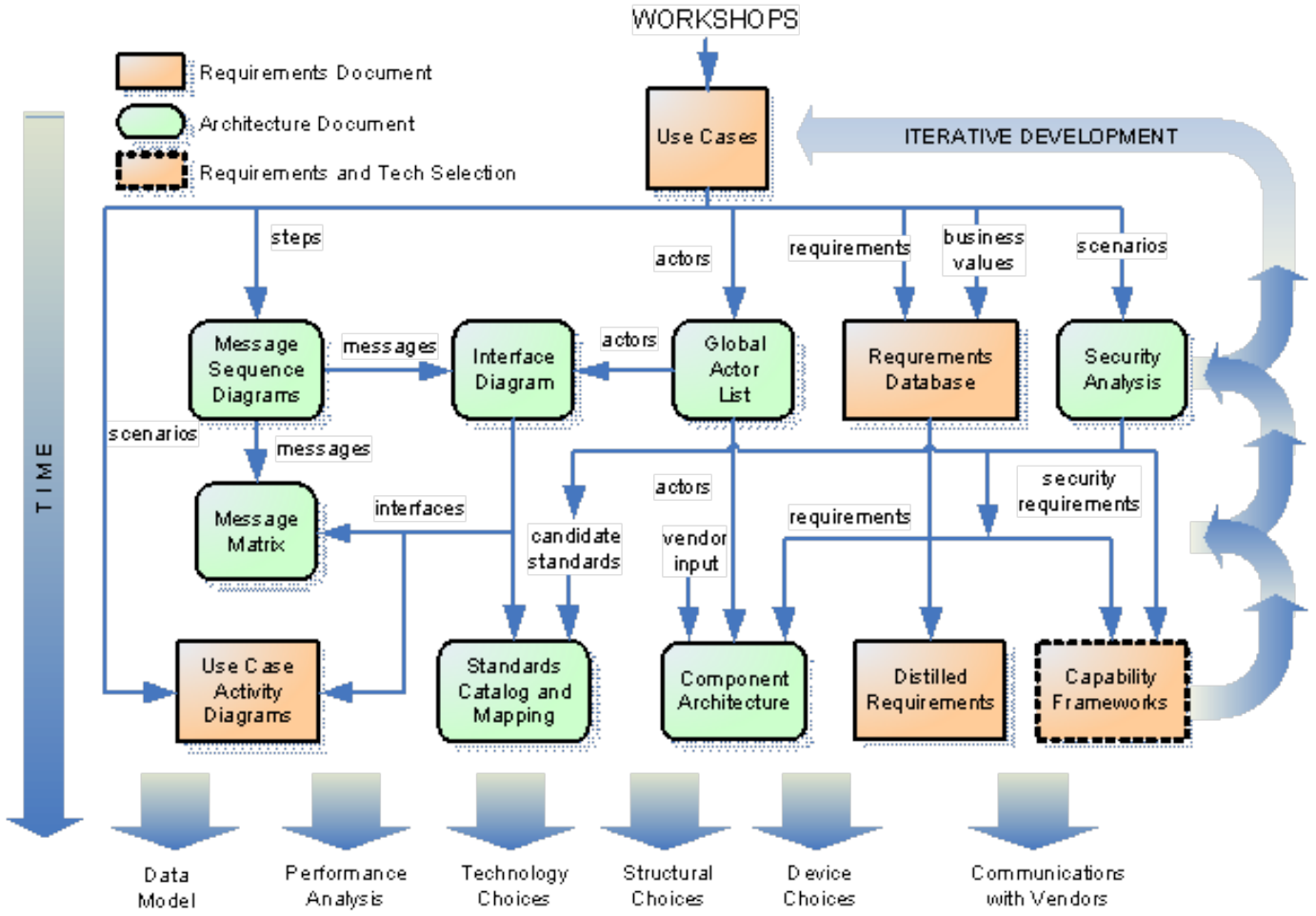


Figure 4-2
IntelliGrid Requirements and Architecture Development Process

Use Cases / Workshops

Use cases are a very useful methodology originated in other industries and tailored for use in the power industry as part of the EPRI IntelliGrid Methodology[7]. This methodology is applicable in a wide range of situations for technology adoption and deployment. In simple terms, if the technology being considered is proven or presents a low business risk or is planned for a minimal deployment over a reasonable time frame then a reduced scope use case approach is suggested. However if the technology being considered is new or presents a high business risk or requires a thorough cost benefit analysis or is complex or will interface with many other systems, and will be deployed in a large and costly program on an accelerated schedule, then a rigorous use case approach is strongly suggested. The detailed cross functional requirements development, risk mitigation, business value identification and life cycle benefits are invaluable. An excellent example of using this rigorous use case approach is at Southern California Edison[8].

The use cases developed for the Roadmaps referenced in this document are of the simpler variety with one or two scenarios with a primary purpose of identifying higher level requirements and the primary actors. This approach has served well for the Roadmaps and is recommended for the SGRM. However, in the instances where a roadmap leads to a large complex deployment, a rigorous and detailed set of use cases will be necessary.

In addition to the benefits mentioned above, many utilities have found that the cross functional engagement that is a part of the use case workshop and document reviews results in; greater cooperation between departments, in much improved requirements that can be used in the writing of procurement documents and can also result in identifying much higher business values.

It is helpful to note that a large number of excellent use cases have already been developed that are publicly available and can be used as reference material for new projects[9][10][11]. Some of these use cases are rigorous and detailed with multiple scenarios while some are higher level.

---

[7] IEC PAS 62559 - " IntelliGrid Methodology for Developing Requirements for Energy Systems" - http://webstore.iec.ch/preview/info_iecpas62559%7Bed1.0%7Den.pdf

[8] "Designing the Future", Smart Grid Newsletter Case Study - Nov 2006 - http://www.smartgridnews.com/pdf/SGNCaseStudySCE.pdf

[9] EPRI Use Case Repository - *http://www.smartgrid.epri.com/Repository/Repository.aspx*

[10] *Southern California Edison - http://www.sce.com/CustomerService/smartconnect/industry-resource-center/use-cases.htm?from=usecases*

[11] *NIST Interoperability Knowledge Base (IKB): http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/InteroperabilityKnowledgeBase*

Background on Use Cases

A use case is simply a "story" that includes various "actors", and the "path" they take to achieve a particular functional goal. By considering the actions of the actors working to achieve this functional goal, a completed use case results in the documentation of multiple scenarios, each containing a sequence of steps that trace an end-to-end path. These sequential steps describe the functions that the proposed systems and processes must provide, directly leading to the requirements for the given use case.

A selection of use cases with utility wide scope have been identified by the IntelliGrid Architecture Project. The IntelliGrid Architecture team organized the energy industry into six functional domains:

1. Transmission operations
2. Distribution operations
3. Distributed energy resources
4. Customer services
5. Market operations
6. Centralized generation

Referring to the SGRM, the selection of use cases follows the identification of the application and technology visions developed in the Vision step which are selected to address the business objectives and drivers. The EPRI team then uses the IntelliGrid and other reference use cases and narratives to identify specific use cases for the client. These specific use cases are chosen on the basis of the following criteria:

- Address business objectives and drivers
- Address application and technology vision statement(s).
- Present the most architecturally significant applications in terms of requirements.
- Have a high probability of being justified on the basis of improving reliability, access to asset and customer information, improved system performance and efficiency.
- The goals of the use case methodology as part of the SGRM are:
  - Collect all requirements that will have an impact on the architecture
  - Collect all requirements that will have a financial impact on the business
  - Identify the primary actors

Requirements and Actors List

Once the use cases titles and narratives are developed the following steps are followed:

1. A series of workshops and webcasts will be scheduled with representation from multiple stakeholder departments.
2. In preparation for the workshops the EPRI team will typically prepare workshop material as follows:
    a. Summary description
    b. Discussion topics
    c. Scope and assumptions
    d. Success scenario
    e. Actors

The EPRI team then facilitates the workshops by walking through the meeting material for each use case, asking questions, proposing possible solutions, informing of new and pending technologies and thoroughly documenting the contents of the meetings. In some cases steps are developed.

The information gathered during the workshop can include:

- Existing technology and communications infrastructure.
- Primary actors and interactions
- Technical requirements – Functional Requirements (FR) and Non-functional Requirements (NFR)
- Concerns and issues regarding the current system. This information will be used as part of the gap analysis developed in the Assessment Step
- Business requirements and potential business values
- Views on necessary and preferred new applications, requirements, characteristics, integrations and architectures.
- Current projects and technology pilots underway
- Regulatory, policy and tariff information that is applicable

The meeting notes are then documented and translated into functional requirements, non-functional requirements, business requirements, business values and primary actors with actor definitions. Figure 4-3 provides an example requirements list for a use case.

Actor/ Component	Reqt ID	FR or NFR	Requirement Description
Distribution Load Shed Application			
Communications System	1.0	FR	Communications system shall securely support reliable remote access from the Distribution Load Shed application to the substation relays controlling the breakers.
Communications System	1.1	NFR	All aspects of the communications infrastructure used to enable the Distribution Load Shed application shall comply with the Cyber Security Policy and applicable NERC requirements.
Communications System	1.2	NFR	All aspects of the communications infrastructure used to enable the Distribution Load Shed application shall be designed for a high level of availability.
Distribution Load Shed application	1.3	NFR	All software and hardware equipment used operate the Distribution Load Shed application shall be designed for a high level of availability.
Operator – TCC or ISO	2.0	FR	The Distribution Load Shed application shall accept input data from the TCC operator.
Operators – TCC and SOC	3.0	FR	The Distribution Load Shed application shall accept an initiation command from either/or the TCC or SOC operators.

Figure 4-3
Example Requirements List for Distribution Load Shed Use Case

Interfaces (Actors)

Primary actors (applications, equipment, staff) are identified and their relationship with other actors documented in the form of interface diagrams for each use case. Links between each actor are numbered. Figure 4-4 provides an example actor list.

Actor	Type
Operator - SOC	Person
SOC	System
Operator - TCC	Person
TCC	System
Reliability Coordinators / MISO	System
Bulk Power Marketing staff	System
DRAACS	Application
DLRC, TLRC	Applications
Planning	Person
OMS/CIS	System
Communications system	System
Communications processor and RTU	Device
Relays	Device
Customer	Person
GIS	Application

Figure 4-4
Example Actor List for Distribution Load Shed Use Case

Message sequence diagrams (Unified Modeling Language -UML format) can then be created to indicate the data/information movement between actors.

Information for each of the numbered links on the interface diagram can be documented to provide the utility guidance on the technologies, standards and communications performance that should be considered. Figure 4-5 below shows a typical interface diagram.

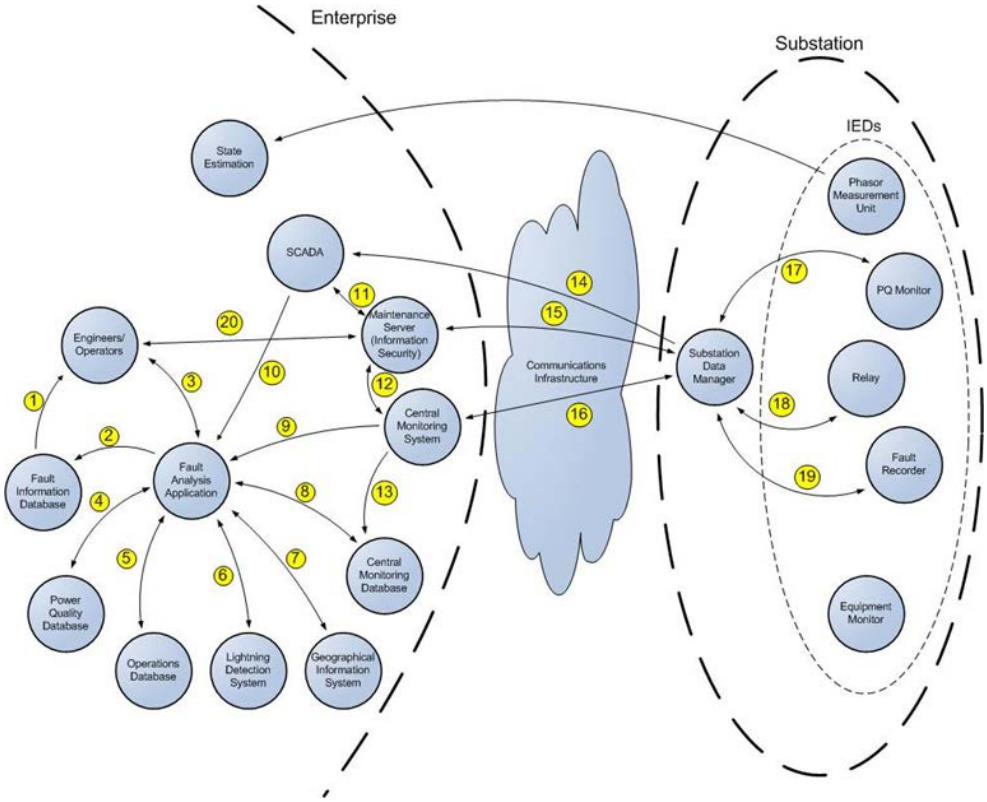


Figure 4-5
Typical Actor Interface Diagram

Current Technology Projects and Existing Communications & Technology Infrastructure

The documenting of the existing infrastructure along with known deficiencies is an important part of the SGRM. Understanding the current situation is essential in developing the gap analysis task in the Assessment step as well as the starting point (tail of the fish) for the implementation plans task in the Planning Step.

Assessment and Technology Selection/Mapping

The first task for this step consists of identifying the candidate technologies, applications and standards. Sources for this list include the NIST Standards

Framework and Roadmap[12], the SGIP Catalog of Standards[13], published industry technology roadmaps and discussion documents such as; the **Massachusetts Institute of Technology** (MIT) study on the Future of the Electric Grid[14], the Department of Energy, National Energy Technology Laboratory (NETL) Modern Grid reports[15] and the California Utility Vision and Roadmap prepared by EPRI[16] for the California Energy Commission. The next task is to evaluate each of the candidate technologies according to scoring and ranking criteria. This leads to the third task of selecting the focus (recommended) technologies, providing a visual means of showing the result. The final task is to prepare a gap analysis starting with the development an objective or vision statement for each of the focus technologies and assessing the current situation for that technology. These summary statements are used in the Planning step.

Technology Candidates

This list is developed by referring to a range of industry sources as noted above. It can also be useful to map the technologies by domain as shown in Figure 4-6 below.

In some cases, at the request of the client, the EPRI team has provided a pre-screened list of recommended technologies.

A wide range of methods are used in the industry to evaluate candidate technologies, applications and standards. The method and criteria should be selected based on the needs of the utility but should be as broad as possible.

---

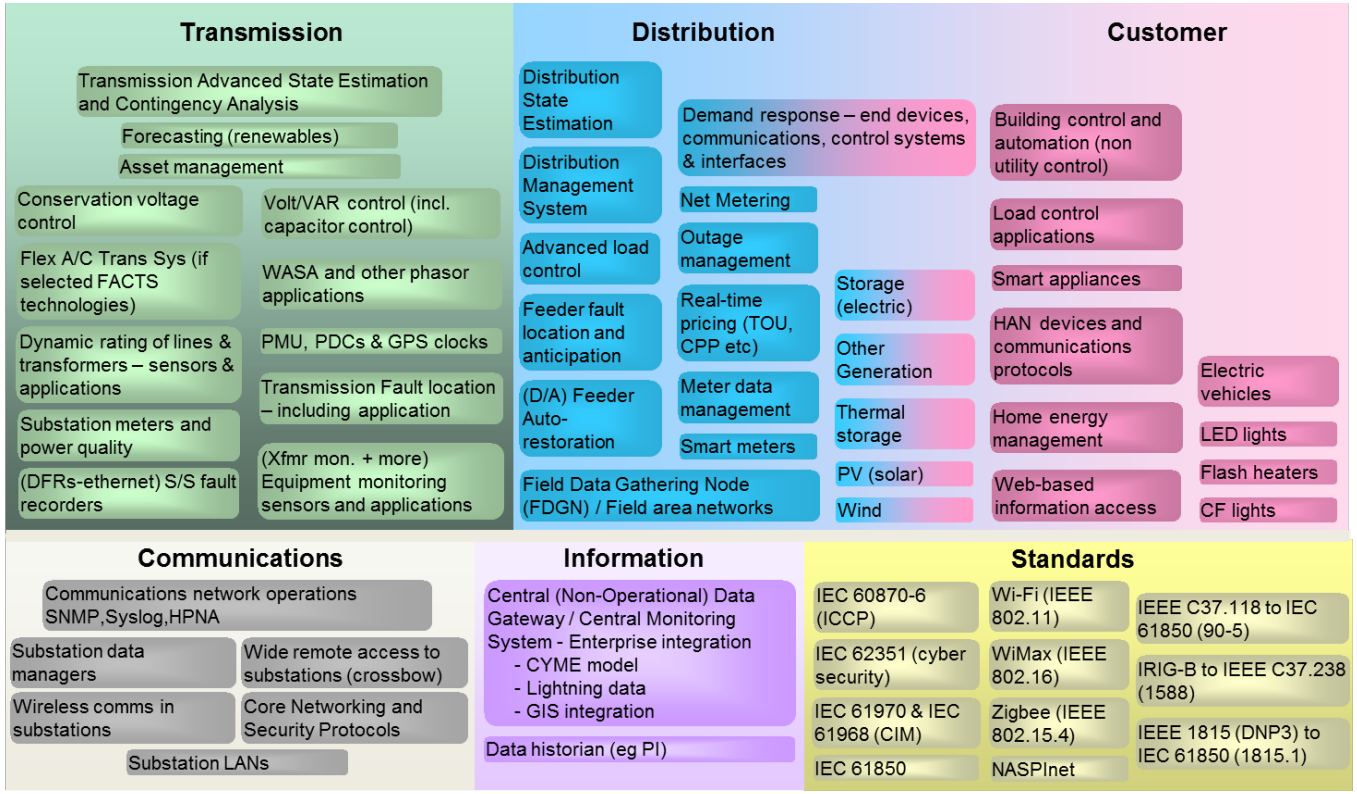
[12] NIST Standards Framework and Roadmap, Release 2.0, February 2012.

[13] SGIP Catalog of Standard: http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/SGIPCatalogOfStandards

[14] The Future of the Electric Grid, an Interdisciplinary MIT Study, December 2011

[15] A Compendium of Modern Grid Technologies, NETL Modern Grid Initiative, June 2007

[16] California Utility Vision and Roadmap for the Smart Grid of 2020, prepared by EPRI for the California Energy Commission, July 2011



Source: EPRI

Figure 4-6
Key Technology Domains for the Smart Grid

Evaluations and Assessments

Detailed Technology Assessment Criteria

A highly ranked technology or standard will clearly exhibit one or more of the following:

- A key enabler for a Smart Grid vision
- Encouraged by a regulatory authority
- Addresses a safety concern or risk
- Essential in maintaining or substantially improving reliability
- Provides a substantial improvement in operational or energy efficiency
- Yields a significant cost reduction
- Addresses an important strategic or business need. Includes risk mitigation.
- Supports a large enhancement in customer satisfaction

A highly ranked technology or standard will exhibit a minimum of:

- Life cycle cost to install and maintain
- Technology maturity risk (includes risk of a lack of wide adoption by the industry)
- Work-force skill challenges and training
- Obsolescence risk
- IT integration and management issues
- Customer acceptance risk
- Regulatory concerns
- Effort to understand or apply the resulting information or data

Typical Standards Assessment Criteria

The following criteria are highly applicable to evaluating communications standard and as such are used in the Communications Technology Assessment in the Annex of this report:

- Level of Standardization - Who recognizes it as a standard?
- Level of Openness – How easy/costly is it to obtain and use?
- Level of Adoption – How widely used is it now? In the future?
- Users' Group Support – Does someone promote it? Improve it? Test it?
- Security – Can it be secured? Is it inherently secure?
- Manageability – Can you control, monitor and/or upgrade it remotely?
- Scalability – Will it work when deployed at a large number of sites?

- Object Modeling – Does it group and structure data?
- Self-Description – Can it automatically configure and initialize itself?
- Applicability:
  - to the Power Industry – was it intended for use here?
  - to the Consumer Area – e.g. metering, building automation?

A Simplified Approach for Technology Evaluation

This higher level approach scores each technology according to two key criteria; impact and difficulty. Scores can be assigned from 1 to 10 (where the higher number is most favourable). This requires that there be an agreed to definition for these terms. The following are typical definitions:

Example Definition: Impact

- Operational reliability & improvements
- Increased customer satisfaction
- Deferred cost of resources
- Efficiency
- Multiple benefits enterprise wide
  - Growth management
  - Politics
- Mitigate rate increases
- Risk Mitigation
- Minimize/avoid negative PR

Example Definition: Difficulty

- Cost
- IT integration
- Ease of interpreting information
- Maturity or capability of technology
- Risk of obsolescence
- Regulatory concerns
- Customer relations (acceptance)

Once the scoring is completed, the technologies being evaluated can be placed on a grid such as that shown in Figure 4-7.

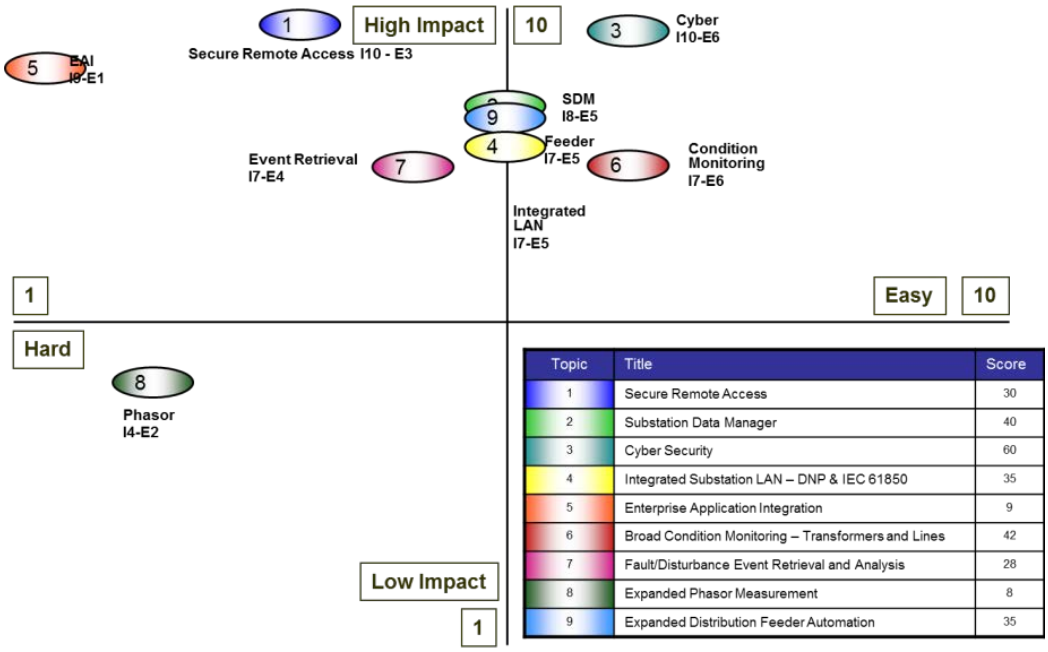


Figure 4-7
Impact vs Effort Matrix (Team Score)

Technology Capability Model

Another evaluation method is referred to as the Technology Capability Model. This method lends itself to a detailed analysis of a specific technology or device. The detailed list of needed capabilities is best derived from the requirements derived from a detailed use case. An example of this approach is shown in Figure 4-8.

Latching Relay Device (Disconnect Device)

Maturity Level	Customer Reset Options	Commercially available & in use now (>10,000 units)	Current limiting with Flexible Set Point Handling	Current Limiting capabilities	On/Off disconnect	Voltage sensing	200 Amp Rating	Integrated device	Collared Solution
5	X	X	X	X	X	X	X	X	
4		X	X	X	X	X	X	X	
3			X	X	X	X	X	X	
2				X	X	X	X	X	
1					X	X	X	X	
0									X

Figure 4-8
Technology Capability Model

Select Focus Technologies

Once the above assessments are completed, the utility's Smart Grid Roadmap team, with facilitation by EPRI, is in a position to select the top candidate technologies, applications or standards for further focus. Upon selection, a new vision or objective statement is developed for each of the focus technologies. This statement will be used in the development of the gap analysis as well as the implementation plans.

Gap Analysis

Once the focus technologies are selected and the objective statements are developed, the next task is to assess the current status, issues, concerns, degree of deployment, plans underway for that technology. The simple form gap analysis is then assembled by comparing the current situation to the objective statement for each focus technology.

Planning for Implementation

Once the focus technologies are selected or a short list has been developed, the tasks in the planning step can be addressed. The first of these is to reengage key stakeholders, especially the subject matter experts to ensure that all needed input is received. The same stakeholders may be key contributors at the Leadership Team Workshop. The next task for the planning step is the development of the Ishikawa diagrams based on gap analysis for each technology. The final task is the revisiting of the technology adoption gate process which is an excellent method for managing risk.

Stakeholder Engagement

The first task of the planning step is to ensure that all stakeholders for a possible technology decision have the opportunity to have input in aspects of the decision. This step is optional but highly recommended. This can also be an opportunity for the subject matter experts, knowledgeable in the area of the technology, to assume ownership of the selected technology for the next tasks. These individuals can present the needed material to the utility's Smart Grid leadership team. The same individuals are central in the development of the Ishikawa diagrams for each of the selected technologies.

Leadership Team Workshop

This is optional task of presenting the Roadmap findings to date to the utility's Smart Grid Leadership team for validation. This task, if successfully completed, can have a significant impact on the successful adoption of the technologies. Possible outcomes of this workshop could be: approval to proceed to the next stage of adoption (per the Stage Gate process described below), approval to spend $$ for short term, broad cross functional support for a program.

Implementation Plans and Ishikawa (Fishbone) Diagrams

The development of the Ishikawa diagrams occurs with close interaction with the utility's subject matter experts and starts with the outcome of the gap analysis for each technology. Refer to Figure 4-9 for an example fishbone diagram. The objective statement is placed as the head of the "fish" in green. The current situation is placed as the "tail" of the fish in yellow. The actions needed to move from the current situation to the objective are described in the blue boxes.

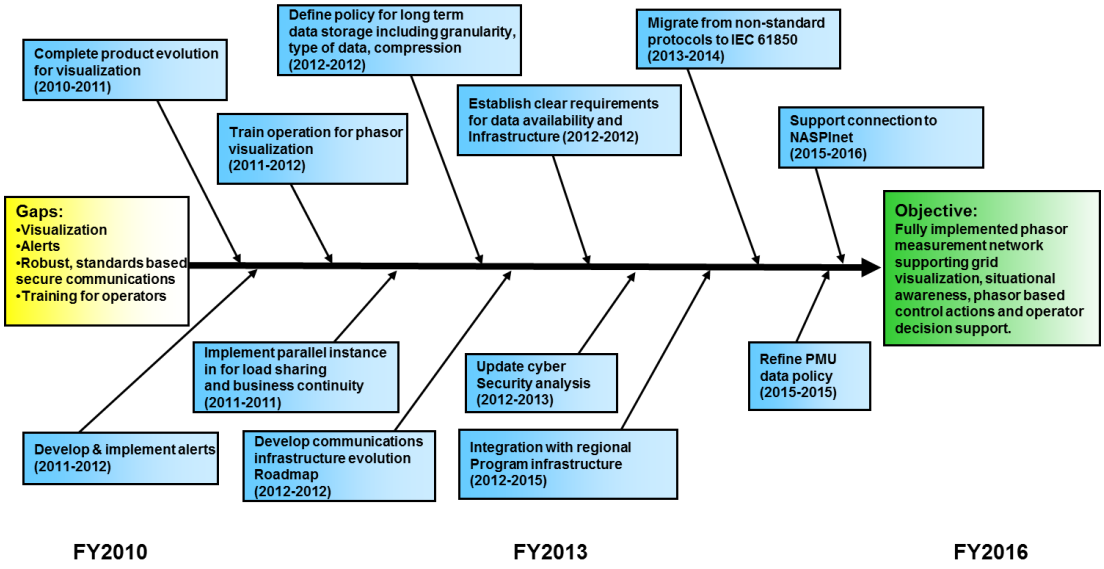


Figure 4-9
Example of Ishikawa Diagram (Fishbone) Showing Gaps and Objective

Gate Process and Risk Management

The last task for the Planning step is the management of risk by revisiting the technology adoption gate process which is an excellent method for managing risk. The discipline of having to meet a pre-determined set of detailed criteria before moving to the next stage is an excellent way of engaging a wider audience and managing risk. See Figure 4-10 for an example diagram.

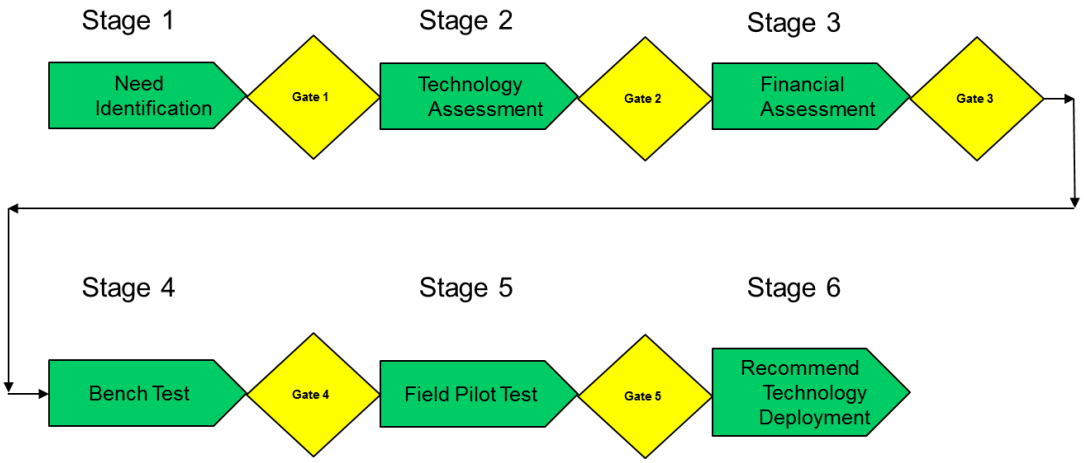


Figure 4-10
Example of a Technology Adoption Stage Gate Process

Roadmap Implementation

This is the now the home stretch for the Roadmap development. At this point a lot has been accomplished. This final step needs to capture all the tangible results and leverage the intangible impact such as cross departmental cooperation that may have resulted. The final report out is usually provided to multiple groups for maximum impact on the organization. It is also important to note that the Roadmap development should not be considered a static result but it far more useful if it kept up to date through periodic refresh cycles. Experience has shown that the leadership and governance capabilities of an organization are by far the biggest determinants of the impact of a Roadmap development.

Final Roadmap Document

This task is the final reviews, editing and publication of the report.

Final Report Out

To ensure the largest possible benefit is derived from the Roadmap effort, the final report presentations need to be delivered to three key sets of stakeholders. Those key presentations should be to the following:

- The C level sponsor or the Smart Grid Executive Oversight Committee.
- The Smart Grid Technology Steering Committee
- Director, Manager, Engineering and other staff stakeholders

Governance and Update of the Roadmap

Experience has shown that the leadership and governance policies and capabilities of an organization are by far the biggest determinants of the degree of impact of a Roadmap development.

Establish a Visible, Long Term, Roadmap Leadership Team (RLT) with C-Level (VP or higher) Support.

One of the most effective steps an organization can take is to implement an effective leadership team with strong visible support by an executive sponsor. The RLT team should have a clearly stated mandate and responsibility to drive long term technology change at Duke. The RLT team, as part of its mandate, should develop and maintain a governance model with project audits required to ensure compliance. Project teams appointed to implement the various selected technology programs may dotted-line report to the RLT. Periodic updates of the Roadmap document may also be the responsibility of the RLT team.

Develop a RLT Governance Model

A governance model can be a key tool for the RLT to both define integrated technology requirements and communicate expectations to a broad project audience. Key elements for the governance model should include:

- Investment expectations
- Requirements development process
- Standards participation
- Integration standards
- Policies & guidelines
- Technology maturity evaluation
- Pilot program approach
- Audit requirements

Developing Personnel Skills to Support Infrastructure

New skills are required to support an intelligent grid. Engineers, technicians, and other staff need to have experience with computer systems, electronic equipment and controls, and information processing in order to perform their fundamental duties.

It is very important for the workforce needs to be identified early in the pilot projects and confirmed or adjusted based on the results of the pilots. These needs to be identified as early as possible because of the long lead times required to implement changes in workforce skills.

Participation in Standards and Industry Groups

It is highly advantageous for an organization to be engaged with key and relevant industry activities. Participation enables the organization to proactively have input on key directions for the industry and remain abreast of changes that may have a direct impact on the company. Important industry and standards activities are summarized here:

- Smart Grid Interoperability Panel (SGIP)
  - Priority Action Plan (PAP) Working Groups
  - Domain Expert Working Groups
- IEEE Power and Energy Society
- International Electrotechnical Commission (IEC)
- DNP Users Group
- UCA Users Group – provides access to ongoing information in many of the required areas of development:
  - IEC 61850
  - Common Information Model (CIM)
  - OpenAMI and UtilityAMI (may be out of scope for this project but others should attend)
- North American Synchrophasor Initiative (NASPI)
- EPRI Smart Grid Workshops

Managing the Progress towards a Smart Grid

The process of implementing new technology through pilots and then expanding to full deployment provides a model for managing the overall implementation of the smart grid. Each pilot project should be structured to provide important feedback and links to overall objectives:

- Manpower and skills requirements for implementation so that requirements for full deployment can be determined
- Technology performance and limitations. Recommendations for improvements, modifications.
- Additional development needed.
- Integration requirements (where the technology fits into overall smart grid objectives and benefits)
  - Communications (infrastructure sharing opportunities, standards)
  - Information systems (applications that can take advantage of the technology)
  - Control systems (real time applications)
  - Asset management
  - Workforce management
- Issues with expansion, full deployment that need to be addressed
- Installation issues
- Reliability/maintenance issues
- Documentation adequacy, needs

Monitoring Progress Toward the Vision

The implementation plans provided in the roadmap illustrate the initial recommended steps to achieve the company's Smart Grid vision through technology adoption. The charts illustrate a time line for implementation that can be used as a dashboard for tracking progress.

Modifying the Roadmap Based on Technology Assessments and Trials

The task statements themselves and the timelines for achieving them may need to be modified as the assumptions in developing them get changed as a result of the lessons learned during technology demonstrations. This is a key output of each demonstration project which then benefits the overall program in terms of progress towards the task statements.

Section 5: Roadmap Summaries

The following individual summaries describe the unique aspects of each Roadmap development. Summaries are included in the following order:

- California ISO
- California 2020
- Duke Energy
- Southern Company
- SRP
- TVA

Roadmap Summary - California ISO

With the significant opportunities and challenges facing the California ISO (ISO) driven by California energy and environmental goals and emerging technologies that are expected to be proven essential in meeting these goals, the ISO engaged EPRI to provide input and guidance in developing a Roadmap for Smart Grid related technology investments including reviewing the objectives, required elements, recommendations, and implementation plans for California ISO's Smart Grid Roadmap. A series of workshops and independent stakeholder and subject matter expert (SME) interviews were conducted covering a variety of critical and challenging operations scenarios. This brief summary outlines the key processes that were utilized, a compilation of unique California ISO issues and recommendations, a technology assessment and ranking process, and other related conclusions and recommendations.

As with most Independent System Operators, the California ISO had plans to invest significantly in communications infrastructures and a wide range of technologies to address corporate objectives for grid reliability, regulatory compliance, operating efficiency, market operations, cyber security, renewables integration, system integration and asset utilization. The California ISO corporate mission is as follows: "For the benefit of our customers, we operate the grid reliably and efficiently, provide fair and open transmission access, promote environmental stewardship, and facilitate effective markets and promote infrastructure development, all through the provision of timely and accurate information."

The Roadmap effort objectives flowed directly from the ISO's corporate mission and included:

- Increase grid transparency, reliability, and efficiency
- Facilitate resource integration including renewable resources and distributed energy resources including demand response
- Implement and maintain physical and cyber security

Planned uses for the Roadmap included supporting a number of internal and external needs including:

1. Input to Smart Grid project funding and project prioritization internally and externally
2. Identification of important technology areas not yet addressed
3. Long-term Smart Grid project planning tool
4. Foundation for public Roadmap document
5. Provide ISO perspective and requirements to standards development and other industry activities

To develop the Roadmap, the EPRI team utilized the IntelliGrid methodology through use cases and associated workshops to discover the most important system requirements and technologies (referred to as the architecturally significant requirements) necessary to implement selected Smart Grid functions and applications at the ISO over time.

A result of the Roadmap development process was the identification and ranking of several ISO relevant technology themes. The ISO team then selected and ranked these projects based on their expected positive impact and the level of effort to implement. The process resulted in the determination of key application benefits, identification of prerequisites, difficulty of implementation, the technologies required, the applicability of various Smart Grid functions to business objectives, and the development of suggested implementation timelines.

As an outcome of the use case workshops and follow up discussions, five technology focus areas were further defined. The ISO team provided the definitions for "Benefit" and "Feasibility," and then ranked the five themes to arrive at a prioritized list of technology theme statements. Criteria for the ranking matrix on "Benefit" and "Feasibility" were taken from the ISO's existing Project Management Office (PMO) tools used for ranking other internal project priorities.

Expected benefits arising from grid system integration included: better cyber and physical security management, wider selection of a broad range of products and applications with more features and pricing options, and minimized costs (integration of enterprise and other applications, operations and maintenance savings, capital investment deferments or reductions, installation and related costs for new systems, and upgrade of existing applications and systems).

California ISO's key infrastructure to support ISO market operations includes the following areas: Market Input Applications, Market Applications, Grid Applications, Metering, and Communications. Bearing these in mind, the Roadmap Team identified and investigated five primary use cases and recorded recommendations for each as follows:

1. Demand Response Providers Adjust Consumers' Energy Consumption in Response to ISO Dispatch Instructions: The purpose of this use case is to describe how the ISO should provide dispatch signals to the Scheduling Coordinator (SC) for bids against their portfolio and generated through the ISO market software for demand response participation.
2. ISO Publishes an Indicator of Grid Conditions with Expectations Consumers Will Adjust Usage: The purpose of this use case is to describe how the ISO should provide an indicator of grid conditions to provide information about needed action by end users or devices.
3. Non-Dispatchable Distributed Energy Resources (DER) Changes ISO Forecast and Unit Commitment Decisions: The purpose of this Use Case is to describe how the California ISO uses information about Non-Dispatchable Distributed Energy Resource (DER) to modify the ISO's system load forecast.
4. ISO Uses Synchrophasor Data for Grid Operations, Control, Analysis, and Modeling: The purpose of this use case is to describe how the ISO uses synchrophasor data for grid operations, control, and modeling.
5. ISO Uses Energy Storage for Grid Operations and Control: The scenarios that should be described in this use case document should support using energy storage for grid operations and control concentrating on the use of energy storage for ancillary services, supplemental energy bids, energy shifting and for transmission loading relief.

As an integral part of the use case methodology, the requirements development process was undertaken using the California ISO technical team facilitated by EPRI. As a further outcome of the use case workshops, the EPRI team and California ISO staff defined five proposed technology themes or focus areas. The California ISO team then defined the definitions for "Benefit" and "Feasibility" and ranked the five themes to arrive at a prioritized list of technology theme statements and recommendations as follows.

1. Phasor Measurement Gathering Recommendation: Establish comprehensive requirements addressing all aspects of phasor data collection and communication in cooperation with the utility equipment owners and Western Electricity Coordinating Council (WECC). Increasingly, phasor data should be used for critical operational applications and decision making. Therefore the requirements should include hardened network components, detailed service level agreements (QoS) where applicable, cyber security, availability, protocol and other standards.
2. Advanced Forecasting Recommendation: As California approaches the state legislated renewable generation targets of 20% of energy usage by 2013 and 33% by 2020, the impact of both variable resources and loads (PEVs) on ISO

operations should continue to grow. ISO Operations should enhance its operational tools to provide advanced capabilities for situational awareness and economic dispatch optimized for more volatile grid conditions. Advanced forecasting is one of these tools and includes: forecasting renewable resources, sub-regional load forecasts, along with availability of emerging demand response resources.

3. Advanced Grid Applications Recommendation: Advanced grid applications working in conjunction with other key applications such as advanced forecasting, external entities supplying data, field data sources, and the communications infrastructure should be essential in providing ISO's staff with the ability to maintain system reliability in the midst of significant change, while facilitating effective market services. The ISO must continue to evaluate and implement the voltage stability analysis (VSA) and dynamic stability analysis (DSA) applications already planned and in process.
4. Cyber Security Recommendation: The ISO should expand its cyber security policy to include application layer security to address this growing area of vulnerability. Also, new policy elements addressing data integrity on the basis of data source and class should be developed. Evaluate, with the intention to adopt, the new DNP3 (Secure Authentication), IEC 62351 & IEEE 1686 standards when judged to be mature. Expand the policy to address centralized authentication management. Applications for centralized automated compliance management products available for use in control systems should be investigated and implemented.
5. DER Enabling Recommendation: Enabling distributed energy resource (DER) participation in the ISO market requires that ISO adopt a robust and flexible system architecture that builds upon recent Market Redesign and Technology Upgrade (MRTU) design. Guiding principles from industry organizations such as the GridWise Architecture Council (Smart Grid Framework) and Open Access Same-time Information System (OASIS) (Service Oriented Architecture, SOA) should be adhered to. When possible, web based services from Internet Engineering Task Force (IETF) -based Requests for Comments (RFCs) and OASIS standards should be used for information exchange (e.g., TCP/IP) and data definitions (i.e., Open ADE). This current and future architecture description was developed by the ISO Team and provides the foundation for the overall Roadmap plan.

Key Technology Recommendations included defining several critical principles that should be instrumental to the future success of California ISO Roadmap programs and investments as they evolve. These best practices principles were:

- Continue to define and implement an open architecture infrastructure and framework based on industry standards and best practices. This should provide the foundation for all future application integration and should protect these investments as technology changes.
- Select architectures, technologies, and standards to position California ISO to adopt and integrate new technologies in the future with optimal time and effort.

- Consult industry best practices, such as the NIST SGIP Working Groups and the GridWise Architecture Council, and become involved in key industry initiatives to ensure the California ISO is in the best position to make informed technology decisions.
- Ensure cross-functional requirements are identified and system integration with all relevant applications is planned upfront for new technology investments.
- To the maximum extent possible, leverage existing technology investments by integration.

The individual studies and pilot efforts identified provided the basis for evaluating and understanding new technologies that can become part of the integrated architecture as well as verifying the economics and work force requirements for larger deployment of the technologies.

The ISO architecture vision allows each network service (software designed to do a specific job) to operate individually but share information with other services all through a base system using service oriented architecture (a collection of services that make up a network system). One key architectural component is a centrally managed network model. The Enterprise Model Management System (EMMS) that the ISO planned to implement should centralize the functions of several current ISO services and significantly reduce the time between network model updates — it currently can take up to three months to get any changes into the network model.

A critical determination of the workshop and use case processes was the importance of Governance in organizational buy-in and long-term implementation. The ISO had an existing successful Governance structure and leadership model in place for managing all strategic initiatives. The Roadmap was immediately integrated within this structure. Each strategic initiative within the ISO has an Executive Sponsor, Initiative Owner, Initiative Manager, and a host of Project Managers. The Roadmap and its recommendations were treated as potential projects as part of the CAISO System and Tools Initiative for the corporate distributed energy resources (DER) initiative. This approach ensures immediate Governance with a proven governance and leadership team. Furthermore, each initiative has a steering committee responsible for shaping the scope of future work as well as continually assessing progress of current activities.

Additional key elements provided through the Governance included: standardized investment expectations, **Maturity Model Integration**-based system lifecycle processes, robust policies & guidelines, routine technology maturity evaluation, consistent pilot program approach, and quality assurance requirements.

In conclusion, the California ISO plays a key role in the reliable operation of the California power grid and the efficient operation of the market systems and services. The ISO faces an unprecedented combination of policy, regulatory, and technology change in addition to new categories of risk such as cyber security.

To effectively address these challenges the ISO must implement a wide range of technologies, standards, policies, and practices that the Roadmap identified and that are available today as well as a number of options for the future. The Roadmap also provided proposed implementation plans for the key recommended technology themes.

Epilogue: The following is a brief synopsis of selected follow-up feedback (personal opinions given and not speaking for California ISO) after allowing for the lapse of sometime from the Roadmap's completion and circulation within the organization.

Regarding the usefulness of the Roadmap process and use cases completed, the ISO achieved its initial objectives. The Roadmap helped clarify the benefits of the Smart Grid to the California ISO, and it is referenced in their Annual Report. The Smart Grid Roadmap supported a number of internal and external needs which included:

- Input to Smart Grid project funding and prioritization
- Identification of important technology areas not yet addressed
- Long term Smart Grid project planning tools
- Foundation for public Roadmap documentation
- Provide an ISO perspective and industry requirements to standards development and other industry activities

As a result of these efforts, ISO staff now has a better understanding of Smart Grid technologies and how they can be of benefit to California. At a high level, the benefits from the identified applications and activities were realizable. In addition, the workshops positioned staff to participate in policy discussions, as well as regulatory, environmental, customer response, net metering, and other pivotal issues. The entire process was essentially an intense educational workshop where one could begin to understand what was possible and to understand the whole 'big picture' around Smart Grid technologies and applications and how to move forward in a planned and methodical manner. It was especially helpful in educating and orienting new staff. Other benefits of the process included the generation of a Roadmap plan to realize how the ISO could use these benefits. Although the use case process was not formally used internally, an unexpected benefit had been applying both the process and Roadmap lessons to other projects. The Roadmap also had direct impact on how the ISO's Advanced Grid Technology Center (public area) was designed for visitors. Other internal applications of the Roadmap have included: DR and standards, energy storage, electric vehicles (EV) and micro-grids, energy forecasting and DG, potential plans to add someone on advanced technologies.

In hindsight, because of the different levels of internal staff Smart Grid knowledge and experience, it would have been helpful to bring in more experts to teach the foundational technology and provide technology workshops to reduce the unexpected resource load that ended up being required. Additionally, more time on scoping, assumptions, defining success upfront, expectations, and

budgets was required than originally scheduled. California ISO could have presented options for additional workshops and/or more appropriate content if more up-front transparency in the process had existed. For example, additional expertise could have been provided during a use case if a tutorial workshop had directly preceded it.

One suggestion for presentation of use-case results was that the four-box matrices were more effective than the fishbone diagrams (content was good, but the format sometimes problematic). Note California ISO currently uses fishbones for root cause analysis (Duran Quality Improvement), but this was a different application of the technique.

A final suggestion to minimize organizational impact would be to 'package' completed use cases from other companies as a starting reference for technology, standards, and methods to learn what others have done, whereas new use-case processes were sometimes cumbersome before cross-functional teams were up to speed and fully engaged. However, after the use case learning curve was mastered, California ISO is now considering performing several other use cases including DR and forecasting methods. In general, it would be helpful to provide effective reference methods, standards, technologies, and descriptions for those people who do not intend to do an entire Roadmap so that they can still learn from others and leverage these previous Roadmap outcomes.

Finally, regarding ISO Governance and leadership, the Roadmap was strongly supported both before and during engagement, and the ISO has a culture that is supportive of strategic activities. The Roadmap is used quite frequently, however some people felt additional pressure since the process required incrementally more effort and unplanned time. Interestingly, the Roadmap structure assisted California ISO in making structural changes that more effectively positioned the organization.

The public version of the Roadmap is frequently cited and used, whereas the internal (more detailed) version is not used currently. Given staff turnover, some continuity and familiarity tends to be lost since the new people are not familiar with the Roadmap and methodology. The California ISO Governance model is robust and includes: strategic initiatives, rankings, strategic value, risk mitigation, and business case justification. California ISO executive support has been excellent and was well aligned before the Roadmap effort started. The Governance structure is one of the most critical requirements to the overall usefulness of the Roadmap outcome as well as its effectiveness in describing challenges and finding solutions. California ISO leadership has indicated that a refresh Roadmap is likely in 2013.

Roadmap Summary - California 2020

EPRI, PG&E, SCE, and SDG&E with assistance from The California Energy Commission Public Interest Energy Research (PIER) Program undertook developing a ten year plan for California's Smart Grid Roadmap in 2011 looking forward to 2020. This report outlines the key drivers, findings, and going-

forward recommendations required to achieve California's 2020 Vision. The Roadmap described in this report represents the California utility vision of the technical infrastructure and corresponding operating environment that are needed to meet the policy goals. It identified the technical developments that are needed in different domains, and recommended supporting activities and expected time frames of those activities to support Smart Grid deployment.

California's investor-owned utilities (IOUs) have a vision that the California Smart Grid of 2020 should be a more capable, robust, and efficient electricity infrastructure, which should help achieve multiple energy and environmental policy goals. In an earlier comprehensive study, "The 2008 California Smart Grid," it was revealed that California did not yet have a unifying vision for the state's Smart Grid. The vision needs to be defined by bringing stakeholders together to agree on objectives for Smart Grid use, key Smart Grid capabilities, and applications that a Smart Grid would support. This report found that a collaborative process was critical for defining a common vision to assist California's many diverse stakeholders to develop a technology Roadmap for achieving the vision. This Roadmap report was an important step in rectifying this situation. This report described that vision and presented a detailed Roadmap for achieving that vision. The report provided clarity and direction to support California Smart Grid initiatives and the State's energy and environmental policy goals.

The report detailed findings in six domains of technical expertise: Communications Infrastructure and Architecture, Customer Systems, Grid Operations and Control, Renewable and Distributed Energy Resources Integration, Grid Planning and Asset Efficiency, and Workforce Effectiveness. These domains defined a structure of technical topics by which to further develop project findings on: vision, baseline, technology readiness Roadmaps (which identify applications and enablers at each stage of technical advancement), gaps, and recommendations. The envisioned California Smart Grid of 2020 should link electric operations, communications, and automated control systems to create a highly automated, responsive, and resilient power delivery system that should both improve services and empower customers to make informed energy decisions. A Smart Grid with these characteristics would support California's energy policy goals, including increased penetration of renewable resources, reduced greenhouse gas emissions, increased energy efficiency, implementation of demand response, increased use of distributed energy resources, maintained and/or enhanced grid reliability, and transportation electrification. The Smart Grid would also provide greater protection from cyber security attacks and safeguard customer privacy and worker safety. The project also illuminated the challenges associated with Smart Grid development and deployment—such as maintaining and/or increasing reliability in the face of increased grid complexity and managing technologies at different levels of maturity.

The primary objectives of the project described in this report were:

- In partnership with the three major California utilities, combine utility perspectives on development of the California Smart Grid in light of key state and federal policy drivers.
- Define the utility vision of the California Smart Grid of 2020 and define pathways to reach that vision, using 2010 as a baseline.
- Recommend critical activities to fill technology, policy, standards, process, and education gaps, which need to be closed to implement the vision.

The project team considered multiple factors, including regulatory, commercial, and technical considerations, as well as utility priorities for Smart Grid development and deployment. The drivers for the Smart Grid consist of both regulatory policy and commercial considerations, whereas, technical factors determined physical capability and limitations of the Smart Grid, as well as operational readiness. For reference there existed over 80 ongoing Smart Grid projects spanning T&D, workforce, generation, market, substation, and end-use applications.

For California IOUs, a key driver for Smart Grid development was maintaining and/or enhancing reliability in the face of increased grid complexity. Other key drivers were: empowering customers to take control over their energy use and production, reducing GHG emissions, resisting attacks and mitigating natural disasters, enabling energy independence through increased electrification of the economy, opportunity to strengthen the state and national economy by fostering clean technology innovation and related job growth, maintaining or increasing the reliability, efficiency and safety of the power grid. One long-standing and over-arching driver for California has been the legislatively mandated renewable portfolio standard (RPS) of 33% by 2020 (from 20% in 2010).

Additional impetus for Smart Grid capabilities were explicitly supported by the key California and U.S. energy and environmental policies, and fall into four categories: empower consumers and open markets; widespread implementation of intermittent renewable generation; optimized grid reliability, resilience, security and efficiency in the face of increasing complexity to mitigate issues such as plug-in electric vehicles, intermittent renewable generation, and human-caused and natural disasters; and increased worker safety and productivity.

The approach to defining the California Smart Grid vision and Roadmap started with the initial step to comprehensively collect and review existing works through literature review. The project team gathered and reviewed existing materials available from the participating utilities and other sources under a common framework for information collection. The elements of this framework for initial investigation included: existing Smart Grid vision documents, drivers for the Smart Grid, assumptions, cost benefit assessment methodologies, decision models for technology adoption, metrics, and core Smart Grid policy drivers (state and federal) along with policy issues.

The report identified approaches for addressing technology, policy, standards, process, and education needs to support realization of the Smart Grid vision. The project team proposed 10 interrelated research and development streams that cut across domain areas to coordinate development of the Smart Grid with both national and international efforts. The research and development streams emphasized architecture, information models, and interoperability requirements and considered current gaps and different adoption rates for standards and deployments (different for each IOU). The report also documented important technology development needs, including power electronics, energy storage, modeling and simulation, and sensor technologies. The report concluded that these technologies should continue to advance due to market pressures and manufacturer developments. However, for IOUs, demonstration projects should be combined with projects that focus on interoperability requirements to attain maximum benefits.

Technologies were judged to have an "Impact" by using a weighted-average categorization scheme that included: financial, utility, customer, energy policies, GHG, jobs, CAPEX/OPEX, reliability, and safety. Within these broad areas of Smart Grid interest, a "top or near-top priority" rating by all three IOUs elevated the following areas as key over the next ten years to evaluate, plan, design, procure, deploy, commission, and maintain:

- Bulk wind and solar integration to meet renewables portfolio standards (RPS)
- Wide area situational awareness and distribution grid management for system protection and restoration
- PEV integration to reduce greenhouse gas (GHG) emissions and meet customer needs
- Demand response to reduce peak demand and enhance service innovation
- PV for meeting renewable portfolio standards (RPS)
- Customer systems to enhance service innovation
- Distribution grid management to improve voltage regulation
- Grid efficiency and voltage reduction to reduce losses
- Bulk wind and solar integration to reduce GHG emissions
- Data integration for system protection and restoration

The Smart Grid Roadmap provided a pathway for achieving the California Smart Grid vision to support achieving the state's energy and related policy goals. The policy goals were the primary drivers that shaped the vision and Roadmap developed in this report. To be both insightful and actionable, the Roadmap must include a means for measuring progress toward reaching these end-state goals by specifying at any point in time how to measure how far California has gone, and how much farther it must still go. "Impacts" were defined as measures of change in the output or activity of the electricity sector that contributed to the achievement of the goals the state had set. These impacts were described in a

framework for identifying the costs and benefits of Smart Grid Roadmap items that could be used as a common means to seek regulatory approval for investment in Smart Grid initiatives.

The Roadmap described in this report represented the California utility vision of the technical infrastructure and corresponding operating environment that were needed to meet the policy goals. It identified the technical developments that are needed in different domains, and recommended supporting activities and expected time frames of those activities to support Smart Grid deployment. The Vision 2020 Roadmap Plan identified the following as the most critical elements in establishing the Smart Grid in California by 2020:

- 2020 Vision Communication/Architecture Domain: The 2020 Vision for Smart Grid communications infrastructure and architecture was envisioned to integrate diverse, single-purpose communications networks into an efficient and flexible unified information infrastructure. This information infrastructure should support the timely and secure exchange of information using interoperable, model-driven standards across the entire grid supply chain covering bulk generation, transmission and distribution grids, market operations, power system operations, distributed energy resources, energy service providers, and the customer. Field devices, consumer devices, authorized third-party systems, and back-office technologies and systems should be able to be easily secured and integrated—through increasingly unified communications networks—into a resilient and secure Smart Grid architecture which supports reliable and efficient electric system operations.
- 2020 Vision for Customer Systems Domain: The Smart Grid should enable customers to actively support the reliable, sustainable, economic delivery of power by providing feedback to help customers manage the timing and quantity of their energy usage; enabling third-parties, including utilities, to manage energy usage on behalf of customers; and allowing customers to adopt environmentally-friendly technologies (e.g., PEVs, solar PV) without sacrificing grid reliability.
- 2020 Vision for Grid Operations Domain: By 2020, the California transmission grid should be well on its way to being fully monitored in real-time with an integrated set of advanced sensors and monitoring devices and robust communication systems. It should have adaptable and trainable, fast control algorithms that should utilize advanced technologies to enhance or maintain system security and reliability and to maximize transmission throughput to enable high penetrations of renewable resources. By 2020 the California transmission grid is envisioned to: ensure power quality and reliability are maintained and/or enhanced, achieve better efficiency, allow the expanded use of renewable energy sources, and improve system planning and engineering processes for future grid development. It aspires to achieve characteristics of a "self-healing" power grid by anticipating and responding to system disturbances and risks to physical infrastructure due to natural disasters, vandalism or cyber-attack.

- 2020 Vision: Renewables & DER Domain: The 2020 vision for this domain is to utilize, integrate and develop bulk renewable and distributed energy resources (DERs) to meet the varying customer and market demands. Renewables and DERs are developed to ensure secure and reliable service, promote energy independence, achieve RPS goals, and attain sustainability. This is accomplished through the use of intelligent monitoring, climate micro-forecast, protection and control technology, storage technology, and advanced information technology and infrastructure that are integrated with the underlying power delivery systems.
- 2020 Vision: Grid Planning and Asset Efficiency Domain: The Smart Grid of 2020 should operate assets and resources more efficiently by dynamically controlling voltage and optimizing power flows. Monitoring and sensing capabilities should be expanded to enhance asset maintenance and investment decisions. Advanced planning tools should facilitate and leverage the integration of distributed energy resources (PV, PEV) to meet customer needs and ensure system reliability and performance.
- 2020 Vision: Workforce Efficiency Domain: Smart Grid Workforce Effectiveness involves preparing the workforce to support Smart Grid technologies and tools while enhancing safety and productivity. Utilities should be organizationally prepared through internal skills development, external education, recruiting, and knowledge management. The tasking, scheduling and routing of work should be more efficient and seamless. Ultimately, sensor technologies, advanced visualization tools and robotics applications extend to both the "office" and "field" workforce, with a focus on training, safety and situational awareness.

The key recommendations of the final Smart Grid report included:

- Security considerations must be addressed in an integrated state-wide Architecture, in the communications infrastructure, and in all the information exchange requirements at points of interoperability. There should be a tremendous effort required to expand overall enterprise information systems to accommodate the additional information associated with widespread integration of distributed resources in grid and market systems.
- At the transmission level, the WECC synchrophasor initiative and coordination should provide the foundation for significant expansion of synchrophasor applications and development of advanced system management and control applications that take advantage of synchrophasor information.
- Asset management and maintenance strategies should also take advantage of widespread sensors and automation. Ongoing development should build on efforts underway in the areas of dynamic asset rating and condition based maintenance (CBM), both of which require real time information integration.
- Modeling and forecasting improvements were needed to better integrate variable resources with markets and grid operations.

- Utility organizational structures will most likely need updating to deal with the cross-functional nature of the Smart Grid and the new skill requirements for the workforce.

The report also outlined recommendations for workforce educational needs which included: academic research (e.g., developing and analyzing new technologies and operating approaches in theory), practical applications (e.g., working with industry to get promising technology ready for implementation), education (e.g., training the next generation of industry professionals and researchers), and public outreach (e.g., identifying and communicating public interest dimensions of the "Smart Grid").

A final but important element of the California Smart Grid Roadmap was the increasingly important role that natural gas (NG) played in the state's electric Smart Grid. Because of NG-based turbines capabilities for peak-shaving, their fast response to control inputs, their usage as the most GHG-friendly fossil fuel, and the strengthening trend for even less expensive supply, NG could potentially affect California in both positive and negative ways. DERs should play an ever increasing essential role in the electric Smart Grid and meeting the state's diverse goals. Natural gas is an important fuel for DERs. Typical natural gas-fueled DERs include: (a) individual reciprocating engines, (b) small aero derivative gas turbines and microturbines, (c) combined heat and power (CHP) configurations utilizing either engines or turbines, and (d) fuel cells.

In summary, the California Smart Grid Roadmap report offers an array of potential benefits to customers, society, and the environment. Advanced monitoring and control capabilities should increase utility technical efficiency to improve overall performance of the power system—increasing asset utilization, limiting T&D losses, and enabling many Smart Grid capabilities including integration of renewable resources, reliability-based demand response and customer energy management to reduce peak demand.

Roadmap Summary - Duke Energy

Duke's Transmission Roadmap Leadership Team undertook, with the assistance of EPRI, a thorough analysis of the objectives, required elements, recommendations, and implementation plans for Duke's Transmission Smart Grid Roadmap. Using EPRI's IntelliGrid process, a series of workshops and independent stakeholder and subject matter expert (SME) interviews were conducted covering the previously identified four most critical business and operations scenarios. This brief summary outlines the key processes that were utilized: a compilation of unique Duke Transmission issues and recommendations, a technology assessment and ranking process undertaken, and other related key conclusions and recommendations.

Duke Energy has developed vision and mission statements for the definition and development of a power delivery communications and automation infrastructure, which includes the communications upgrade to substations, the implementation of select technologies and applications and the integration of enterprise

applications, as well as databases and systems as an enabler for Duke to optimize the business. This is called the Transmission Roadmap initiative. Duke already had an installed base of infrastructure investments. Integration over time of these existing systems should enable Duke to leverage additional benefits from these investments. New investments must adhere to the new system-wide integration requirements. The medium to long-term result should be enhanced decision making as more staff in different arenas have access to key performance data and lower costs to upgrade existing systems or add new ones.

This Roadmap's objectives were directly reinforced by Duke's Mission statement: "A communications, information and automation infrastructure that enables the integration of installed equipment and advances in communications, computing and electronics to optimize system reliability, comply with NERC standards, optimize costs, and enable the delivery of services to meet the future needs of our customers" as follows:

1. Comply with NERC standards
2. Implement IP communications to all substations
3. Enhance cyber security at all CIP facilities and plan for future scope changes
4. Retrieve, store, and disseminate non-operational data to all authorized users in a secure manner
5. Obtain equipment condition information to enable condition-based maintenance and enhance reliability
6. Utilize equipment condition data and new applications to provide dynamic rating information of transmission lines and transformers to system operators
7. Reduce outage durations
8. Reduce and/or defer capital costs
9. Integrate Energy Management Systems (EMS) and Distribution Management Systems (DMS) systems

Following these Roadmap objectives, two primary areas of benefits were identified that were anticipated to have a large positive impact on Duke. While some of the benefits should appear in the short term of one to two years after deployment, others should be manifested in the medium to longer term. The first primary benefit was enhanced grid reliability. Many of the recommended projects and technologies contributed to enhanced reliability. For example a number of the technologies contributed to a further improvement in Duke's compliance with NERC standards. Specifically NERC had published a set of standards for cyber security referred to as Critical Infrastructure Protection (CIP) standards that impact reliability from a security perspective. The second identified primary benefit was economics: A key theme of this report's findings was the enhanced integration and dissemination of important data between applications and user groups within Duke. In general, this capability should enable faster and more informed operational and business decisions. Related, sharing asset monitoring data such as measured transmission line loading and condition should assist the asset management team when making decisions on

asset replacement or upgrade. This should aid in avoiding major repair costs. In some cases necessary asset replacement should be arranged in a more cost effective manner with more information earlier in the life of the equipment. In other cases it was expected that capital investments should be deferred for a period.

In addition, from the high degree of integration expected in the future, Duke anticipated the following important benefits: better cyber and physical security management, wider selection of a broad range of products and applications with more features and pricing options, and minimized costs (integration of enterprise and other applications, operations and maintenance savings, capital investment deferments or reductions, installation and related costs for new systems, upgrade of existing applications and systems).

The approach that developed Duke's Transmission Roadmap involved the EPRI team applying the "IntelliGrid" methodology to discover the most important system requirements and technologies (referred to as the architecturally significant requirements) necessary to implement selected smart grid functions and applications at Duke over time. The process resulted in the determination of key application benefits, difficulty of implementation, the technologies required, applicability of various smart grid functions to business objectives, identification of prerequisites, and the development of suggested implementation timelines.

A key result of the roadmap development process was the identification and ranking of several technology and application area vision statements. The Duke Team selected and ranked these project areas based on their expected positive impact (reliability, costs, security/compliance) on Duke as a business and the level of effort (risk, regulatory, cost, workforce, customer acceptance, technology maturity, etc.) to implement. This extensive Technology Assessment was further described and assessed with respect to evaluation criteria and then ranked over eight technology areas and against the following ten criteria: maturity, self-description, security, scalability, manageability, standards, openness, users groups, object modeling, and power industry.

The workshops identified five of the most critical use cases for Duke Transmission going forward: Secure Remote Access to Intelligent Electronic Devices (IED)s, Transmission Fault Analysis, Integrating Equipment Monitoring & Diagnostic into EA Management, Dynamic Rating Integration with EMS, and Distribution Load Reduction. From these, the following nine key technology visions were evaluated and recommended for implementation:

1. Implement secure remote access to substation data. Substation Data Managers (SDMs) should enable Duke to achieve secure enterprise-wide access to key real-time operational and non-operational substation data. SDMs were crucial to Duke's long-term vision and implementation.
2. Deploy new substation data gathering technologies. Widely implement SDMs or substation gateway devices for the initial purpose of providing a cost effective external interface to the new IP network at each substation.

3. Improve on Duke's existing cyber security strategy. Expand the enterprise security policy for cyber security that addresses all elements of information exchange for implementing a smart grid including (but not limited to) the substation networks and devices, corporate network, EMS network, wide area networks, plant controls, and other sources, sinks, and manipulators of data and information.
4. Create and deploy a substation protocol integration strategy. Commence wide implementation of DNP3 LAN in conjunction with the serial to IP upgrade program at all bulk transmission sites. Develop guiding principles, best practices, future DNP/61850 integration strategy, standardized design templates and procurement specifications for the deployment of highly integrated substation automation networks at the bulk transmission level.
5. Implement a strategy for secured and controlled enterprise-wide sharing of applications and databases. Develop the integration policy, strategy and requirements necessary to create the foundation for enterprise-wide data exchange to maximize the value from all data captured from various substation, feeder, generation, and transmission system assets. This strategy should allow information exchange across organizational boundaries while protecting the integrity of the operational data.
6. Migrate from a planned T&D Facility Ratings Project to an on-line continuous asset monitoring approach. Kick-off the T&D Facility Ratings Database (FRD) project and provide system operators real-time access to the FRD. Commence planning for deployment of on-line condition-based monitoring of substation transformers and transmission line providing asset data acquisition, aggregation and management systems to deliver on-line condition information to asset management, maintenance engineering, field staff and system operations.
7. Implement automatic fault record retrieval and analysis. Widely deploy or connect to existing substation based protection relays, digital fault recorders (DFRs) configured to record disturbances and faults. Implement SDMs or other data concentrator devices capable of automatically retrieving, storing and forwarding a wide range of data record types using standard and custom protocols (legacy) in a secure manner.
8. Deploy substation phasor measurement units (PMUs) at select sites. The wide use of phasor measurement technology should have the potential to provide Duke with significantly enhanced visibility and awareness of the status of the grid within Duke's own service area as well as adjacent utilities.
9. Expand the deployment of distribution feeder automation (DFA). Develop requirements, policy, guidelines, and specific implementation plans for the expanded deployment of DFA through it.

In addition to these specific technical recommendations, several overarching recommendations important to the success of the overall program were also developed:

1. Establish a visible, long term Transmission Roadmap Leadership (TRL) team with Senior Management level support.

2. Develop a Transmission Roadmap Governance Model including technology investment requirements development, integration requirements, standards, policies, guidelines, technology maturity evaluation, and audit requirements. Both this Governance Model and the TRL were considered critical to the long-term success of the effort.
3. Ensure that project compliance to the standards and policies becomes a normal part of all project business cases.
4. Establish project teams to begin implementing the recommended technology projects.
5. Audit results to monitor compliance to the Governance model and establish the benefits/effectiveness of the systems. Periodically revisit, refine, and adjust elements of the Roadmap and Governance model as necessary.

As a result of these workshops, EPRI proposed to Duke a high level more fully integrated transmission related communications and automation infrastructure for the future following the framework of the Integrated Grid Communications and Automation (IGCA) Architecture. Integrated systems should enable improved access, analysis, and visualization of key performance data enabling enhanced decision-making at all levels of the organization. Integrated systems should also provide improved cyber security as well as support a wider range of system options that exhibit lower costs, greater price vs. feature flexibility, and ensure continued improvement in the security of power supply.

The report provided recommendations and guidance on implementing organizational mechanisms to effectively drive change at Duke in such areas as assumptions, skills, technologies, priorities, and responses to regulations changes. A Governance model was a critical tool for the Transmission Roadmap Leadership (TRL) to both define integrated technology requirements and communicate expectations to a broad project audience. Key elements for the Governance model should include: investment expectations, requirements development process, standards participation, integration standards, policies & guidelines, technology maturity evaluation, pilot program approach, and audit requirements.

Once the Transmission Roadmap Leadership Team establishes their Governance model, Duke should implement an open, standards-based, enterprise-wide architecture as a foundation for the integration of new medium and long term application investments. The integration of applications, databases, systems and devices should become a high priority and should then yield maximum benefits for Duke.

Epilogue: The following is a brief synopsis of selected follow-up feedback (personal opinions given and not speaking for Duke) after allowing for the lapse of some time from the Roadmap's completion and circulation within the organization.

Regarding the usefulness and spinoffs from the Roadmap process, the effort provided renewed impetus and vision and a way of going forward with a model

for what the future might look like. Initially, the staff perception of the Roadmap process was apprehensive as they were simply instructed to participate by management. Although it took some time (a year or two) for people to really understand what the process was and how it could help, the overall perception after the fact was quite positive. In hindsight, although the original process worked well, it could be improved by doing a better job of communicating what the Roadmap process involved, the results, and the plan going forward so that each participating department would more fully understand (and be less resistant).

Several important and ongoing projects have resulted from the Roadmap effort including: Out of the originally identified nine threads, Duke has seriously considered and is moving forward with projects for at least 7-8 and now have a project to look at Enterprise Integration. An important direct positive impact of the Roadmap process was that it provided a solid starting point for Duke's ARRA proposals and grants, especially the serial to IP conversion project followed by its associated business case. Other projects included: Synchrophasor data (Note: other departments have also started to use data to verify post disturbance analysis) and enhanced visualization techniques to increase operator situational awareness, upgrades to EMS to accept phasor data now. The DOE FOA had asked for phasor data so the Roadmap helped in Duke's proposal. Additionally, other Roadmap initiated projects included: implemented communications upgrades in the MidWest from serial to IP (replacing the frame relay that was there), and a planned pilot next year on automated fault record retrieval (business case completed). Driven by the Roadmap and its Serial to IP project, one key change had been the assignment of a dedicated manager to the system protection SCADA lab which must now support broader organizational needs (e.g., capital justification for new projects such as new data communications between the SDMs and EMS, etc.) and just its historical protection-focused mission.

Regarding Roadmap updates and reviews, Duke staff regularly review the core technology recommendations at the governance meetings to determine which technology has the best bang for the buck. Additionally, they have done their own refresh of the Roadmap – two years ago with System protection, planning, operations, IT groups and went through it again (2010) to review new NERC standards, NIST standards, organizational changes, DOE stimulus funding, technology review, power system operations and communications protocols, integration of EMS/DMS, leveraging T&D technologies, as well as looked at the Smart Grid teams DA.

Finally, the Duke Transmission team emphasized, the importance of senior level management buy-in for all future applications of the Roadmap process. As follow-up, two teams at Duke meet at least once or twice quarterly (the Executive and the Leadership) to review and refine the Roadmap as a dynamic document. The leadership team is composed of a wide cross-section of people drawn from all Transmission related departments (planning, protection, operations). Duke continues to use the Governance structure and uses the established Governance mechanisms to ensure overall organizational integration and coordination.

Roadmap Summary - Southern Company

Southern Company's (SoCo) Team undertook, with the assistance of EPRI, a thorough analysis of the objectives, required elements, recommendations, and implementation plans for SoCo's Distribution focused Smart Grid Roadmap. Using EPRI's IntelliGrid process, a series of workshops and independent stakeholder and subject matter expert (SME) interviews were conducted in 2008 covering the most critical business and operations scenarios. This brief summary should outline the key business and operations drivers, approaches that were utilized, a detailed technical assessment and ranking, most relevant use cases analyzed, a compilation of unique SoCo issues and recommendations, and other related key conclusions and recommendations.

Starting from SoCo's existing Smart Grid Strategy work that had been completed previously, this Smart Grid Roadmap process began with the identification of a set of distribution-focused Smart Grid use cases and scenarios. Smart Grid use cases/scenarios were selected based on Southern Company's interest in pursuing functionalities (and related business value) implied by these use cases/scenarios.

As a result of the IntelliGrid workshops, a set of core Smart Grid Roadmap objectives were determined as follows:

1. Improved Reliability: provide dependable power to customers, deliver customer-valued power quality, anticipate potential problems on the grid and take pre-emptive corrective action, withstand most disturbances without failing, restore service quickly, provide quality, real-time information, and diagnostic tools to system operators
2. Enhanced Security: resist cyber-attacks and provide enhanced facility security
3. Greater Interaction with Customers: provide real-time pricing, supply, system condition information to customers, AMI, smart appliances, and web-hosted applications
4. Increased Efficiency: improve cost control, reduce electrical losses, improve asset utilization, loss reduction initiatives, distribution power flow optimization, remote capacitor monitoring, voltage reduction programs, and AMI (demand response focused)
5. Optimize power flows: reduce transmission congestion and improve overall efficiency
6. Reduced Environmental Impact: facilitate economic delivery of energy from renewable sources, monitor and manage gas insulated substation equipment, underground transmission lines, high capacity conductors, Flexible Alternating Current Transmission Systems (FACTS)
7. Increased Safety: reduce system problems and equipment malfunctions that could place the public or Southern Company employees at risk, equipment sensor and monitoring technologies, automated fault location, fault current limiting devices, automated switching applications

In addition to these core objectives, grid reliability received additional attention and touched on the following technology functionalities and enhancements:

- IEDs
- Automatic Fault Isolation and Service Restoration
- Fault Anticipation/Location
- Fault recording and remote analysis
- Automated short circuit calculation/fault location
- Fault sensors/indicators
- Equipment/circuit sensors
- Protection scheme validation
- Enhanced data visualization
- Automated switching applications
- Contingency analysis application

Several technologies and functionalities were further analyzed, which would be required elements of a successful Smart Grid Distribution strategy. These related areas and more detailed descriptions of SoCo specific systems are indicated below:

- Communications Technologies
- AMI Sensus wireless network
- Frame relay (capture of substation operational and non-operational data)
- Utilinet radio network (DSCADA for substation and line devices; enable peer-to-peer schemes)
- Southern LINC (DSCADA functionality for remote substations and line IEDs)
- Systems Integration
- Integrated Distribution Management System (IDMS)
- AMI-OMS-SCADA Integration
- Asset Optimization
- Equipment sensor technologies
- Power Quality
- Harmonic data acquisition
- Voltage sag suppression
- Loose neutral detection
- Distributed Generation and Energy Storage
- Backup generators

- Energy storage
- Plug-in Hybrid Vehicles
- Wind
- Solar
- IT Applications/Technologies
- Data Historians

Building on both these technology functionalities and the Smart Grid objectives outlined earlier, the use case workshops and the follow-up detailed discussions resulted in further investigations around four Distribution-based Smart Grid scenarios. All four of these scenarios were AMI relevant. The first two use cases dealt with outage location and power restoration, where the detection of the outage was from either AMI notification or fault detection means. The second two use cases dealt with utilizing AMI data to optimize network performance from either a historical 'look back' analysis or by determining more real-time information such as the phasing of single-phase meters (and then subsequent balancing). These four use-case scenarios are described in greater detail here:

Use Cases 1-2: Distribution Operator Locates Outage Using AMI Data and Restores Service:

Outage location and service restoration is facilitated by AMI data. Outages reported by AMI meters should substantially augment customer-reported outage data, resulting in faster collection of more extensive outage data and faster, more accurate outage predictions. The AMI system should also facilitate the identification and resolution of nested outages. AMI meters should report the presence of line-side voltage, allowing "false" outages to be identified by customer service requests (CSRs), eliminating unnecessary truck rolls. Advanced data filtering should filter out other potential "false" outages through the identification of redundant events, momentaries, and events caused by internal utility operations.

Distribution Operators utilize oscillography and line monitoring (fault detection) devices to locate faults. The fault analysis application should capture and analyze a broad range of fault-related data, allowing a predicted fault location to be calculated and presented in a useful graphical interface to the Distribution Operator. This capability should substantially improve the speed and accuracy of fault location.

Use Cases 3-4: Distribution Uses AMI System to Optimize Network:

Distribution Planning should utilize historical feeder load information to optimize load balance on the distribution system. By capturing actual peak load data on feeders rather than using estimates, Distribution Planning is better able to target and plan capital improvements to the distribution system: optimize

capital investments, avoid feeder loading problems (over/underload detection), and improve asset utilization.

AMI data should facilitate determination of phasing of single-phase meters thereby enabling balancing of voltage among phases.

As a result of the Intelligrid use case workshop process and related analyses into these topics, the following summary of findings and recommendations were made for Southern Company:

- Upgrade of communications infrastructure
- Transition to open standards to support future technology investments (no new legacy systems)
- Continue growth in AMI installations
- Integration and organization-wide coordination of Enterprise Applications such as Outage Management System (OMS) with AMI (RNI) system that should deliver substantial benefits to SoCo as well as SoCo customers.
- Application integration using open standards on a prioritized strategy basis was recommended for all Southern operating companies
- Implement substation Local Area Network (LAN)s using open standards and associated devices to enable improved substation data retrieval
- Continue investments in high value applications: utilizing greater penetration of power system monitoring to derive key system knowledge yielding improved efficiencies and reliability

The workshops and subsequent discussions with SoCo and EPRI experts derived the following set of Distribution-specific Recommendations that should allow the four previously described use cases and their desired outcomes to be realized:

- Enhance distribution communications infrastructure to: distribution substations, AMI, feeder devices and Feeder fault detectors.
- Implement an SOA using an enterprise service bus and GID/CIM for enterprise application integration
- Implement a cyber-security strategy for distribution automation: wireless, WAN/LAN, operational and non-operational data.
- Move toward effective use of protocol standards: transition from SES-92 to DNP, prepare for 61850.
- Implement new distribution management applications across Southern Company
- Transition to WAN/LAN technology between and internal to distribution substations
- Expand penetration of substation data managers (SDMs) at distribution substations

- Increase the on-line monitoring of key assets such as power transformers and lines (condition based maintenance, dynamic rating, etc.).
- Implement infrastructure elements for DR with HAN and home gateway technologies
- Plan and pilot test new infrastructure elements for DER and Microgrids: photovoltaic energy sources, energy storage, PHEV, other Microgrid elements)
- Enable support of distribution data by eDNA (Instep historian database): plan for addition of AMI data to the historian

To help enable many of these Distribution recommendations described above, several key principles were derived that must be applied to SoCo's Distribution Architecture to be successful and are described here:

- Organization-wide adoption of open standards to protect current technology investments, benefit from wide industry input, and optimize costs and time for future technology investments
- Assurance of scalability to provide longevity to the architecture and help protect future investments
- Adoption of technology layering to leverage generic technology (non-utility specific) for maximum benefit at lowest cost. Technology layering also enables upgrades of specific components or technologies with minimal impact on associated applications.
- Measurement and retrieval of non-operational data (such as events and asset condition data) to the enterprise to enable high value applications
- Application and data integration and analytics to derive maximum value from acquired data
- Early policy development and requirements definition for cyber security, privacy concerns, and network/device management to minimize later impacts

A detailed Technology Assessment was also completed applicable to SoCo's requirements for Distribution-focused use cases. Technology evaluation criteria were developed to assist the SoCo as it continues to invest in the Smart Grid Distribution Infrastructure. Each technology was described and assessed with respect to the evaluation criteria. In addition, each assessment included a more detailed analysis of its 'impact' as defined by a weighted average compilation of the following evaluation criteria: increase reliability, decrease cost, security/safety compliance (risk mitigation, minimize/avoid negative PR), risk of obsolescence, ranking, regulatory concerns, customer relations (acceptance), cost, IT integration, ease of interpreting information, maturity or capability of technology, as well as finally work force requirements.

Following the Intelligrid use case process, detailed functional and non-functional requirements were investigated and recorded including key 'actors', interfaces, flows, and decision-making. Furthermore, the following ten more fully described Distribution-related recommendations and next steps were made:

- Transition from SES-92 to DNP3: Develop guiding principles, best practices, SES-92 to DNP3 integration strategy, standardized design templates and procurement specifications for the deployment of integrated distribution substation and feeder devices.
- Cyber Security strategy for DA: Comprehensive security policies, risk assessment methodologies, implementation guidelines, use of standards based solutions, equipment procurement specifications, guiding principles that anticipate technology and regulatory change.
- Moving Toward IEC 61850: Develop guiding principles, best practices, DNP to IEC 61850 integration strategy, standardized design templates and procurement specifications for the deployment of integrated distribution substation and feeder devices.
- Deployment of Substation Data Managers: Widely implement substation data managers or substation gateway devices for the initial purpose of providing a cost effective replacement for the RTU function and IED data concentration as well as local HMI.
- Enhance Distribution Communication Infrastructure: Develop a comprehensive set of infrastructure requirements for a field area network (FAN) to fulfill a Southern Company wide defined set of performance and service level criteria using IntelliGrid use case methods for the full planning horizon.
- Implement an SOA on Enterprise Service Bus using GID/CIM for application integration: Develop an integration policy, strategy and requirements necessary to create the foundation for enterprise wide data exchange to maximize the value from all data captured from various substation, feeder, generation and transmission system assets.
- Transition to WAN/LAN Technology Between and Internal to Distribution Substations: Develop a comprehensive set of requirements for WAN/LAN support to and within distribution substations to fulfill a Southern Company wide defined set of performance and service level criteria using IntelliGrid use case methods for the full planning horizon
- Increase the On-Line Monitoring of key assets such as power transformer and lines: Develop an asset monitoring strategy for distribution substations and key lines sourcing these stations.
- Implement new distribution monitoring applications across territory.
- Finally, plan and pilot test new infrastructure elements for DER & microgrids.

As with other IntelliGrid Roadmap processes, it is important to manage the inevitable changing requirements and scenarios as both internal and external drivers evolve. Importantly, the Roadmap is a living document to be updated as new challenges, supporting activities, and opportunities arise. This change process and evolving leadership role requirements are best accomplished through visible Governance processes, and therefore, the Roadmap contained suggested governance to provide oversight for implementation including feedback processes

to ensure that grid modernization continues to address SoCo's evolving challenges. The Roadmap report recommended that SoCo establish a visible, long term Smart Grid Roadmap Leadership (SGRL) team with VP level support. Going forward, the SGRL Governance model must be more thoroughly developed to include the following elements: investment expectations, requirements development process, integration standards, policies & guidelines, technology maturity evaluation, and audit requirements. Other roles that the SGRL would fulfill include monitoring SoCo's progress toward its original vision statement and making necessary modifications and refinements to the Roadmap on a periodic basis or as required.

An integral aspect of managing the Roadmap also includes adhering to the following activities: developing personnel skills to support infrastructure (workforce training and education), participation in standards and industry groups, actively managing the progress towards a Smart Grid (from hands-on to management levels), monitoring progress towards the vision, and periodically or as needed, modifying the Roadmap based on further technology research and pilots.

The final steps for SoCo (and its newly established Smart Grid Roadmap Leadership) were to obtain approval to move forward with the Smart Grid Roadmap and achieve the following:

- Adopt Guiding Principles
- Appoint an ongoing Smart Grid Roadmap Leadership Team to promote the Vision & Guiding Principles, and to support cross-departmental communications
- Create individual, cross-functional teams to conduct in-depth evaluations of each recommended technology
- Review results and adjust the Roadmap appropriately

Roadmap Summary – Salt River Project (SRP)

SRP's Smart Grid Leadership Team undertook, with the assistance of EPRI, a thorough analysis of the objectives, required elements, recommendations, and implementation plans for SRP's Smart Grid Roadmap. Over a nine month period, using EPRI's IntelliGrid process, a series of workshops and independent stakeholder and subject matter expert (SME) interviews were conducted covering seven of the most critical business, operations, and customer-related scenarios. This brief summary outlines the key processes that were utilized, as well as describing key SRP issues and recommendations.

A cross functional team was formed in July 2007 and recognizing the need to establish a company-wide identity for the SRP Smart Grid program, SRP developed vision and mission statements for the definition and development of a fully architecturally-integrated power delivery communications infrastructure, which included the integration of all related applications, databases and systems

as an enabler for SRP to optimize its business and enhance and protect its relationship with its customers.

For SRP, several drivers were most critical including: core application issues (e.g. Cyber-security, AMI, DFA, PMUs, Asset Management, and Operations Back-up Center), which then led to a more in-depth analysis and recommendations covering several key areas including: IEEE 1588 (precision time protocol), 61850, security/privacy issues at all levels (AMI, HAN, WAN, DFA, back-office, etc.), as well as other unique local drivers including regulatory, risk and adoption maturity, starting points, inter-departmental coordination and inter-dependencies, and taking advantage of cross-silo data and infrastructure sharing and other potential synergies that could be realized corporate-wide.

SRP's Roadmap effort expected to reap a variety of specific benefits from its future enhanced grid integration including: integration of enterprise and other applications, operations and maintenance savings, capital investment deferments or reductions, reduced upgrade and installation and related costs for new systems, better cyber and physical security management, much wider selection of products and applications with more features and pricing options.

In addition to the standard level of descriptions utilized for use case requirements, the Roadmap Summary also included a descriptions and analyses of each area's benefits, industry best practices, current state and gaps, and maturity of both technology and industry. These efforts resulted in the development of Roadmap use cases in the following seven most pressing areas (by internal ranking) for SRP:

- Enterprise Strategy for cyber-security: system wide and fully integrated from HAN, AMI, WAN, DFA, SCADA, back-office, EMS, etc.
- Automated Tools for WAN Monitoring: in preparation for significant growth in all categories of devices, automated tools for the monitoring and control of all aspects of network traffic and optimization.
- Integrated Substation LAN-DNP & IEC 61850: detailed plans for migration to 61850 in large-scale deployments at both T&D levels.
- Unified AMI & DFA Communications: develop policy and specific guidelines to assure that future deployed communication systems are scalable and versatile enough to handle not only current AMI issues (e.g. DR, TOU, outages, HAN, PEVs, DG, etc.) as well as unforeseen future applications.
- Expanded Distribution Feeder Automation Policy: primarily focused on outage management issues and strategies, locally intelligent but globally optimized systems for power restoration and management.
- Electric System Data Acquisition & Data Management: improve system efficiency, safety, and reliability through wide deployment of enhanced sensor and data aggregation and management systems at the substation, feeder, and transmission line levels.
- Enterprise Application Integration: create the framework, policies, and unifying strategies for the foundation of an enterprise-wide data exchange

which optimizes safety, protection, and operations with enterprise efficiency, customer access, and power delivery reliability and efficiency.

As with other Roadmap engagements, SRP and the EPRI teams undertook a more detailed review of SRP's needs as well as their costs and benefits expectations, associated technology deployment timelines and any other unique drivers and goals. Cross-disciplinary teams were a critical requirement for organizational buy-in. The team further developed a Technology Assessment Matrix spanning each of the eight architectural domains (e.g. security, core network, WAN, etc.) and assigned rank weighting to each. The technology assessments were ranked according to "impact" (includes: economic, efficiency, reliability, etc.) and "effort" (includes: cost, risk, skills needed, etc.).

The application scenarios (use cases) developed during the course of the project yielded valuable technical requirements for use by the project teams charged with implementation. The recommended technology projects are expected to provide significant benefits to SRP in the broad areas of reliability, operational economics, and customer service. Future projects should be planned using similar cross functional teams in a formal process to define broad system requirements that set the framework for the development of detailed requirements and system design. As with the use case process, SRP must periodically reassess and fine-tune all aspects of their roadmap as their objectives, implementation plans, and available technologies and standards evolve.

Once a SRP roadmap management model is established, SRP should implement an open, standards based, enterprise wide architecture as a foundation for the integration of new medium and long term application investments. The integration of applications, databases, systems and devices should yield maximum benefits for SRP and should become a high priority. Integrated systems should enable improved access, analysis and visualization of key performance data enabling enhanced decision making at all levels of the organization. Integrated systems should also be able to provide improved cyber security and support a wider range of system options that exhibit lower costs, greater price vs. feature flexibility, and ensure continued improvement in the security of electric power supply.

In conclusion, SRP has already successfully invested in many technology areas and gained significant benefits from these investments and now has a substantial opportunity to leverage existing technology investments, such as the upgraded communications infrastructure to implement and realize business value from the smart grid applications identified through the efforts of the Smart Grid Leadership Team.

Epilogue: The following is a brief synopsis of selected follow-up feedback (personal opinions given and not speaking for SRP) after allowing for the lapse of time after the Roadmap's completion and circulation within the organization.

Regarding the overall usefulness of the Roadmap process and use cases completed, the initial purpose was served as it helped to provide organizational

direction and cross-cutting efforts. A side and important benefit of the Roadmap process was to increase collaboration between departments and to develop a cross functional Smart Grid leadership team of the company. The Roadmap was helpful in providing direction for where SRP wanted to go. However, with the first four initiatives complete or well under way, the Smart Grid leadership has been dissolved and the remaining initiatives reside within their respective departments. Currently, the main focus is completing the ARRA projects that run through 2013 and determining performance and benefit/cost ratios of specific technologies. Additionally, MDMS implementation plan utilized the Roadmap's cross functional requirements since their culture has supported the process and some use case work is still applied within their AMI effort.

Initially in 2007, the staff perception of the Roadmap process was that it took time to get buy-in to the proposed process, but people soon began to see results. Also, people's expectation was that the Roadmap process would be more specific in terms of detailed action plans, but in reality staff realized that they need the guiding strategy and framework first. In hindsight, it would have helped to have more up-front business benefits, drivers, and the applications with business values which would have helped to generate more immediate top-down buy-in.

Regarding ongoing or new projects that resulted from the Roadmap effort, a lot of initiatives are still moving forward within their respective departments and business cases are being developed to determine which technologies best meet SRP's corporate objectives. Many of these projects had their genesis in the Roadmap workshops including: cyber security, a new NOC, utilize tools to monitor and manage the WAN, using Telenium, and reviewing a corporate data warehouse. Additionally, the original team has used Roadmap methods to help develop the following: AMI – MDMS requirements (including OMS integration in the future), customer services (fraud deterrent), integration into other systems like OMS, TIBCo (IT side), substation network (research only), DNP over IP in many substations, evolution of also using 61850 GOOSE RAS, unified AMI and DFA (with EPRI), a FAN Pilot (including water using WiMAX and LTE), DFA (only surgical where needed in critical locations – still working cost/benefit), reviewing Fault location, deployed Subnet and DGA at four sub-stations, deployed temperature monitors, and studied Enterprise Application Integration with OT. It is hoped that the process that has begun bringing together the OT and IT sides through the cross-functional teams will continue to improve coordination and unity across the company.

Part of the leadership team challenge was how to address:

- NERC CIP impacts along with Data management issues in the substations.
- Defining/articulating the business case rational for integration of technology and systems for which is no one existing model, only various models in pilot phases.
- Determining the details of data management and potential broader corporate use of operational data.

Although the SG Roadmap is no longer being used, SRP's new corporate objectives continue to pursue modernization of the electrical system with a customer-focused, system performance analysis approach. The first five roadmap areas have evolved and will continue within their perspective departments, though re-aligned with the new corporate objectives. The last two areas of the roadmap may or may not proceed as envisioned, depending on whether they meet a need that aligns with the corporate objectives.

Roadmap Summary – TVA

The Tennessee Valley Authority (TVA) is the nation's largest public power provider serving nine million people in parts of seven southeastern states. TVA has a rich history of improving quality of life and economic prosperity for people and businesses in the TVA service area. Down through the years, as times have changed, TVA has changed with them, updating and refining its focus to better serve its enduring mission in: affordable electricity, economic and agricultural development, environmental stewardship, integrated river system management, and technological innovation.

In August 2010, the TVA Board of Directors adopted a corporate vision for the company to become one of the nation's leading providers of low cost, clean energy by the year 2020. The TVA 2020 Vision was built around six goals. The first three goals embody the company's core business foundation - to continue providing low electricity rates, high system reliability, and responsible environmental stewardship. The second three goals embody a new focus on cleaner air, more nuclear generation and greater energy efficiency.

Various challenges threaten TVA's ability to sustain its enhanced mission. Increasing environmental regulation by federal agencies requires changes to the generation portfolio. Increasing reliability and infrastructure security mandates impose new and rigorous reporting requirements. The transmission asset infrastructure is aging. Customer requirements are becoming more complex and challenging. At the same time, TVA has to overcome constraints imposed by growing capacity demands, an aging workforce and a tighter fiscal environment. TVA recognizes that a strategic initiative to modernize the grid will enable the company to respond to these challenges in a coordinated and timely manner.

In 2011, TVA undertook, with the assistance of EPRI, an effort to develop a Roadmap that would help guide Grid Modernization investments through 2020 and beyond. The TVA Grid Modernization Roadmap provides a high level framework for implementing the tools and capabilities that are required to modernize the grid.

TVA Grid Modernization Roadmap

Within TVA, the Energy Delivery (ED) organization is responsible for the reliable delivery of electric power throughout the valley. ED's mission is to maintain a cost effective, reliable, safe and compliant transmission system for TVA.

ED supports corporate goals to increase energy efficiency through better asset utilization and reduced system losses. Cost effectiveness drives efforts to improve work force efficiency. Likewise, improvements to core processes and performance reduce operational costs. Demand response initiatives through distributor and direct served customers reduce the need for additional generation capacity by allowing peak load shaving. TVA's 2020 vision sets a goal of national leadership in cleaner air by 2020, and the company's Integrated Resource Plan outlines an energy roadmap to make that happen. In 2011, the TVA Board voted to retire 18 of TVA's 59 coal-fired units by the end of 2017. ED's role in this shift in the generation portfolio is to plan transmission options required by this retirement as well as for new generation facilities.

ED's most pressing compliance objective is to meet or exceed ongoing North American Electric Reliability Corporation (NERC) mandates for reliability and critical infrastructure protection (CIP) developed by NERC. Revisions to NERC CIP are occurring more frequently and the time for utilities to achieve compliance is being reduced. Interregional planning is now mandated by the FERC 1000 regulations. Other equally important challenges include constrained transmission, reduced operating margins, aging workforce, and changing customer requirements.

TVA's change in focus towards cleaner air, more nuclear generation and greater energy efficiency creates new challenges for the transmission infrastructure. The emphasis on energy efficiency and low cost power challenges the way that the existing transmission infrastructure is operated. Large-scale changes in the generation fleet significantly impact power flow on the transmission system. Changes in power flow on the TVA and regional interconnections may result in some lines being overloaded while others are underutilized. These issues will be further exacerbated as TVA is on target to grow its clean power from 39% to 57% by 2020 (in addition to 5% efficiency improvement). At the same time, ED faces additional challenges from outside the Valley in the form of ongoing regulation, expanding customer requirements and rapid changes in grid technologies.

TVA realizes about 86% of its revenue from 155 local public power distributor companies that deliver power from the TVA grid to end-use customers, a situation which adds to the complexity of grid management and optimization. Distribution companies seek improved operational efficiency, better control over costs, and exceptional service levels. Demand response is expected to play an increasingly important role in controlling customer cost.

With this as a backdrop, the Grid Modernization Roadmap development process began as an executive request within ED for an actionable plan to address potential challenges facing the transmission system in the next 5 to 10 years. An initial workshop was held with stakeholder groups to gather input and feedback to identify the transmission system elements that the organization should focus on initially. From this workshop, a vision statement and four initial focal areas were drafted.

During March, 2011, workshops were held on each of the four focal areas - reliability, efficiency, asset management, and communications. These workshops brought together stakeholders from across TVA's organization to develop a set of Future Statements to describe how modernizing the grid will enable ED to sustain its mission. Twelve Future Statements were developed across the four focal areas. These twelve future statements were subsequently vetted by internal and external experts to establish priorities among the many tools and capabilities that could be leveraged to modernize the grid. In addition the original focal areas were refined into a set of operational objectives to provide directionality towards the future vision. The operational objectives identified were:

- Optimize utilization of assets
- Improve efficiency of transmission system
- Increase situational awareness
- Improve tools for operator control
- Enhance coordination with customers
- Compliance and Safety

The priorities and objectives identified in this way form the basis for a set of Roadmap recommendations. The recommendations are organized into four targeted Roadmap Initiatives describing activities TVA should undertake to lay the foundations for grid modernization over the next ten years. Each Roadmap Initiative contains near term (1-3 years) activities and a timeline with medium and longer-term activities. The recommendations cut across operational boundaries to lay the foundations for Grid Modernization. Several activities are listed for each Roadmap Initiative. Activities include technologies that TVA should monitor, evaluate, adopt, or lead; processes that should be evaluated or changed; studies to launch; and industry collaborative efforts in which TVA should participate.

Roadmap Initiative 1 – Information Communications and Technology Infrastructure:

The applications and technologies that TVA will implement to modernize the grid generate significant information flows. To realize full value from the applications, the data should be available throughout the TVA organization including (as needed) customers. At the same time, data security should be carefully designed to ensure appropriate authorization prior to access. Building the ICT infrastructure to accommodate these data flows and relevant security is a foundational activity in the grid modernization roadmap.

Roadmap Initiative 2 – Modeling and Analytical Tools for Planning and Operations:

To continue improving reliability, cost-effectiveness and security/compliance, TVA will invest time and resources into advanced planning, modeling and operational tools. TVA will evaluate and deploy advanced tools to improve

planning, modeling and system operations, especially in areas such as customer load management where new uncertainties complicate the operating environment. These tools will provide an accurate and integrated decision support environment that improves TVA's ability to operate the grid reliably and cost effectively.

Roadmap Initiative 3 – Advanced Control Strategies:

Advanced tools, technologies and systems are improving operator control over uncertainties (e.g. voltage, reactive power, frequency, reserves, distributed energy resources and renewables). Consequently, TVA will investigate and implement strategies that improve operator analysis and control of the power system with a particular emphasis on preparation for greater diversity in generation portfolio.

Roadmap Initiative 4 – Strategies and Systems to Optimize Asset Management:

TVA continues to make significant investment in transmission assets. Adopting state of the art strategies and systems to manage these assets cost effectively offers the best return on TVA's grid modernization investment over the next decade. In the near term, TVA will focus on initiatives that maximize the value of existing infrastructure investments.

To continue the process from this point forward, the Roadmap recommended that TVA organize a business process to implement Roadmap Initiatives required to modernize the grid. Therefore, the Roadmap contains suggested governance to provide oversight for implementation including feedback processes to ensure that grid modernization continues to address TVA's ongoing challenges until 2020 and beyond. Importantly, it also recognized that the Roadmap is a living document to be updated as new challenges, supporting activities, and opportunities arise. In recognition of the importance of governance and organization buy-in, the following organizational activities are required to make sure that the Roadmap comes to fruition:

- Alignment and Endorsement within TVA
- Roadmap Governance
- Employee Communication Strategy
- Grid Modernization Implementation Plan
- Establish Implementation Teams to Address Roadmap Initiatives
- Coordinate with On-Going Projects
- Develop Medium and Long Term Planning
- Project Execution
- Assessment against Objectives
- Revise as Necessary

In conclusion, the Roadmap is a living document to be updated as new challenges, supporting activities, and opportunities arise. Over the next ten years, TVA must modernize its electric grid to meet its many opportunities and challenges. The implementation of this report's Smart Grid Roadmap will assist TVA in continuing to deliver cost effective, clean, reliable, and secure power to its 155 distributors and 9 million customers for the foreseeable future.

Section 6: Technology Recommendations

EPRI Roadmap Technology Recommendations Summary:

This chapter is a compilation of all the most important technology recommendations which were made spanning EPRI's Roadmap efforts. Although each Roadmap is unique to the entity that initiated the engagement, there often exists overlap in technology requirements and associated recommendations.

Each technology recommendation described in this chapter is comprised of the following six essential elements (two additional elements from the actual roadmaps are not included here; the utility's current situation and gaps) as follows:

- Objective Statement: the summary goal statement.
- Recommendation: the summary recommendations for this technology theme.
- Industry Best Practice: the best in class application and practice across the industry in this area of technology
- Benefit/Rationale: key benefits expected as a result of investing in the technology or the rationale to do so
- Challenge: anticipated difficulties, costs or risks that must be overcome to implement the technology
- The remainder of this chapter outlines by technology theme category many specific technology recommendations, their benefits/rationale, best practices, and challenges to come.

(1) Technology Recommendation Theme: Integrated Enterprise Architecture, Information Technology, etc.:

On almost all levels, grid modernization eventually requires a hard look at a utility's overall enterprise architecture, information flows and technology, as well as ability to share and easily add/modify new services. The following technology recommendations were deemed most relevant for this summary document:

Technology Recommendation: Implement a service oriented architecture (SOA) using an enterprise service bus and Generic Interface Definition (GID)

and Common Information model (CIM) enabling company-wide Enterprise Application and Database Integration

It is most typical within utilities today that an enterprise service bus (ESB) is not currently implemented at the utility. However, it is planned for the future. The utility must develop the integration policy, strategy and requirements necessary to create the foundation for enterprise wide data exchange to maximize the value from all data captured from various substation, feeder, generation and transmission system assets and be able to utilize it throughout the organization. This strategy allows information exchange across organizational boundaries while protecting the integrity of the operational data. The policies and system architecture developed respect the requirements of the core application and its users (e.g. performance, priority, and security) while facilitating data exchange to other internal and potential third party entities that can use it and extract value for the utility. The integration guidelines support efficient and seamless information exchange through classic service oriented architecture principles but also supports selective process decoupling to support disaster recovery, maintenance, system upgrade and other exceptional conditions as they arise. Effective data integration will enable the utility to utilize advanced visualization tools and analysis applications to drive optimization toward key performance targets.

Although specifics may vary utility to utility, the consensus amongst all utilities who have participated in Roadmaps cannot be underestimated on the long-term strategic importance of a consistent and integrated architectural approach. The following set of general recommendations apply to a broad spectrum of these enterprise-wide architecture issues:

- Develop an integration policy, strategy and requirements necessary to create the foundation for enterprise wide data exchange to maximize the value from all data captured from various substation, feeder, generation and transmission system assets.
- Integration policy should stipulate the use of the SOA, GID interfaces, and CIM
- The strategy should allow information exchange across organizational boundaries while protecting the integrity of the operational data.
- The policies and system architecture developed must respect the requirements of the core application and its users (e.g. performance, priority, and security) while facilitating data exchange to other internal and potential third party entities that can use it and extract value for the utility.
- Follow a layered approach to the technology interfaces to enable any utility specific functions to be added to generic technology that is in widespread use. This minimizes the utility specific technology (lower volume) required.
- The integration guidelines should support efficient and seamless information exchange through classic SOA principles but also support selective process decoupling to support disaster recovery, maintenance, system upgrade and other exceptional conditions as they arise.

- Effective data integration will enable the utility to utilize advanced visualization tools and analysis applications to drive optimization toward key performance targets.
- Generate a comprehensive set of requirements for an SOA enterprise service bus that includes the requirements for current and/or transition support GID interfaces and CIM
- Establish a project to select and implement an SOA enterprise service bus as defined
- Ensure the iDMS requirements set and project definitions include integration with an SOA enterprise service bus, GID compatible interfaces and CIM
- Establish a project based on the above to integrate AMI data (RNI) with the OMS applications (TCMS, DOES, new IDMS)
- Establish a project based on the above to integrate CSS data with the OMS applications (TCMS, DOES, new IDMS)
- Application integration planned for IDMS:
  - Distribution SCADA
  - Distribution Automation
  - Electronic MapBoard
  - Outage Management System
  - Switching Management
  - Unbalanced Load Flow Analysis tool
  - Crew Management
  - GIS
  - AMI
  - Asset management

Current Industry Best Practice includes the following: integration policy, guidelines and requirements process in place, all enterprise level applications integrated including: EMS/DMS, OMS, GIS, Asset Management, Meter Data Repository (MDR), publish/subscribe based services, standards based interfaces (GID) and object models (CIM), and central databases/historians for all non-spatial and spatial data (one each)

Emerging technology trends include: integrated applications for EMS/DMS, OMS, GIS, Asset Management, MDR, standards based interfaces (GID), standards based object model – CIM, single central non-spatial database, single central data historian for all non-spatial data type, and single central spatial database designs.

The technology and Industry Maturity of this recommendation is still developing: LIPA are a key user of CIM/GID, CIM/GID are evolving but more work needed, some suppliers starting to offer CIM/GID compliant interfaces, and the future is model sharing between EMS, planning, DMS (future).

Several of the key Benefits/Rationale of this recommendation include: significant life cycle cost reductions for enterprise applications, operations and maintenance savings, capital investment deferments or reductions, installation and related costs for new systems, upgrade of existing applications and systems, better cyber and physical security management, wider selection of a broad range of products and applications with more features and pricing options, reduced cost of upgrading or adding new applications, enterprise wide access to key performance data enables further optimization (performance and costs), broader data access supports enhanced business case development, future savings in support and testing with object modeling, and future common object model definitions with IEC 61850and minimize vendor lock in issues.

Additional Benefits/Rationale also include:

- Lowest life cycle cost of technology implementation while achieving maximum integration benefits across the enterprise
- Interfaces with applications, devices, and sensors that can be connected via off-the-shelf adapters.
- Adapters can be fed with data from hundreds of devices and applications with little or no investment or development.
- Increased data independence enables user specific customizations without affecting coding
- Application data self-description eliminating a great deal of configuration effort
- Model awareness allows applications and users to see the meaning of data and its relationship to other data. Also allows changes to models to be propagated automatically.
- The layered approach to the technology interfaces enables utility specific functions to be added to existing generic technology that is in widespread use. This minimizes the utility specific technology (lower volume) required and reduces overall cost.
- Application independence from data sources enables reusability of applications without configuration changes
- Standard power system object definitions, future harmonization with IEC 61850 substation device models for integration with enterprise applications and databases

Technology Recommendation: Designing for Information System Integration (CIM)

Although this recommendation ties into the previous recommendation for system-wide integration of enterprise applications and database, it is important enough to warrant another view of the overall communications and information architecture with a more detailed view of some of the capabilities that are required in the network management functionality. The use of the Common Information Model (CIM) as the basis of central data management and

coordination along with the functions that interface with the CIM allows for a more consistent design and approach as follows: transport of data including queuing and translation over different protocols, routing, workflow and security management, connection of services to the proper information, including adaptors that may be required for data translation, and through use of service containers (running the service applications).

At the remote ends of the communication system, the substation is only one of many possible end points for the communication infrastructure. The system may provide communications not only to devices in substations, but feeder devices, or even end user devices (meters, energy storage, distributed generation, etc.). The system also must be able to support legacy systems. This could include for example, legacy AMR systems as well as legacy substation communication systems.

Many CIM implementation examples abound. Some of the important functions for typical CIM implementations have been:

- Handling Customer Outage Calls (, Interactive Voice Response (IVR)
- Managing Substation and Circuit Load History
- Scheduling Single-Person Work (SPS)
- Billing Wholesale Transmission Transactions
- Providing Enterprise Reports (Data Warehouse)
- Integrating EMS/SCADA
- Forecasting and Risk Management
- Managing Distribution Facilities Joint Use (GIS)

One of the primary Benefits/Rationale for CIM is how these functions can be integrated for access to common data using service oriented architecture (SOA) and an integration bus that is managed by appropriate middleware.

As stated earlier, from an industry and technology Maturity perspective, CIM has been embraced for its integration benefits by Long Island Power Authority (LIPA) and a number of vendors. They have integrated systems so that planners can update their simulation model with actual EMS data or access historical models through the PI Historian database. Other vendors have utilized CIM as a general model for application integration from IEC 61968/61970 standards efforts. CIM is planned for interfaces with the ESRI GIS system (distribution system model) and there is g rowing recognition of the value of integrating applications to benefit from AMI data and the new iDMS system planned.

The CIM utility infrastructure specification will build on major infrastructure elements that are already in place and would typically include: ongoing network transformation project for WAN improvements, SAP applications provide basis for data integration model leading to CIM implementation, system-wide EMS infrastructure provides basis for system models (supports a common network

model for access by a wide range of applications), OMS/GIS infrastructure already set up with maintenance for representation of connectivity at distribution level, and is just starting to implement system for asset management project prioritization (ECATS) and should be integrated via CIM.

(2) Technology Recommendation Theme: Information Communications and Technology Infrastructure

A key element of grid modernization has been the upgrade and/or wholesale replacement of a utility's legacy-based communications technologies for much more capable and fully-integrated open standards-based set of technologies. This section reviews key technology recommendations which span most aspects of a utilities existing infrastructure from meters to distribution and transmission. The following technology recommendations were deemed most relevant for this summary document:

Technology Recommendation: Advanced Information Communications Technology (ICT)

The applications and technologies that the utility will implement to modernize the grid generate significant information flows. To realize full value from the applications, the data should be available throughout the utility organization including (as needed) customers. At the same time, data security should be carefully designed to ensure appropriate authorization prior to access. Building the ICT infrastructure to accommodate these data flows and relevant security is a foundational activity in the grid modernization roadmap.

An ICT infrastructure allows diverse data to be quickly and accurately transmitted across an entire network. Users may customize their data and information needs. Emerging end-use applications facilitate the work of planners and operators. Two-way communication between applications enables management of demand response, energy storage, and other end-use applications.

Various activities are already underway at the utility concerned with implementing an ICT infrastructure through Transmission Infrastructure Management and Monitoring (TIMM) and elsewhere. In addition, the utility will take the following key actions to implement a modern ICT infrastructure:

1. Develop requirements (data, communications, security, etc.) for anticipated applications (protection, control systems, condition monitoring and asset management, event analysis, demand response, voltage control, etc.) This activity is foundational to all subsequent activities. Requirements will be determined through the development of use cases. Cross-organizational teams will be formed to develop the use case.
2. Develop an integrated architecture for the modern grid. This architecture will define: enterprise systems, interface requirements between systems applicable standards, substation communication and information architecture, enterprise to substation communication technologies and

architecture, communication interfaces with customers and other third parties, integration with distributor communications infrastructures,

3. Develop security services architecture to support security requirements as a function of application: application-based risk assessment, required security services, implementation plan within architecture.
4. Define the interfaces between the utility and it Distributers/Customers/Partners. The interfaces should identify: data to be exchanged, communication protocols, data formats, and security.

Timeline for ICT Infrastructure Roadmap Initiative

1. Develop a strategy for data management and systems integration. This strategy should include: define data and information requirements as a function of application, define data exchange requirements, define requirements for an enterprise data repository and evaluate vendor products, develop a data management architecture to facilitate ongoing application development, conduct a pilot implementation of the Common Information Model (CIM – IEC 61970) standard,
2. Develop a substation Communication and Information Model Implementation strategy. The strategy will include: substation communications architecture, substation data manager and communications manager, protection functions, control systems interfaces, engineering and model data management from IEDs and sensors, integration of data from transmission lines and assets, cyber security implementation, and migration to plan from legacy systems.

Technology Recommendation: Infrastructure for Customer Systems Integration

Advanced metering infrastructure (AMI) and the integration of customer systems with the operation of the grid has the potential to greatly benefit both the utility and the customer and has often been a cornerstone in business case justification. Customers will be able to respond to real-time prices and have a better understanding of their energy use and the utility will be able to use the vast amount of information from individual customer locations to understand conditions on the distribution system the utility may also be able to control resources at the customer location to improve the performance of the distribution system (either through direct control or other means like pricing).

The communication infrastructure for communication to individual customers for advanced metering and coordination of distributed resources can take many forms: BPL, fiber or cable, radio, public cellular network, wireless mesh, WiFi, WiMax, or any combination of the above. Standards based interfaces at important points of interoperability are key in minimizing integration issues.

Careful consideration to the full range of potential benefits and applications should be considered when developing the requirements for the advanced metering system due to the tremendous cost of full deployment, training,

maintenance, and application development. Over a wide-range of utilities and utilities, the basic principles include:

- Open standards at points of interoperability (UtilityAMI)
- Two-way communications
- Distributed access to information (some at meter, others at meter data management system)
- Local processing vs central processing
- Integration of distributed resources as an integral part of advanced metering infrastructure

Some of the following examples of advanced applications for the customer infrastructure and its associated Benefits/Rationale include:

1. Advanced metering can enhance the accuracy of system simulations and state estimation as follows: accurate load profiles are developed for virtually all customers based on advanced metering data (meter data management system), system models are expanded to include connectivity and electrical characteristics to every customer, solutions are designed to incorporate load models that are parametric in nature (function of customer energy efficiency technologies, distributed resources, day of week, temperature, and other parameters), these parameters are available to the solution to estimate the load conditions at any instant in time across system, the load models are calibrated in real time based on actual monitoring data (transformers, branches, etc.), and finally the system solves accordingly.
2. Once accurate state estimation takes into account customer characteristics, customer resources that can be controlled and can become part of the system optimization. PHEV and other storage, distributed generation, and demand management are examples. This creates a need to significantly expand the customer information system to include a much richer representation of the customer in terms of potential interaction with the system.
3. Ultimately, local controls for individual customers or groups of customers should allow islanding to maximize the benefit of distributed resources for reliability improvement. This will require substantial communication infrastructure to assure safety, coordinate protection, and optimize the system performance. Standards for this communication system and the associated information models are just starting to be defined.

From an industry and technology Maturity perspective, AMI systems now have tens of millions of meter points. However, many of the more advanced AMI features are at different stages of testing and usage.

Technology Recommendation: Unified AMI and DFA Communications

Although AMI often represent a cornerstone in grid modernization, considerable benefits can be realized through the further integration and synergies achieved in implementing a unified AMI and distribution feeder automation (DFA) strategy.

This requires the utility to develop policy and guidelines for the evaluation, design, procurement and deployment of communications infrastructure necessary to implement specific applications that takes into account the common requirements necessary to support a wider range of other applications. These policies and guidelines will result in the deployment of one or more communications related technologies that results in a unified versatile communications infrastructure capable of scaling and adapting over time to support multiple applications including advanced metering, distributed energy resources (e.g. photovoltaics, plug-in hybrid electric vehicles, other generation, demand response technology, etc.), distribution feeder automation, and other as yet unforeseen applications.

This further step in integration often yields the following Benefits/Rationale: address challenges with the current 900 MHZ DFA communications, significant future capital cost savings, able to justify a better last mile communications solution with cross functional requirements and benefit identification, and support of application integration and optimal architectures.

The Industry Best Practice includes many well-developed and proven technologies including:

- Integration policy, guidelines and requirements process in place
- Single communications infrastructure for AMI, DR, DER
- Time of Use & DR
- Prepayment
- DFA & Capacitor control
- Remote connect/disconnect (theft)
- Outage management (last gasp)
- Customer access to information
- Home gateways, HAN, PCT
- AMI-Sec including ANSI 12.19

The current technology and industry Maturity of this approach includes: AMI manufacturers slowly moving into Open AMI, high bandwidth communications solutions are early in the product development curve (WiMAX), as well as AMI-Sec is making good progress (ASAP).

Technology Recommendation: Transition from SES-92 to IEEE Std 1815 (DNP3) and eventually full 61850 for fully integrated substation LAN

Depending upon a utilities current state of substation and feeder communications infrastructure, appropriate technology recommendations were made with varying degrees of scope. Initially, commence wide implementation of IEEE Std 1815 (DNP3) LAN in conjunction with the serial to IP upgrade program at all bulk transmission sites and if a utility had limited experience with DNP/61850, a transition recommendation would be to integrate DNP3 more thoroughly, but

most recommendations included an eventual final transition to the more capable and secure IEC 61850 platforms. This strategy involves the gradual procurement and deployment of substation equipment (compliant with electromagnetic environment standards) that utilizes both DNP3 and IEC 61850 based communications technologies with a gradual, longer term shift toward fully integrated IEC 61850 based systems. The strategy also includes the implementation of a fully integrated 61850 substation to develop the utility specific best practices and auditing methods necessary to evaluate the benefits and overall effectiveness of the proposed substation network infrastructure design template with the goal to lower costs and improve performance. These transition strategies often included the following initial recommendations which were followed by the subsequent 61850 recommendations:

- Develop guiding principles, best practices, SES-92 to DNP3 integration strategy, standardized design templates and procurement specifications for the deployment of integrated distribution substation and feeder devices.
- Implement the gradual procurement and deployment of equipment that utilizes both SES-92 and DNP3 based communications protocols with a gradual, longer term shift toward fully integrated DNP based systems.
- Utilize channel optimization capabilities within DNP3 such as Unsolicited Report by Exception (URBX) to minimize channel loading
- Plan for future upgrades to DNP3/IP where applicable (see separate recommendation on substation LANs)

These initial recommendations were often followed by the following 61850 recommendations:

- Develop guiding principles, best practices, IEEE Std 1815 (DNP3) to IEC 61850 integration strategy, standardized design templates and procurement specifications for the deployment of integrated distribution substation and feeder devices. This strategy involves the gradual procurement and deployment of equipment that utilizes both DNP3 and IEC 61850 based protocols with a gradual, longer term shift toward fully integrated IEC 61850 based systems.
- The strategy also includes the implementation of a fully integrated 61850 substation to develop specific best practices and auditing methods necessary to evaluate the benefits and overall effectiveness of the proposed substation network infrastructure design template with the goal to lower costs and improve performance.
- As familiarity with IEC 61850 grows, the utility staff should begin using 61850 point naming conventions for all data points even for non 61850 applications. This will greatly aid in the future transition to 61850.
- Scope, to include: substation networks and devices (initial phases), and distribution feeder devices (later phases)

There exist many strong Benefits/Rationale for utilities to make this transition and include: lowest life cycle costs, security of supply and wide range of device

options, reduce protocol support costs (definition, documentation, updating), reduced project costs for protocols development, testing, schedule impacts, enhanced configuration support using XML device profiles and other schemas.

In addition to these benefits for transitioning to IEEE Std 1815 (DNP3), the following additional Benefits/Rationale exist for transitioning to IEC 61850:

- Lowest life cycle costs
- High-level services enable self-describing devices & automatic object discovery that reduces cost in configuration, setup and maintenance.
- Standardized naming conventions with power system context eliminate device dependencies and tag mapping reduces cost in configuration, setup, and maintenance.
- Standardized configuration file formats enables exchange of device configuration reduces cost in design, specification, configuration, setup and maintenance.
- Higher performance multi-cast messaging for inter-relay communications enables functions not possible with hard wires and reduces cost in wiring and maintenance.
- Multi-cast messaging enables future sharing of transducer (CT/PT) signals reduces cost by reducing transducers and calibration costs.
- Standard object definitions will enable future harmonization with CIM Power System Models for integration with enterprise applications and databases

The current best practices for transitioning to IEEE Std 1815 (DNP3) include: all IEDs support DNP3 or DNP/IP – Level 2 or 3, DNP implementations are independently verified, XML/SCL used for configuration, moving toward new cyber security standards for DNP3 for substations and feeders, and more widespread participation with industry protocol standards efforts and user groups. In addition, embracing 61850 also brings the following best practices:

- High bandwidth (100mbps) fiber Ethernet networks within substations
- All IEDs support DNP3/IP and 61850
- GOOSE implemented and operational
- Redundant (A/B) VLANs at critical sites
- Separate VLANs - non-operational data
- Moving toward new security standards for DNP3 and IEC 61850
- XML/SCL used for configuration
- Moving toward new cyber security standards such as DNP3 and IEC 62351 for substations and feeders

The industry and technology maturity of these technologies is relatively well developed:

- DNP was initially launched as a public domain protocol in 1993 and is based on IEC 60870-5 standards as a robust, feature rich protocol for utilities
- Many North American utilities use DNP for SCADA to substation and feeder communications as well device to device communications in substations
- DNP is supported by a large and effective user's group that continues to evolve the definitions, specification documents and test procedures
- Recent advancements include basic self-description, XML device profiles and the DNP3 Secure Authentication Specification
- A joint effort is underway between EPRI and DNP User's Group to conduct pilot testing and enhance the DNP3 Secure Authentication Specification
- DNP3/IP implementations can work with the IEC 61850 GOOSE application
- DNP3 does not currently support the IEC 61850 standard device object models so may eventually be replaced as the majority solution for within substations
- Lowest life cycle costs
- Configuration savings (meta data/SCL) using XML device profiles and other schemas
- Capital savings in future (GOOSE)
- Standard object definitions, future harmonization with CIM for integration with enterprise applications and databases
- Adoption of IEC 61850 is growing rapidly in other areas of the world (much more so than North America).
- Hydro Quebec is moving forward with 61850. Many utilities are piloting: e.g. TECO, PG&E, Hydro One, others
- The utility has completed commissioning of Bradley substation
- New security standards - nearly complete
- User group is well supported.
- SCL tools are becoming more widely available.

Technology Recommendation: Transition to WAN/LAN Technology Between and Internal to Transmission and Distribution Substations

Advanced integrated communications has strong justification not only at the substation level, but increasingly at the distribution level as well. The details of this recommendation are as follows:

- Develop a comprehensive set of requirements for WAN/LAN support to and within distribution substations to fulfill a the utility Company wide

defined set of performance and service level criteria using IntelliGrid use case methods for the full planning horizon as follows:

- Fully equipped distribution substations (all expected IEDs and new/expanded stations) connected using LAN/WAN technology
- Support of both operational and non-operational data
- New communication protocol (DNP3/IP) and integration policies
- Compliance with new Cyber Security policies
- All applicable environmental standards and requirements
- Support for a wide range of IP protocols for web viewing of local displays, file transfer, network & device management, pass through, remote time synchronization, other
- Consider future implementation of wireless LANs for devices installed in the switch yard as technology evolves
- Substation LAN technology will avoid coming technical obsolescence of serial communications:
- IED manufacturers are no longer offering serial communications on some of their new models
- Develop a comprehensive infrastructure development plan for each operating company leading from the current infrastructure to the planned future FAN based on a common set of requirements
- Consider the merits of a transitional phase of using contracted communications services for non-operational data at key distribution substations and feeder devices
- Ensure all network equipment used for the substation LAN meets hardened requirements as specified in the applicable IEEE and IEC standards (eg IEEE 1613)
- Plan for the additional network loading of new applications such as extensive event/fault record retrieval in a timely manner and a large penetration of phasor measurement devices.
- Consider the use (and plan the bandwidth for) of substation based standard and infrared video for security and asset monitoring.

The primary Benefits/Rationale for embracing WAN/LAN Technology both internal and between substations and (in the future) feeders is:

- Improved performance for operational and non-operational data retrieval eg. fault records
- Mitigate technical obsolescence of serial communications (some new IED are LAN only)
- Supports secure remote access to the substation for maintenance, configuration changes and firmware changes

- Integration with the identity management server for effective local/remote credential management
- Long term support for standards protocols such as DNP3/IP and IEC 61850 with associated benefits such as GOOSE messaging saving significant installation/capital costs
- Long term support for new data types such as phasor data

The current industry best practice includes the following:

- Growing number of utilities are implementing WAN/LAN technologies to their substations
- In addition many are installing LANs within the substations
- A large range of hardened network components are available for substations
- Substation data managers are approaching the 2nd or 3rd generation of software and hardware. These devices serve as gateways, data concentrators, protocol translators, security application clients/servers, event record managers, automation application hosts and HMIs
- Support for operational and non-operational data on separate virtual networks
- Use of substation data managers as substation gateways and data concentrators
- Secure device policy per IEEE 1686
- Cyber security applications such as local/remote credential management
- Wide enterprise access to central maintenance host
- Secure (terminal server) pass through to station IEDs for maintenance
- SNMP and SysLog network management applications

Technology Recommendation: Enhance Distribution Communication Infrastructure:

It is important for utilities to develop a comprehensive set of infrastructure requirements for a field area network (FAN) to fulfill a utility-wide defined set of performance and service level criteria for the full planning horizon as follows:

- Maximum expected AMI system penetration (primary and back-haul)
- Fully equipped distribution substations (all expected IEDs and new/expanded stations) connected using LAN/WAN technology
- All expected feeder control, capacitor, fault detection devices, standby generator sites and network underground sites
- Applicable smaller transmission switch sites
- Support of both operational and non-operational data
- New communication protocol and integration policies

- Compliance with new Cyber Security policies
- All applicable environmental standards and requirements
- Urban and rural regions

Additionally, related recommendations include the following:

- Develop a comprehensive infrastructure development plan for each operating company leading from the current infrastructure to the planned future FAN based on a common set of requirements
- Consider the merits of a transition phase of using contracted communications services for non-operational data at key distribution substations (other than GPCo) and feeder devices
- Define a hybrid system that addresses the full range of end devices, performance requirements, geographical factors and densities.
- Continue / begin technology investigations leading to pilot testing
- Tower based technologies, and/or
- Mesh technologies (Note: IEEE WG for Mesh – IEEE 802.15.4g, WPAN)
- Distribution substations supported with WAN/LAN technologies
- Back-haul technologies such as fiber optic to collection points such as towers with future expansion planned
- Long term FAN requirements should include:
- Scalability for number of end point devices
- Scalability for bandwidth available per end devices
- Flexibility for a range of performance and service requirements for different end devices (in support of operational and non-operational data types)
- Frequency agility – effective spectrum management
- WAN/LAN to distribution substations with LANs in substations
- Support for local wireless networks in substations
- IP connectivity to all devices
- Future anticipated data types such as device firmware, device configuration files, phasor data
- Some data types will transition from non-operational to operational as power system operating requirements and enterprise applications evolve. For example: equipment condition data and phasor measurement data

The primary Benefits/Rationale for utilities to adopt these recommendations typically includes:

- Supports greater penetration of AMI and distribution devices such as fault detection devices

- Enables retrieval of non-operational data in support of key new applications such as fault analysis, fault anticipation and other applications planned for iDMS
- Addresses the issue/risk of future technology dead ends and spectrum reallocations
- Fulfills the requirements of a new Distribution Cyber Security Policy
- Supports new open standards for communication protocols

Examples of Industry Best Practice include:

- Point-to-point radio systems
- Large mesh networks
- Some distributed logic processing
- Comprehensive set of infrastructure requirements based on IntelliGrid methodologies.
- Some IP based mesh topologies are a model for the future
- Point-to-point technologies
- Automated event record retrieval
- AMI networks can be utilized for DA communications
- WAN/LAN support to substations with LANs in the substations to support feeder equipment
- Standards based protocols such as IEEE Std 1815 (DNP3)
- Cellular and leased line backhaul
- Cyber Security policy compliance for all elements and devices
- Use of environmentally hardened devices

The current state of technology and Industry Maturity is:

- UtiliNet mesh network is mature (but limited capacity)
- Distributed logic is proprietary to a single vendor
- In general, field area networks are still not interoperable
- WiMAX is new – but standard and could dominate
- Some tower based solutions are still new
- Defined with the utility Company input
- Large number of new clients in 2008
- Active development program to add spectrum and bandwidth
- Some mesh networks are mature in the DA space however performance needs to be carefully evaluated
- WAN/LAN and substation LAN technologies are mature

- Standards based communication protocols such as IEEE Std 1815 (DNP3) are mature with a large rate of adoption in North America. The adoption rate of IEC 61850 is high internationally and starting to grow in North America
- Cyber security standards and specifications are new with pilot programs pending or underway

(3) Technology Recommendation Theme: Advanced Grid Applications & Automation:

The previous technology themes have touched on the importance of both an integrated enterprise-wide architecture and system-wide communication technologies. This technology theme discusses the importance of utilizing these capabilities and the vast amount of data they will generate to perform advanced grid applications and automation services. The following technology recommendations were deemed most relevant for this summary document:

Technology Recommendation Theme: Advanced Grid Applications.

Often a utility's driving objective for achieving advanced applications is to become an Industry leader in advanced grid monitoring, wide area control, and decision support applications providing grid transparency, efficiency, and reliability.

Advanced grid applications working in conjunction with other key applications such as advanced forecasting, external entities supplying data, field data sources and the communications infrastructure will be essential in providing utility's staff with the ability to maintain system reliability in the midst of significant change, while facilitating effective market services.

The utility must continue to evaluate and implement the voltage stability analysis (VSA) and dynamic stability analysis (DSA) applications already planned and in process. In addition, the utility must continue to identify, test and implement new applications that are available or close to available today such as dynamic line rating and a phasor enhanced state estimation techniques. Additionally the utility must seek out new phasor data applications. Finally, the utility should seek or fund the development of applications for decision support, predictive Automated Generation Control (AGC), joint VAR management. In parallel with the above application developments, the utility must continue to develop and provide comprehensive visualization tools and training for its personnel.

The following recommendations were often given to achieve some of these advanced grid applications: continue toward enhancement / implementation of situational awareness visualization tools, applications for decision support, test and evaluate new applications using phasor data such as dynamic rating, plan for future VAR management, predictive AGC, evaluate and implement redundant and parallel instances (separate location) for all candidate applications, operator training (phasor applications and other)

Current Industry Best Practice does include many of these recommendations:

- Advanced visualization tools
- Dynamic Security Assessment (VSA/DSA)
- Dynamic line (& transformer) rating
- Advanced contingency analysis
- Phasor data inputs
- Condition monitoring inputs
- Intelligent decision support
- Wide-area volt/VAR management
- Meteorological-based load/gen forecasts
- Integrated with market
- Redundant system at alternate location

A primary Benefit/Rationale for implementing these recommendations is enhanced reliability & operational efficiency. Additional benefits include: improved situational awareness and management of renewables, decreased operator stress with improved awareness tools and decision support, improved day-ahead scheduling as forecasting tools are improved, and recorded rationale (context) for control decisions.

Most often the challenges associated with making these improvements include: cost of new communications, technology maturity, and the raw volume & synthesis of data.

The technology and industry maturity of this recommendation is:

- Visualization tools are evolving – e.g., Space-Time Insight
- On-line VSA/DSA applications including Small Signal Stability analysis are maturing
- Growing suite of phasor based applications
- Phasor enhanced state estimators are an emerging practice
- 5 major EMS vendors (ABB, AREVA/Alstom, GE, OSI, Siemens) compete on features
- Future – integration of "system-of-systems" will lead to unforeseen new applications
- Future – Remote Access Services (RAS) – wide area visibility needed

Technology Recommendation: Implement new Distribution Management Applications company-wide

As advanced technologies are justified at new levels, many opportunities are being justified for implementing advanced distribution management applications.

These recommendations most often include:

- Distribution management system advanced applications as defined for IDMS at APCo
- AFISR (Automatic Fault Isolation and Service Restoration)
- Fault Detection and Location
- Optimal Volt/Var Loss Management
- Unbalanced Load Flow Analysis
- Short Circuit / Coordination Analysis
- Distribution Contingency Analysis
- Advanced Outage Analysis / Prediction
- Vehicle Location System Dynamic Deration of Power Equipment (Harmonic loading)
- Distribution Operator Training Simulator
- Expanded use of feeder switching devices including automatic sectionalizing and restoration schemes across the utility. Support with new FAN technology
- Expanded use of fault detectors
- Utilize data to augment the IDMS applications
- Application integration planned for IDMS:
  - Distribution SCADA
  - Distribution Automation
  - Electronic MapBoard
  - Outage Management System
  - Switching Management
  - Unbalanced Load Flow Analysis tool
  - Crew Management
  - GIS
  - AMI
- OMS additional future integrations to be considered: CSS and asset management
- Support for a connected distribution electrical model by integration with the GIS for all the utility operating companies
- The utility should require the use of GID compatible interfaces and CIM for the IDMS to ensure future application integrations can be effectively implemented at minimal cost

The primary Benefits/Rationale for these recommendations include: enhanced system reliability with outage restoration, prediction capabilities, improved contingency and long term planning, reduced system losses, and new applications added faster and at lower costs.

The existing state of best Industry Practice is as follows:

- The suite of advanced DMS applications considered "best practice" includes:
  - Fault Isolation and Service Restoration
  - Fault Detection and Location
  - Optimal Volt/Var Loss Management
  - Three phase Load Flow Analysis
  - Short Circuit / Coordination Analysis
  - Early versions of Distribution Contingency Analysis
  - Integration with Lightning Tracking system
  - Distribution Operator Training Simulator
  - Integration with other enterprise applications such as OMS will typically be in place.
  - Best practice is integration using GID and CIM

Finally the technology and industry Maturity of this recommendation include the previously discussed aspects of: CIM/GID usage by both utilities and vendors. In addition, some of the applications listed such as Distribution Contingency Analysis and Advanced Outage Analysis/Prediction are new applications where new developments are still occurring.

(4) Technology Recommendation Theme: Cyber Security

Cyber Security (and privacy) has increasingly become a focal point for utility, regulatory, and customer interaction. Some aspects of cyber-security are still developing while others are beginning to be either specified or guide-lined. The following technology recommendations were deemed most relevant for this summary document:

Technology Recommendation: Develop an Integrated Enterprise-wide Cyber Security Strategy

The objective of achieving a Standards compliant cyber security policy and resulting infrastructure that automatically identifies, visualizes, and resolves threats and vulnerabilities has quickly risen to the forefront at many utilities. The development of an enterprise strategy for cyber security that addresses all elements of information exchange for implementing a smart grid including (but not limited to) the corporate network, EMS network, field area networks including AMI & DFA, wide area networks, home area networks, substation networks and devices, SCADA , plant controls, distribution feeder devices, back office systems, data repositories, customer, employee, and executive information portals, extranets, and other sources, sinks, and manipulators of data and information. Copper and wireless networks will be included. The strategy will address specific requirements associated with specific NERC CIP regulations as well as the underlying intent. The cyber security strategy will include comprehensive security policies, risk assessment methodologies, implementation guidelines, equipment procurement specifications, and guiding principles that facilitate evolving the strategy over time to account for technology and regulatory change.

The following generic recommendations are offered (followed by a more specific list): focus on application layer security, policy for addressing data integrity, define and plan for infrastructure (cyber security) situational awareness including dashboard, new IEEE Standard 1815 (DNP3) (Secure Authentication), IEC (62351) & IEEE 1686 standards, centralized authentication management, investigate automated compliance management products available for use in control systems, review and adopt risk based standards and practices as recommended by the National Institute of Standards and Technology Interagency Report (NISTIR) and OpenSG – SWG are out or expected shortly, and future capability - automatic audit of applications and configurations.

More specific recommendations organized by area include:

- Continued Focus on Application Layer Security: Traditionally, power system related applications have relied on network and transport layer security mechanisms for protection. Application-layer attacks are very attractive to a potential attacker because the information they seek ultimately resides within the application itself and it is direct for them to make an impact and reach their goals. The utility should continue to focus on adding application layer security to critical applications as an overall part of its defense-in-depth strategy moving forward.
- Develop Policy for Addressing Data Integrity: As much of the power system data the utility handles is utilized in decision making, data integrity is of the utmost importance. Once a policy addressing data integrity is developed, requirements and solutions can be defined.
- Review and Adopt Risk Based Standards and Practices:
  - NISTIR 7628, Guidelines for Smart Grid Cyber Security has been published. This is a three part document covering all facets of Smart Grid from a high level functional requirements standpoint. This document is a companion document to the NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0 (NIST SP 1108), which NIST issued on January 19, 2010.
  - The OpenSG/SG Security Working Group is vetting and releasing a series of Security Profile documents which are intended to work at a level below NISTIR 7628. These documents are being targeted at specific Smart Grip applications with the goal of providing specific and actionable. The OpenSG/SG Communications Working Group is also developing requirements for the information flows relating to smart grid applications
- Collaborate with Partners and Participants: End-to-end security is a major goal for protecting the systems which support power system and market operations. From data source to data consumer, vulnerabilities and risks need to be assessed at each and every step. As utilities rely on its participants for much of the power system and market data which it utilizes, it may be necessary to extend its security focus into these domains. This "overlap" will help to minimize the potential vulnerabilities caused by gaps at the handoff points between the utility and its participants and partners.

- Integrate newly developed standards into the utility systems: Specifically, three new or updated standards should be integrated into The utility security program as follows:
  - Updates to the IEEE Std 1815 (DNP3) protocol specification now provide secure authentication. The utility should evaluate the current security model utilized for DNP communications and if necessary, develop a migration plan to address any areas that are not in alignment to the new DNP3 specifications.
  - IEEE STD 1686-2007, IEEE Standard for Substation Intelligent Electronic Devices (IEDs) Cyber Security Capabilities should be consulted for additional requirements for all equipment and components added to The utility control systems moving forward.
  - IEC 62351 Parts 1-8, Information Security for Power System Control Operations, define security requirements for power system management and information exchange, including communications network and system security issues, TCP/IP and MMS profiles, and security for ICCP and Sub-station automation. The utility should evaluate all communications which are covered by the IEC62351 suite of documents and develop a migration plan to address any areas that are not in alignment to the new specifications.
- Integrate applications to help maintain the utility's security posture: Once created, The utility must effectively and efficiently maintain its security posture. Control systems and their supporting communications and IT infrastructure are becoming more complex as are the methods which must be utilized to protect them and this complexity presents a significant challenge in maintain security posture. Specific application recommendations which are aimed at this area are summarized as follows:
  - Centralized Authentication Management: Authentication credentials should be centrally managed so that changes do not need to be made in the various end devices and system which utilize them.
  - Real-time system analysis: It is recommended that utilities explore methods and applications to improve its real-time situational awareness of the IT systems supporting power system monitoring and control. The current ability of systems supporting monitoring and forensics make it difficult to impossible to do this in real-time with the goal of stopping the attack before it affects power system reliability. Real-time monitoring of the operational and security state of all systems components and devices to detect unauthorized activity on the system will require the correlation and analysis of a great deal of data from the various systems (e.g. logs, IDS, etc.) as well as new capabilities in field devices.
  - Automated Compliance Management: It is recommended that The utility explore the use of an automated compliance management application within its control system environment to proactively assess its compliance to both internal utility policies as well as any applicable regulatory requirements (e.g. NERC CIP).

- Automated Tracking and Auditing of Field Device Configurations: It is recommended that The utility develop and implement an automated system to centrally monitor, track, and audit software (configuration data, firmware, operating system) related to remotely deployed assets. Most field devices currently are supported by vendor specific/proprietary configuration and management environment that provides limited revision control. As the number of components and devices requires for observation and control of the power system increases, the effort required to validate proper configuration increases along with the potential for inadvertent system events due to outdated configurations or errors in configurations.

In summary, the following recommendations are offered for the utility's review:

- Focus on application layer security
- Policy for addressing data integrity
- Define and plan for infrastructure (cyber security) situational awareness including dashboard.
- New DNP3 (Secure Authentication), IEC (62351) & IEEE 1686 standards
- Centralized authentication management
- Investigate automated compliance management products available for use in control systems
- Review and adopt risk based standards and practices (NISTIR) and OpenSG – SWG are out or expected shortly.
- Future capability - automatic audit of applications and configurations

This has been an extensive list of specific cyber-security related recommendations. The primary Benefits/Rationale of adopting an enterprise-wide cyber security policy include: compliance with NERC-CIP audits, mitigation of real security threats, lowest life cycle investment if planned now, ready for future changes to NERC-CIP.

The current Industry best practices include:

- Policy development compliant with NERC/Critical Infrastructure Protection (CIP) Standards and industry best practice
- Diligent evaluation of cyber related security threats and mitigation
- Adoption of new cyber security technology standards (eg protocols)
- Moving toward new cyber security standards for DNP3 and IEC 61850 for substations and feeders
- Participation with industry security technology definition and standards efforts
- Risk analysis for needed controls (AIC)
- Internal audits

The primary Benefits/Rationale given for adopting these recommendations include: NERC & other regulatory compliance, address known/possible security threats, evolution of the utility security program, and readiness for future regulatory changes.

The most often cited challenges include: tailoring policies for power system monitoring and control applications, real-time metrics on grid monitoring and control functions, and communications infrastructure, and implementing, maintaining, monitoring, and improving information security so it is consistent with the organizational culture.

The technology and industry Maturity of this recommendation is:

- New IEC 62351 standard addresses cyber security for ICCP (IEC 62351-3), DNP3 (IEC 62351-5 Secure Authentication) and IEC 61850 (IEC 62351-6)
- Many suppliers offering cyber security applications, systems and devices such as credential management solutions and secure substation gateways
- The DNP User's Group have developed the DNP Secure Authentication Specification in compliance with IEC 62351-5
- IEEE 1686 standard addresses cyber and physical security requirements for IEDs
- Centralized authentication management
- Automated compliance management products available for use in control systems
- Risk based standards and practices (NISTIR) and OpenSG – SWG available or expected
- Future focus needed - system situational awareness with dashboard with requirements for connected entities
- Future capability - automatic audit of applications and configurations

Technology Recommendation: Cyber-Security Strategy for Distribution Automation (DA):

Although cyber security must be applied system-wide to be effective, the following recommendations are specific to distribution automation:

- Comprehensive security policies, risk assessment methodologies, implementation guidelines, use of standards based solutions, equipment procurement specifications, guiding principles that anticipate technology and regulatory change.
- Secure device policy per IEEE 1686
- Address on-going equipment upgrades to correct security vulnerabilities
- Plan for future upgrades to IP networks and devices system wide

Scope:

- Corporate network (The utility Network)
- DMS/iDMS network
- Substation networks and devices – operational and non-operational data
- FANs including AMI & DFA (wireless)
- Distribution feeder devices - operational and non-operational data
- Home area networks

The primary Benefits/Rationale for these recommendations include: mitigation of real security threats, lowest life cycle investment if planned now, and readiness for future changes to NERC-CIP.

The current best Industry Practice in distribution automation cyber security include:

- Policy development compliant with NERC/Critical Infrastructure Protection (CIP) Standards where applicable and industry best practice
- Anticipate extension of CIP standards to distribution
- Secure device policy per IEEE 1686
- Use of substation data managers (and routers/firewalls)
- Diligent evaluation of cyber related security threats and mitigation
- Moving toward new cyber security standards for IEEE Std 1815 (DNP3) and IEC 61850 for substations and feeders
- Participation with industry security technology definition and standards efforts
- Internal audits

The current technology and industry Maturity of these recommendations is:

- New IEEE Std 1815 (DNP3) (Secure Authentication), IEC (62351) & IEEE 1686 standards
- Many suppliers offering cyber security applications, systems and devices such as credential management solutions and secure substation gateways

Technology Recommendation: Secure Remote Access

Previous technology recommendations have discussed system-wide communications upgrades especially in more remote locations associated with substations, feeders, and distribution circuits. This section briefly discusses how these upgrades are also essential to the implementation of secure remote access. Substation Data Managers (SDMs) enable the utility to achieve secure enterprise wide access to key real time operational and non-operational substation data. The SDM will be designed to abstract the authentication, authorization and addressing for all remote device and data access. In addition device will integrate

with the utility's identity management server, eliminating the need for community logins and published IP addresses for individual IEDs. Device may also be installed in conjunction with a router/firewall for electronic security perimeter implementation. SDM will incorporate a range of security applications to facilitate secure remote data access including pass through for use with native IED software. This effort has close ties to the Substation Data Manager and Cyber Security Policy topic areas to facilitate secure and reliable information exchange.

Key elements of the Benefits/Rationale include: secure access by all authorized the utility staff requiring key data or performing remote maintenance, NERC compliance, and long term efficiencies such as firmware application upgrades.

There are several emerging technology trends and Industry best practices that are worth noting, including:

- IP WAN/LAN to substations
- Use of SDM for perimeter security
- Secure device policy per IEEE 1686
- Cyber security applications
- Local credential management
- Secure (terminal server) pass through to station IEDs
- Wide enterprise access to central host.

The technology and industry Maturity of this recommendation is:

- Growing number of suppliers serve this space including Subnet, Cybectec and GE
- Large number of utilities doing or planning to do this
- NERC audit requirements pressing

(5) Technology Recommendation Theme: Information, Monitoring, and Management

Within grid modernization exist a large number of specific recommendations associated with the monitoring and information flows coming from the grid. The following technology recommendations were deemed most relevant for this summary document:

Technology Recommendation: Expanded Distribution Feeder Automation

Utilities must develop requirements, policy, guidelines, and specific implementation plans for the expanded deployment of distribution feeder automation (DFA). This effort will build on the existing the utility design practices that allow a high degree of flexibility in distribution feeder automation (e.g. multi feeder open loop design) and identify opportunities to deploy locally intelligent but globally optimized systems capable of improving reliability and

reducing the time needed to restore service with optimized utilization of company resources and lower cost. The DFA strategy will initially target hard to reach and traditionally lower reliability area where automated restoration strategies can dramatically improve system performance.

The primary Benefits/Rationale for implementing DFA recommendations include:

- Improved SAIDI/SAIFI
- Faster fault location for field staff
- Feeder load balancing
- Emergency load shedding
- Less complex to maintain than central approach with DMS and GIS based model

The current state of emerging technology trends and best Industry practices include:

- Wide implementation of auto-sectionalizing and auto-restoration system
- Fault break pole/pad switches
- Mesh radio network
- Peer-to-peer operation
- Coordinated with substation devices
- Connection to EMS/DMS for operator control

The technology and industry Maturity of this recommendation is:

- There exist several well respected and quality manufacturers
- Over 3000 devices installed to date with happy clients such as ONCOR, FP&L, AEP, ENMAX, BC Hydro
- Future is a hybrid distributed control, substation participation and DMS/GIS model based system

Technology Recommendation: Infrastructure for Transmission System Applications

The communications infrastructure for transmission system applications involves communications to transmission substations and possibly even communications to transmission line locations (advanced sensors). Existing approaches for communications to substations is typically implemented on an application-by-application basis. The range can go from microwave radio (EMS) to fiber to phone lines.

A more future-proof approach needs to migrate to a communications architecture (as discussed earlier) with security guidelines that can facilitate a wide range of applications and that takes advantage of standards-based protocols,

security management, and multiple levels for implementation of system intelligence. The wide area network should support requirements for critical applications, including the EMS, disturbance data management, PMU data management, and equipment diagnostic monitoring. The infrastructure should support future applications that may involve management of video and infrared monitoring data. All of the functional implementations described below start with deployment of a communications network to substations that provides a foundation for the applications that are built around this network.

Other important applications would include:

- Integrated Monitoring for Disturbances and Power Quality: Various IEDs and monitors can provide data for both disturbances and steady state trending. Integration of these different monitoring technologies can provide an integrated database for intelligent applications. Integration should include power quality monitors, digital relays, digital fault recorders, and other IEDs. The database management application should provide open access to the integrated monitoring data for intelligent applications (fault location, equipment diagnostics, event diagnosis).
- EMS/CIM Integration to support advanced visualization tools and other advanced analysis tools (real time system models available to applications)
- Automatic alarm analysis applications (neural network). Breaker operations, relay operations, overloads, etc.
- Transmission Fault Analysis and Fault Location (including lightning integration): fault location and analysis is an example of an application that requires access to real time system status and configuration data, electrical models, and disturbance monitoring data. This application should demonstrate the open interfaces that allow access to these different systems for advanced applications. This application will also include integration with the lightning detection system database and GIS systems. The system should automatically identify lightning-caused faults and use the lightning database to help locate these faults. Integration with a special purpose application can provide additional verification of system models for lightning events.
- Phasor Measurement Unit (PMU) Deployment and Data Management: This provides wide area data for monitoring of system oscillations. Future phasor measurement unit applications will likely require a parallel data management system within the utility infrastructure. The phasor management data management system will facilitate advanced applications that take advantage of real time phasor data. IEEE C37.118 standard provides requirements and IEC 61850-9-5 will support phasor measurement in the future.
- Advanced State Estimation incorporating PMU data and other system monitoring: advanced state estimation incorporating phasor measurement data will provide improved visibility of system oscillations and conditions. Faster solutions using measurement data will also allow more sophisticated risk analysis simulations.

- Advanced Transmission Line Sensors and Monitoring: the communications and information infrastructure should also support management of data from advanced sensors at transmission towers and on transmission lines. Other examples of transmission line technologies that could be appropriate are being developed at the Intelligent Power Infrastructure Consortium.

Technology Recommendation: Infrastructure for Distribution System Applications

The communications and information infrastructure must be extended to distribution substations and then to the distribution systems themselves. The infrastructure will facilitate expansion of the EMS to distribution substations and implementation of distribution management systems (DMS) that can be utilized by regional distribution operators to improve the performance and reliability of distribution systems.

As with transmission, several of the more important distribution applications would include:

- Substation Automation and Data Integration: the same concepts described previously for transmission substations apply exactly the same for distribution substations. This can include power quality monitoring, IEDs, and RTUs for extension of the EMS to distribution substations. The EMS/DMS for substations should provide visibility and control down to feeder breakers for all distribution substations. Migration to IEC 61850 for substation communications will facilitate advanced applications. Integration of data at the system level will take advantage of the CIM. These systems should integrate with Autonomous Storm Detectors employed to facilitate improved reliability and reduced crew loading during storms.
- OMS/GIS: a utility's OMS/GIS system should be integrated with the customer information system and system maintenance procedures are in place to maintain the accuracy of the system and full system connectivity. This is already an example of best practices.
- Distribution System Electrical Models/Simulation Tools/CIM Integration: distribution system electrical models should be linked with the accurate GIS systems that are maintained with the OMS. Ideally, this integration should occur using the CIM. The integration will facilitate advanced visualization applications, system analysis applications, planning, and fault location. Note: Unfortunately, the CIM is incomplete for full distribution system integration. This is an area of ongoing development in the standards community and more complete specifications can be expected in coming years. Utilities like LIPA are already implementing distribution model integration through the CIM and their work is providing a foundation for the standards completion.
- Fault Location and Fault Analysis Based on Substation Monitoring: the substation monitoring systems can provide the basis for accurate fault location on the distribution systems. Fault location has two primary advantages: improved reliability through faster repair times (faster location of

the faults), and locating temporary faults can identify equipment issues and potential reliability problems before they cause permanent faults. The fault location application should also integrate with the lightning detection system and the OMS/GIS for maximum benefit. Integrated visualization is needed for operators.

- Other Advanced Applications Based on Substation and Distributed Monitoring: other advanced applications can also take advantage of substation monitoring. The EPRI Distribution Fault Anticipator technology is an example of using substation monitoring to identify equipment issues on the feeder. This will also require integration with electrical models and asset management systems for identification of equipment that may be affected. The CIM can provide the basis for this integration. The EPRI Advanced Distribution Automation (ADA) Roadmap can provide input for development of automation plans.

Distributed PQ monitors that have waveform capability can be used for even more accurate fault location because they provide an indication of distance from the fault through the voltage waveform characteristic. This is an extension of the substation-based fault location described previously. It is likely that the waveform recording will have other equipment diagnostic applications as well. The monitors can be distributed monitors on the distribution system or at customer locations.

- Distribution Feeder Automation (Automated Reconfiguration): substantial reliability improvements are possible through investments in automated system reconfiguration schemes. Pilots of these systems are being deployed to understand technology issues, installation and maintenance costs, and integration issues. Two approaches for fast restoration and minimizing customer impacts include: fast communication between intelligent devices that allows smart clearing of fault in localized manner and reconfiguration of the system accordingly, and technologies that allow checking for faults without imposing full fault on the system

The POD Concept developed by the Distribution Vision 2010 (DV2010) group provides a model for incremental implementation of automated systems. A POD is a Premium Operating District, which is a section of a feeder that should only be affected by faults within that section. Reconfiguration (assuming conditions allow it) should prevent outages (not necessarily momentaries) for faults on other parts of the feeder. The POD can be made as small as justified based on economics, existing reliability, etc. An average size of a POD in the long term might be 1/4 to 1/3 of a feeder.

- Steady State Performance Management and Condition Assessment for Distribution Systems: RTUs and IEDs on the distribution systems can provide information to facilitate improved operation of the system as well as identification of equipment issues. Locations for intelligent monitoring can include: reclosers and sectionalizers, other smart switches, capacitor bank controllers, regulators, and some transformers. Ideally, the communication infrastructure should provide IP-Based communication to these devices. The infrastructure should migrate to IEC 61850 type of approaches that allow

self-discoverability and auto configuration but these standards are not complete for distribution system devices at this time. Integration of this information at the system level (DMS) should take advantage of developing industry standards (CIM).

- Automated Voltage/VAR Control Systems for Distribution Systems: this is a particular application that has high value. It can also enable other advanced applications like conservation voltage reduction and voltage reduction for emergency load reduction. The application will integrate RTUs on the distribution system with capacitor controllers and voltage regulator controls to minimize losses and provide accurate voltage control throughout the distribution system.
- Real Time Distribution State Estimation for Performance Optimization: the volt/var control algorithms described above are one example of an important application that takes advantage of real time information from throughout the distribution system. Continuous state estimation will provide additional advanced application opportunities: minimizing losses, optimum configuration based on losses and reliability issues (create lowest risk of outages), integration with automated system reconfiguration systems, equipment and system loading assessments, asset management integration, fast problem identification and cause assessment, provide basis for incorporating customer resources, real time state estimators require more complete integration with system electrical models than the basic volt/var control application. This application should make available visualization of the actual state of the system at all times to operators. Integration should take advantage of the evolving CIM.
- Communication infrastructure should be IP-based to distributed sensors and monitors. The number of sensors needed would depend on the accuracy needed of the solver. Intelligent monitoring nodes indicated above. In some configurations, monitoring nodes may be available at every transformer. In other examples, primary monitoring points will be selected to make sure adequate accuracy is obtained.

All these applications must be integrated with operator visualization and control tools (DMS). Future applications will include advanced features such as adaptive protection systems, intelligent switching to avoid unnecessary momentary interruptions, and advanced assessments of loading issues for reconfiguration.

Technology Recommendation: Advanced Control Strategies

Advanced tools, technologies and systems are improving operator control over uncertainties (e.g. voltage, reactive power, frequency, reserves, distributed energy resources and renewables). To continue to improve reliability, safety and compliance with reserve standards, utilities should implement the following recommendations to take advantage of advanced control strategies:

The first step is for utilities to implement advanced operator analysis / control tools including:

1. Voltage control: Perform hierarchical voltage control studies and reactive power management using new tools for optimum VAR reserve allocation (capacitor banks, dynamic VAR, generation, etc.). The utility will drive research by third parties and implement the results in their system. Familiarity should also be gained with power electronics from inverter-based wind sources.
2. Frequency control: the utility will apply analytical approaches for allocation of damping resources.
3. Automate operator controls: Research is ongoing into automatically coordinating all VAR reserves in a logical way as part of operations. China is the world leader in closed loop control. PJM is doing off line studies on open loop control. The utility will explore using PMUs to monitor VAR flow and reserve management.
4. Control systems for renewables and distributed energy resources: Commercial systems exist to support automatic system response, frequency support, and voltage regulation. The utility will evaluate these approaches and tech watch emerging advances in this field.
5. Investigate emerging power electronics technologies to support reactive power management, active control, and sufficient damping capability.
6. Flexible AC transmission systems (FACTS): FACTS systems have great potential, particularly in voltage support. However, maintenance costs are high. Reliability, availability and initial cost need to improve for FACTS to be widely accepted.
7. Improve ancillary services management
8. Utilize reactive power management and voltage stability study tools and techniques
9. Engage in reactive power planning, or volt VAR planning to find the most economic investment plan for new reactive sources at selected load buses while ensuring proper voltage profile and satisfying operational constraints.

Finally, the implementation of operational control strategies and capabilities in preparation for greater diversity in the generation portfolio (eg to accommodate distributed energy resources) is also important. The timeline for the medium and long-term required activities in addition to the near term recommendations is required here.

Technology Recommendation: Substation Data Managers (SDM)

The wide implementation of substation data managers (SDMs) or substation gateway devices has been a recurring theme in smart grid Roadmaps and is amply justified. Starting with the initial purpose of providing a cost effective external interface to the new IP network at each substation, SDMs value can be expanded incrementally. SDMs may be installed in conjunction with a router/firewall for electronic security perimeter implementation. SDMs will serve as a data concentrator for all substation IED operational and non-operational data and

will include all common standard and custom (eg SEL) protocols and templates. Device will incorporate a range of security applications to facilitate secure remote data access including pass through. SDMs will provide local data storage and HMI functions and will support extension expansion capabilities. WAN data loading models should include the requirement for widespread implementation of SDMs.

Given the importance of Substation Data Managers (SDM) in grid modernization an overview of the SDM follows:

- Equipped with all defined substation serial and LAN interfaces and media.
- Includes support for all standard and select custom serial and LAN protocols for external interfaces to enable a migration strategy of hybrid mixtures of old and new devices.
- Equipped with standard and legacy IED protocols and data formats plus configuration support templates.
- Support for the new DNP Secure Authentication Specification and compliant with IEEE Std 1686
- Provides a comprehensive suite of secure applications such as SSL/TLS, SSH, HTTPS and SFTP
- Includes applications such as PAM (Password Authentication Module) for local authentication and access control.
- Equipped with network management applications: SNMP and SysLog.
- Provides integrated automation applications or user programming for local intelligent applications such as equipment monitoring applications, volt/var control, auto-reconfiguration, auto-restoration.
- Capable of automatically retrieving, storing, forwarding disturbance & fault records.
- Support for connection to a precision time source such as a Global Positioning System (GPS) time signal and distribution within the substation
- Includes applications for integrated on-line and separate off-line configuration.
- Includes a facility for secure local or remote configuration upload, download, verification and version control.
- Provides facility for secure local or remote firmware download, verification and version control.
- Functions may be performed by multiple devices such as hardened routers, legacy data concentrators.
- Integrated support for local human machine interface and annunciator displays.
- Options for redundant communication ports, power supplies and operation with other (redundant) SDMs.

- Integrated local data logging with future support for local data historian.
- Compliant with stringent environmental requirements with no fans or moving parts
- Designed to abstract the authentication, authorization and addressing for all remote device and data access. It resides at the substation and will integrate with the utility's enterprise and identity management servers, eliminating the need for community logins and published IP addresses for individual IEDs.
- Future support for IEC 61850 protocol with related security applications (IEC 62351) plus substation Configuration Language (SCL) support for substation and IED configuration.

Bearing in mind the SDM overview just described, the primary recommendations concerning the wide deployment of SDMs include:

- Widely implement substation data managers or substation gateway devices for the initial purpose of providing a cost effective replacement for the RTU function and IED data concentration as well as local HMI.
- In the future the SDM will provide an effective external interface to the new IP network at each substation. SDM may be installed in conjunction with a router/firewall for electronic security perimeter implementation.
- SDM should serve as a data concentrator for all substation IED non-operational data and will include all common standard and custom (eg SEL) protocols and templates. Devices must incorporate a range of security applications to facilitate secure remote data access including pass through.
- SDM should provide local data storage and HMI functions and will support extensive expansion capabilities. WAN data loading models should include the requirement for widespread implementation of SDMs.

Some of the many Benefits/Rationale for SDMs include:

- Non-operational data acquisition & storage
- Reliable platform for automation and analysis applications
- Secure remote access (pass through)
- Lower cost than discrete components
- Improved configuration tools

The emerging technology trends and Industry best practices include:

- Broad implementation of current generation data concentrator/gateway
- Effective management of operational and non-operational data types
- Cyber security applications
- Local data storage
- Redundant options, IEEE 1613
- Local user interface (web server/client)

- Dedicated SDM for non-op data
- Effective IED data integration & management of operational and non-operational data types (including application for automatic event record storage and forward to enterprise client)
- Support for DNP3, DNP3/IP, IEC 61850
- Support for a wide range of IED legacy protocols and configuration templates
- IED / Substation Data Manager maintenance server at the control center
- Drag and drop and other configuration assist tools
- Local data storage (removable)
- Options for redundancy
- Fanless and hardened for the environment per IEEE 1613 and IEC 61850-3
- Integrated local user interface function including web browser server/client

Finally, the technology and industry Maturity of this recommendation is based on the following:

- First SDMs appeared in 2004
- Large installations in Florida, Ontario, Quebec
- Growing number of utilities
- Cybectec/Cooper and Subnet/SEL have offerings.
- Some suppliers have a good product vision and plan but are slow in getting product out so it is important to ask for test samples and conduct a thorough lab test before selecting the vendor
- Future upgrade to a proxy server.

Technology Recommendation: Fault/Disturbance Event Retrieval and Analysis

A component of grid management and improved reliability is fault/disturbance events and analysis. Utilities must widely deploy or connect to existing substation based protection relays, Power Quality (PQ) meters and/or Digital Fault Recorders (DFRs) configured to record disturbances and faults. Implement Substation Data Managers or other data concentrator devices capable of automatically retrieving, storing and forwarding a wide range of data record types using standard and custom protocols in a secure manner. This deployment includes developing an overall strategy, design, and procurement practices substation data managers, local storage devices, secure remote access to substation IED's, enterprise servers with security applications and access control and related equipment. This topic area also includes the applications necessary to support automatic fault and disturbance analysis for a range of purposes such as line fault location. Other applications can be considered that use the same data such a protection performance analysis. This effort has close ties to the Substation Data Manager topic area to facilitate secure and reliable information

exchange. WAN data loading models should include the requirement for widespread fault record retrieval.

The primary Benefits/Rationale are:

- Broad access to valuable (90%) of the substation non-operational data
- Faster (few minutes) and automatic availability of fault records for engineers
- Accurate (vs relays) fault location and other key data provided to EMS operator within minutes

The emerging technology trends and Industry best practices are:

- Use of SDM for fault/disturbance record retrieval and storage of other non-operational data types.
- Application to coordinate fault record management with central host
- Secure pass through to station IEDs for native IED software
- Wide enterprise access to central host.

The technology and industry Maturity of this recommendation is:

- Growing number of suppliers serve this space including SoftStuff, Subnet, Cybectec and GE
- Large number of utilities doing or planning to do this
- Future – automated fault analysis including fault location, fault anticipation/prediction and protection performance.

Technology Recommendation: Phasor Measurement Data Gathering and Storage

The objective to help achieve more timely and accurate information about the state of the grid requires the wide implementation phasor measurement network for the utility and inter-connected regional entities supporting grid visualization, situational awareness, phasor based control actions and operator decision support.

Associates recommendations include the establishment of comprehensive requirements addressing all aspects of phasor data collection and communication in cooperation with the utility equipment owners and regional grid operators. Increasingly phasor data will be used for critical operational applications and decision making. Therefore the requirements will include hardened network components, detailed service level agreements (QOS) where applicable, cyber security, availability, protocol and other standards. In addition the requirements should establish an understanding regarding static and dynamic measurement accuracy and class, time synchronization accuracy.

The utility must plan for the migration from non-standard protocols and the current IEEE C37.118 to the new communications method being defined for IEC 61850. Continue with the evolution of the applications for the ePDC, and RTDMS. Develop and implement a policy for long term data storage including

data types, durations, granularity and compression. Continue coordination with WECC in the pursuit of integration and application sharing as part of the WISP program.

In the future, as phasor applications mature, plan for the integration of the outputs of phasor applications with the market simulator. In addition, plan for integration with the future NASPInet. Recommendations for the proposed implementation plan for synchrophasors are offered here:

- Robust, standards based, secure communications
- Hardened components where necessary
- Migrate from non-standard protocols and IEEE C37.118 to IEC 61850-90-5
- Address current and pending security requirements as the application of phasor data transitions from off-line analysis to real time operational applications and automatic control.
- Continue product evolution with – ePDC, RTDMS
- Integration with WISP
- Define utility policy for long term data storage including granularity, keeping what type of data?
- Compression for storage purposes
- Integration of phasor applications with the market simulator
- Establish clear requirements with utilities on data availability and infrastructure requirements
- NASPInet

Industry Best Practice

- Statewide penetration of phasor measurement units or phasor equipped relays with GPS
- Phasor data concentrators at key substations and central location(s)
- Communications network to PMUs and PDCs:
- Standard protocols, reliable, secure
- QOS support with SLAs
- Long term data storage
- Communications to regional/national Super PDC
- Applications for operator visualization, VSA/DSA, oscillation detection, dynamic rating
- Methods, practices and applications for situational awareness and operator training

Benefit/Rationale = Reliability & Efficiency

- Operator visualization / situational awareness Tools
- Oscillation (Mode) Detection
- Nomogram / model validation
- Small-signal stability assessment
- Line impedance / dynamic rating
- Market benefit – increased capacity

Some challenges include the communications infrastructure and application development as well as others.

The technology and industry Maturity of this recommendation is:

- TVA, BPA, Entergy, SCE, APS, BC Hydro, WAPA, others have large installations of PMUs
- Industry needs focus & academic involvement in applications & standard PDCs
- Standards migration and new functions are being defined (IEEE, IEC, NIST PAP-13)
- New projects (DOE funding) driving development
- Vendors such as EPG, Space-Time Insight and ABB are offering a growing suite of applications
- NASPInet is being defined
- Clear requirements for cyber security are pending
- Future possible use of phasor data to trigger RASs

Technology Recommendation: Increase the On-Line Monitoring of Key Assets such as Power Transformers and Lines

Adopting state of the art strategies and systems to manage these assets cost effectively offers the best return on the utility's grid modernization investment over the next decade. Medium and long-term Roadmap activities under this initiative are shown in the Timeline. In the near term, utilities should undertake the following actions to optimize asset management:

1. Maximize the value of existing investments
    a. Increase line throughput by managing demand peaks, and/or filling in off-peak valleys. This strategy includes utilizing bulk energy storage to manage peak demand and other valley fill strategies.
    b. Maximize existing transmission Right of Way (ROW) use. Evaluate and implement advanced transmission line design tools to increase ROW efficiency and utilization (e.g. voltage upgrade, compact line design). The tools for this action include technologies to upgrade 161 kV to 230 kV

on existing ROW. This typically requires compact line design. The upgrade may use existing structures and insulators.

c. Implement Dynamic Thermal Circuit Rating (DTCR) applications to estimate optimal line ratings and increase throughput. DTCR is principally used to defer transmission expansion, or as a stopgap until transmission is built. The decision applications and feasible decision time horizon to use DTCR data are unresolved questions. As environmental parameters change the ability to leverage DTCR may change rapidly.

2. Improve maintenance and operations to maximize the value of investments

   a. Automate work management systems. Explore using hand held devices (tablets, iPADS) to improve worker efficiency. Seek out solutions involving process change and technology to improve work management system efficiency. Technology innovation includes using GIS systems and integrating data across the enterprise.

   b. Sensors and analytics: Explore data analysis applications such as Prism by Instep Software, Smart Signal, and other similar tools to increase the value and use of sensor data. Continue participation in sensor development research, especially with regard to sensor data analysis and management.

   c. Advanced sensors implementation to support maintenance and equipment diagnostics – sensor data collection, data management, and data analytics infrastructure

3. Evaluate advanced components

   a. Assess advanced conductors for new and existing lines. Advanced conductors can deliver more power and lower losses than conventional equivalents

   b. Use Volt/VAR control systems to maximize power transfer capabilities

   c. Assess Cost-Competitive Storage Options. Focus on Bulk Storage to Reduce Congestion and Losses.

   d. Maintain a technology watch on Superconductivity and HVDC. These have potential value to the utility but are not crucial for success. Superconductivity remains very expensive and a niche market. In essentially all project scenarios, existing technologies offer less expensive solutions compared to an unsubsidized superconductor solution. The potential for HVDC has increased because it supports long distance renewable resource integration. Converter station costs continue to be an obstacle

Long term monitoring and management of key assets in meeting utility needs of the future is a key component of grid modernization. Key recommendations include:

- Develop an asset monitoring strategy for distribution substations and key lines sourcing these stations. Strategy should cover:

- Definition of risk categories based on probability of a failure or scenario of a given severity and the expected impact
- How condition data would be used as part of the overall asset management and operations utilization functions
- The expected impact on asset maintenance practices if condition data is available
- Technologies to be considered and tested
- Identify highest risk power transformers and lines for testing
- Select the optimal range of technologies and communications solutions for each risk category
- Begin deployment

The primary Benefits/Rationale for key asset management and monitoring are:

- Enhanced condition information for transformer units and lines:
- Reduce probability of failures and outages
- Change maintenance practices to condition based
- Support dynamic utilization by operations for reliability and maintenance

The current Industry best practices include the following:

- Multiple integrated transformer & line monitoring devices
- Condition based maintenance using reliability centered maintenance (RCM) methods with real time condition data
- Dynamic loading capability of each asset continuously calculated & provided to EMS operator
- Input for State Estimator and Contingency Analysis applications

Finally, the technology and industry Maturity of this recommendation is:

- Power transformers
- Fault gas monitoring is addressed by a number of established suppliers (such as GE Syprotec, Harley, Kelman, and Serveron)
- Transformer dynamic rating is addressed by GE and Dynamic Ratings who have been supplying products with these functions (unit dynamic rating) for 5+ years.
- A number of large installations
- Line monitoring -
- Variety of sensor suppliers exist
- No line dynamic rating suppliers – just sensors at this time.
- Future – integrate real time sensor and analysis information into the asset management application

Technology Recommendation: Implement automated tools for WAN Monitoring

Implement automated tools for control, capacity planning, traffic simulation, and application to bit stream level utilization and bandwidth monitoring of the wide area communications network (WAN) to maximize asset utilization, improve its operational and cost effectiveness and as a result, defer capital expenditure until truly necessary. These WAN management tools will facilitate preparing for the significant growth in the number of devices and applications associated with the smart grid that produce, consume, and manipulate data that will utilize the WAN for its transport.

Optimization, reliability, and better workforce management are some Benefits/Rationale to implementing this recommendation in addition to the following:

- Able to derive maximum benefit for the utility of the investment in SONET (including upgrade) and other elements of the communications infrastructure
- Maximize system utilization
- Defer capital costs
- May enable direct or indirect reliability enhancement

The current state of Industry best practice includes: wide range of off the shelf management for monitoring WAN, application level utilization management, unified WAN management tools, WAN cyber security policy, WAN traffic simulation tools for planning,

Finally, the technology and industry Maturity of this recommendation is: some good tools exist, unified WAN management tools continue to improve, traffic simulation tools that can help plan for smart grid bandwidth and facility planning.

Technology Recommendation: Electric System Data Acquisition and Data Management

Utilities should widely deploy substation, feeder, and transmission line asset data acquisition, aggregation and management systems to improve the operational effectiveness of the system. These systems will include wider deployment of advanced voltage, frequency, current, phasor, and physical parameter sensing devices and their associated systems to facilitate better situational awareness and the ability to operate the system more efficiently, reliably, and securely. This deployment includes developing an overall strategy, design, and procurement practices for asset management systems, substation data archivers and managers, secure remote access to substation IED's, substation management consoles and related equipment. This topic area also includes the applications necessary to support dynamic rating for transformers, feeders, and transmission lines. This effort has close ties to the integrated substation LAN topic area to facilitate secure and reliable information exchange.

Primary Benefits/Rationale of these enhanced data acquisition and management recommendations include:

- Integration policy, guidelines and requirements process in place
- Enhanced cyber security external and internal to substations
- Reduced capital and installation costs for new substations
- Engineering effort reduction for substation data retrieval
- Reduced field efforts with faster/more accurate fault location data
- Lower probability of costly asset failures
- Optimized and flexible utilization of assets
- Reduced apparatus maintenance costs using condition information
- System wide (operational) security enhancement & black start assistance with phasor data operator displays

Currently, the Industry best practices include:

- Broad implementation of current generation data concentrator/gateway (effective management of operational and non-operational data types including event records, comprehensive suite of cyber security applications and features, and secure enterprise wide access to substation real time and event data)
- Risk based wide implementation of transformer and transmission line monitoring enabling dynamic loading capability for operator dispatch
- Analysis based broad installation of phasor measurement units and related equipment (eg GPS) with displays for system operator and direct connection to regional (WECC) and national phasor databases

Technology Recommendation: Broad Condition Monitoring of Key Transformers and Lines with Integrated Analysis

With the greatly enhanced quality and quantity of sensor data from almost all points within the grid, a utilities can begin to plan for and implement a variety of on-line condition monitoring of substation transformers and transmission line providing asset data acquisition, aggregation and management systems to deliver on-line condition information to asset management, maintenance engineering, field staff and system operations. This effort would include the development of comprehensive, cross functional application and requirements definitions as well as policies and guidelines and conducting additional pilot testing and sensor selection and begin deployment of sensors where substation data managers or other data gathering devices are present. In addition, define the requirements and implementations of the applications necessary to support condition monitoring and diagnostics, including dynamic rating for transformers and transmission lines. Finally, this effort has close ties to the integrated substation LAN and Substation Data Manager topic areas to facilitate secure and reliable information exchange.

The primary Benefit/Rationale drivers for conditioned base maintenance include:

- Enhanced condition status of units and lines for reliability and maintenance
- Avoided failures
- Enables operator to reliably extend utilization of assets for periods of time.

Emerging Technology Trends

- Multiple integrated transformers
- Multiple sensor (system) monitoring of Lines
- Dynamic loading capability of each continuously calculated.
- Data provided to EMS operator
- Input for State Estimator and Contingency Analysis applications

The technology and industry Maturity of this recommendation is:

- Several vendors have been supplying products with these functions (unit dynamic rating) for 5+ years.
- A number of large customers have experience with these techniques

(6) Technology Recommendation Theme: Advanced Forecasting and Modeling (Load and Variable Generation)

Advanced power systems modeling (both distribution and transmission) and forecasting are now practical for utilities to undertake because of the convergence of widespread high resolution sensors, high speed communications infrastructure, and high speed (and affordable) computing resources.

A utility objective to be a leader in advanced forecasting accounting for variability introduced by renewable generation and incentive based programs, minimizing forecast error for optimal unit commitment is now not only feasible, but a necessity for future grid operations.

Utility Operations should enhance its operational tools in order to provide advanced capabilities for situational awareness and economic dispatch optimized for more volatile grid conditions. Advanced Forecasting is one of these tools and includes 1) forecasting renewable resources, 2) sub-regional load forecasts along with 3) availability of emerging demand response resources. Improving weather forecasting for renewable generators, will give operators a tool to gauge current grid conditions and better anticipate generation levels 15 to 30 minutes into the future and set resources to respond appropriately. Market-based dispatch continues to be an area that supports the efficient and economical utilization of the system. A more economic grid dispatch is possible by supplementing current systems with advanced forecasting tools. No longer is demand response a resource only available during emergencies. Price-responsive demand response holds the promise of becoming a valuable fulltime participant in new the utility

markets through enhanced dispatchability that makes it integral to offsetting the intermittent nature of renewables.

Because renewable resources are weather dependent, available supply will swing 30 percent, depending on location, resource type (e.g., wind or solar) and specific technology, which makes system balancing more challenging. The utility should improve the use of weather forecasts. Wind and solar renewable generators have highly variable energy production as they depend on the wind blowing and the sun shining. As the amount of renewable generation in California increases, the existing fleet of traditional generators will be called upon more than ever before to ramp up and ramp down their production to compensate for the variability of renewable power production. In addition, the existing fleet will need to provide more regulation energy to maintain grid stability within the parameters set by NERC reliability standards. To adapt to this new operating reality, the utility should adopt procedures and modify existing ones to create more sophisticated forecasting and dispatch tools to manage grid voltages and transmission line loadings as more renewable generation comes online.

Increased amounts of weather-dependent renewable resources drives the need for major improvements in forecasting capabilities in order to "see" what conditions will be minutes and hours ahead and respond appropriately. Renewable resources outputs are directly affected by cloud cover, moisture or dust in the air, and wind conditions. Improved forecasting tools should be developed to help identify transmission facilities that may overload or areas of undersupply. Promising tools should include sub regional load forecasting, short-term event predictor and ramp-forecasting tools that would allow grid operators to anticipate major events by recognizing correlated meteorological and system events.

The following technology recommendations for modeling and forecasting were deemed most relevant for this summary document:

- Develop a database of load profiles that are segmented by energy usage
- Develop a set of DR scenarios to develop programs against
- Look at First Generation Wind Shear Radar (surplus) for wind farm forecasting
- Experiment with higher granularity forecasting data
- Look at 3-D weather models
- Develop a range of scenarios for forecasting to create a forecasting band
- Develop a forecasting game to allow for the testing of new forecasting ideas
- Develop a DER database for the state and include charge stations (pick a starting size as a first pass, pick an area to look at smaller DER sizes and their impact, look at high density areas with lots of small DER)
- Model the impact of building code changes on new developments (i.e. develop a ramp rate database for all DER and Generation Sources, including weather related ramps and cutouts)

- Look at using cloud cover from satellites for short term PV forecasting, including smoke as well
- Determine how rain and fires will impact transportation, usage and supply in the model
- Look at a long term forecasting model that will allow the development of targeted incentives for DER
- Apply trading Risk Management Techniques to forecasts to get "mark to market" and "quality" ratings for 24 hour and longer forecasting periods

Industry best practices have made dramatic strides in the last few years and include:

- Use of national and international weather forecast providers (e.g. NOAA/NWS/Earth Resource)
- Utilize forecast service providers for renewable forecasting
- Weather data specific for day ahead forecast, hour ahead rolling forecast, and park specific forecast
- Use of wind shear radars for short term forecasting on large wind farms
- Generator availability, near real-time and historical meter data as input to forecast
- Algorithms for ramping and filtering and neural network
- Inclusion of confidence bands in results
- Bottom up load forecast with 13 part profiles by segment or major customer
- Scenario based profiling to provide a band of likely outcomes
- Demand Response forecasting system for value of each DR program at a specific interval
- Database of actual information to use as basis for forecasting

The following Benefits/Rationale helps justify the importance of enhanced forecasting and modeling:

- Improved accuracy in unit commitment
- Reduction of cost through more accurate procurement of Ancillary Services and load following energy
- Matching load to available supply
- Lower import requirements
- Reduction in congestion
- Better utilization of renewables
- Less demand on peakers and that reduces emissions

Naturally, some challenges exist including: field Measurement equipment for weather and DERs, quantity, location and quality, latency in data arrival, forecasting algorithms, quality of existing data on the load side, privacy and security, and range of DR programs.

The technology and industry Maturity of this recommendation is: majority of forecast applications used by the industry are custom designed, DER Identification, location, max output, acceptable Forecast error is defined, solar, standard forecasts techniques for ST and PV units, intra hour forecasting is developed, wind, NWS/NOAA forecast improvement, boundary layer forecast, forward observation points, LiDAR usage, doppler usage, system GUIs, consensus forecasts, forecast price responsive demand, forecast ramping events requirements defined, bottom up segmented forecasts being developed, and the use of portfolio of DR resources to balance the system.

Technology Recommendation: Modeling and Analytical Tools for Planning and Operations

In order to continue improving reliability, cost-effectiveness and security/compliance, utilities must invest time and resources into advanced planning, modeling and operational tools. These tools provide an accurate and integrated decision support environment that improves the utility's ability to operate the grid reliably and cost effectively. Operational tools also assist with compliance and security monitoring.

Many of these recommendations are foundational – laying the groundwork for advanced systems to capture and process data in a timely manner and for data integration across systems. The utility will also evaluate and deploy advanced tools to improve planning, modeling and system operations, especially in areas such as renewable generation where new uncertainties complicate the operating environment. The following discussion describes three primary areas in greater detail: Planning, Modeling, and Operations.

Utility planning processes will necessarily have to change to meet the changing requirements of variable generation and weather impacts on both sources and loads. Large-scale variable generation integration, the conventional generation retirement and increasing demand response add uncertainty in planning and operations and may alter the reliability landscape. Risk-based approaches help justify and prioritize long-term capital investments, and help secure appropriate resources to meet operational needs. Available Transmission Availability Data System (TADS), Generating Availability Data System (GADS) and Demand Response Availability Data System (DADS) data provided by NERC facilitate probabilistic techniques.

Roadmap planning for modeling and analytical tools involves the following the utility actions:

1. Evaluate and implement risked-based (probabilistic) planning tools that incorporate variable generation and demand response intermittency.

2. Assist in developing and incorporating new models for customer response, distributor programs, market conditions, etc.
3. Expand planning strategy to incorporate improved economic analysis, including the following efficiency improvements (e.g. for asset utilization): equipment and system specifications for optimum lifetime investment, and utilize tools to assess advanced conductors for new and existing lines. Advanced conductors deliver more power and lower losses than conventional equivalents.
4. Broaden area planning for inter-regional expansion, including cost allocation and siting. The utility will participate in broader planning forums required by FERC Order 1000.
5. Expand transmission and resource planning to include unknown renewable resource expansion and reserves determination. Incorporate carbon tax impact and other future scenarios into the planning process. Estimate how generation cycling effects total operation cost (including efficiency, reliability, and life).
6. Improve utility understanding about bulk energy storage and demand resource planning. The ability to charge and discharge bulk storage potentially improves system reliability and reduces curtailment and congestion costs associated with integrating variable renewable generation. However, optimizing bulk energy storage charging and discharge as well as identifying appropriate storage locations requires complex algorithms not found in current planning models. Similar complex analysis is required to manage demand response. To gain operational experience, utilities should deploy and operate bulk energy storage systems. The utility is already familiar with pumped storage (Raccoon Mountain). Lithium ion would be a good candidate for deployment, as it appears to be the front-runner in chemical storage.

Secondly, modeling will play an increasingly important role as well since electricity is generated and consumed immediately, system optimization, reliability, cost control, safety, etc. is extensively modeled offline to improve performance. Current model environments are clustered around specific applications and generate data silos that are difficult to share. The utility grid modernization roadmap includes the following actions to improve modeling quality and integration:

1. Design and implement a model management system that can support future planning, operations, and asset management requirements. The model management system should have a single database with a standard object naming convention. Redundancy and security needs are addressed as well as sharing and updating responsibilities. For example when a shared model is used by operations and planning, the utility is able to export the data throughout the enterprise. The model management system should handle data from multiple sources such as SCADA, sensors, IEDs and PMUs as well as distributors and customers.

2. Improve utility familiarity with modeling emerging advanced power system components. These components include wind turbines, solar systems, energy storage devices, PHEV, and end use loads.
3. Evaluate advanced models for generators, renewables, distributed resources, and demand response. Power flow and dynamic models will be developed for new equipment such as HVDC as well as supply-side and demand-side devices. In some instances, three-phase models are required to conduct electromagnetic transient studies (e.g. sub synchronous resonance (SSR) studies).
4. Validate and continuously update models. This is both good practice and a NERC requirement, (e.g. NERC MOD 26 and 27). The utility has the appropriate measurement systems for validation in place and will participate in industry committees promoting validations as a high priority. The utility can also evaluate and test emerging vendor models.
5. Improve load modeling by evaluating available enhanced analytical approaches and monitoring R&D work in this area. The scope of this activity will also include developing demand response and plug-in electric vehicle modeling among other emerging technologies.

Finally, concurrent with planning and improved modeling, are operational tools. The data available to system operators is steadily increasing in volume as the environment becomes more complex and decision support is closer to real time. There are more transactions and new, novel devices are being added to the system. New line construction has lagged at an industry level. It is crucial that operators know their operator margins, and the direction the system is moving. Additionally, tools to help operators take corrective action are needed. New and advanced tools are improving situational awareness and decision support in operations. The utility should take the following actions to ensure that they are familiar with (and where appropriate) using advanced operational tools:

1. Improve state estimation and situational awareness using advanced models in real time fed by PMU data. Increased system status information and power system measurements accelerate EMS convergence. Research is needed to determine the optimum number and placement of the PMU's. Algorithms for state estimation need to be upgraded to resolve more quickly. Utilities should work with their EMS vendor to incorporate PMU data into the state estimator to improve situational awareness.
2. Improve contingency analysis quality and speed to filter out important system events and integrate real time information on equipment health. The utility is participating in EPRI programs to assess equipment health (transformers and breakers).
3. Build decision support tools for system performance optimization, system security, and reliability (expert systems, pattern recognition, etc.) Operating reserves are expensive and optimizing the reserves in today's more uncertain environment is difficult.

4. Increase forecasting quality and frequency. Gains in short term forecasting have been achieved. Long term forecasting is more uncertain and does not appear to be improving in accuracy. Solar remains in its infancy. The utility should evaluate vendor-forecasting tools including new tools measuring renewables and customer response characteristics.
5. Evaluate advanced human-centric visualization tools for the following capabilities: improved wide area oscillation, voltage, and transient stability margin analysis using PMU data. The utility will participate in industry committees to develop applications, utilize tools to visualize multi-dimensional operating boundaries. The utility will work with their EMS vendor to develop a simplified display and enhance operator awareness (balancing variable generation and load, storage, volt/VAR control, reserve management).
6. Evaluate using operator-training simulators that develop credible grid scale and operating characteristic simulations. Capturing and replaying large-scale events, various generation dispatch and loading models, etc are a challenge. Capturing and replaying limited grid models with high-speed data from synchrophasors should help create more credible simulators and improve operator training.
7. Evaluate and implement tools and methods to help operators restore the system after a blackout. Utilities need tools that can help operators identify optimal restoration paths and their sequence when the system is being restored in a step-by-step fashion following a major blackout.

Technology Recommendation Theme: Enabling Distributed Energy Resources

Almost all of technology recommendations previously outlined lay the foundation for a utility to be able to efficiently utilize, operate, and reliably provide power to their customers in the evolving and ever higher penetration scenarios of DER. Meeting the overall objective of deploying infrastructure built on national business and interface standards that provide the flexibility to support advanced storage, DR, and DER applications is key.

Addressing emerging issues that have been identified in the many Smart Grid Roadmaps requires that the utility adopt a robust and flexible system architecture that builds upon recent MRTU design. Guiding principles from industry organizations such as GridWise Architecture (Smart Grid Framework) and OASIS (for SOA) should be adhered to. When possible web based services from IETF based RFCs and OASIS standards should be used for information exchange (e.g. TCP/IP) and data definitions (i.e. Open ADE). the utility must evaluate the extensibility of the current operational communication systems such as ECN and VPN-based Internet against growing performance requirements. The utility may need to explore alternative mid-tier communication infrastructures going forward. As NERC cyber security requirements become more stringent, the utility should develop a thorough security policy implementing the guidelines listed in NISTIR 7628, Cyber Security for Utilities, August 2010. Additional systems and components should be supplied using internationally agreed upon standards for information models and interfaces.

These include the Common Information Model - CIM (IEC 61968/61970) for centrally managed network model, and for communication to field devices and resources - Secure DNP 3.0 (IEEE Std. 1815), and IEC 16850. Utilities will be required by FERC to implement resource targeted Tariffs to meet adopted policy and regulations under FERC Order 719. Adoption of AutoDR will support these requirements. As more market participants provide resources to the utility, an extensible and highly reliable price delivery mechanism must be created to provide enrollment in a real-time Publish/Subscribe service that updates LMP locational pricing and system conditions.

State by state and with large regulatory input, the entire arena of DER often is in the limelight. Given these drivers, the following technology recommendations were deemed most relevant for this summary document:

- Work toward definitions of standard interactions/interfaces including using consensus CIM models for external interfaces
- Continue to implement Service Oriented Architecture:
- Web services for remaining candidate interfaces
- Fine grained business services
- Centrally managed network model
- Implement IEEE Std 1815 (DNP3) Secure Authentication specification
- Establish quality and reliability metrics for prices
- Implement Pub/Sub for locational system condition
- Adopt emerging OpenADR standards (NIST/FERC/NAESB)
- Clear mapping of business requirements to determine mid-tier communications infrastructure

The current Industry best practices for DER include:

- Public Internet communications with clear SLAs
- CIM as a reference model (internal/external)
- Service-oriented Architectures
- OpenADR specification as currently defined
- Adoption of other open standards such as GreenButton
- Moving toward with new version (NIST/NAESB/FERC) of OpenADR
- NAESB Std. DR Business Practices
- Centrally managed network model
- Transitioning to IEC 61850 based communications with field devices
- Transitioning to CIM based communications with external control centers
- Comparable treatment for supply and demand (Fully compliant with FERC Order 719)

- Inverter communications compliant with IEEE 1547 (today), DNP3 and IEC 61850-7-420 in the future
- New forecasting methods for DER

Benefit/Rationale

- Cheaper and quicker internal and external integration
- Reduce barriers for Storage, DR, and DER participation in utility markets
- Additional types of resources to balance intermittency due to renewable integration
- Increased choice of vendors
- Facilitate price/grid condition responsive DER

Naturally, challenges that have arisen to implementing these recommendations include:

- Disconnect between wholesale price/grid conditions and retail prices
- Security of the public Internet
- Handling potential significant increase in number of connections and resources modeled and dispatched in the market systems
- IT Resource availability
- Range of DR programs
- Maturity of OpenADR and inverter communication standards
- Technology maturing and operational characteristics not well-understood

Finally, the technology and industry Maturity of this recommendation is:

- Public Internet is proven technology however service provider performance varies widely
- Standards based interfaces widely implemented
- Finer granularity business services widely implemented
- Pub/sub model for prices
- More granular prices
- Quality and reliability metrics for prices
- Pub/Sub for locational system condition
- Integration of storage in utility markets is beginning
- Inverter communication standards are moving toward new standard status
- Use of portfolio of DR programs to balance the system

Technology Recommendation: Plan and pilot test new infrastructure elements for DER and Microgrids

To help meet some of the challenges and evolving requirements outlined in the previous recommendation, this final section address the continuing need for planning and pilots which investigate some of the more pressing issues more thoroughly. Most utilities and industry observers would agree with the following current observations:

- Distributed Energy Resources will play an increasingly important role
- Demand response is a DER and suitable for cheap peak management
- PHEV penetration will increase rapidly post 2010
- PV technology is viable in the Southeastern US
- Thermal storage (e.g. Ice Bear) is a viable peak management tool
- Microgrids hold promise for increased reliability in heavy storm areas

Given these observations, some pertinent recommendations include the following:

- Evaluate the benefit of peak management via DER to defer capital expenditure
- Test thermal storage concepts
- Implement commercial rooftop PV – evaluate utility owned models
- Evaluate readiness of distribution circuits to support high PV penetration
- Evaluate potential for microgrids – is there value in storm situations (develop new planning methods and tools)

The primary Benefits/Rationale for these recommendations includes the following:

- DER can be very cost effective when compared to building new infrastructure to manage peak
- PV in the south is favorable and is an easy means to increase renewable mix
- Being ready for PEV will prevent problems later

The primary Industry best practices are:

- Western and Southwestern states are successfully deploying PV and DR
- The Galvin Initiative has developed recommended best practices for microgrid modeling and deployment
- Ice based thermal storage systems are increasing being used to manage A/C load peak
- Prepare FAN requirements to support extensive penetration of DER technologies over the specified FAN technology life.

- Plan for the support of current or pending industry standards related to the connection of DER technologies such as IEEE 1547 and IEC 61850-4-720

The current technology and industry Maturity of this recommendation is:

- Commercial rooftop PV technology and business model is mature
- Thermal energy storage – especially ice storage – is mature and cost effective
- PHEV integration is in its infancy
- Planning tools to account for DER and DR loads are not mature
- Standards are evolving for DR dispatch
- Microgrid control and planning is in its infancy

This section provides a summary for each of the technology recommendations made in the Roadmaps. The recommendations were developed based on the business objectives and drivers, technology vision statements, key applications

Section 7: Key Insights and Lessons Learned

As an outcome of the many roadmap projects completed to date, common themes have clearly emerged. Some roadmap projects have been more successful than others both in the development of the roadmap and the implementation than others. The insights gained and the lessons learned are summarized below.

Management

The importance of governance, which we define as engaged oversight, has been confirmed with every roadmap project. The governance should involve both the executive level and the management levels. The value of the involvement of executive or senior management in the roadmap process cannot be over stated. The highest levels of the company should all be involved in establishing the company's technology adoption strategy followed by the initiation and oversight of the roadmap project through to completion. This would ideally include the Board of Directors, and Chief Executive Officer, the Chief Financial Officer, the Chief Engineer, the Chief Information Officer, the applicable Executive VPs and Senior VPs or their equivalents. For the design and construction of a major power plant, those executives would be keenly aware of the status of the project and the cost/benefit summaries, status of regulatory and permitting approval. Grid modernization involves the same magnitude of expenditure and requires the same level of oversight and approval. Without this the roadmap report will probably end up in the company library with the other consultant reports that were never implemented.

Note: *The responses to the recent EPRI survey of the Members of the Smart Grid Roadmap Interest Group on the topic of governance, 64.3% indicated that there existed a smart grid oversight group comprised of executives.*

Steering Committee

In terms of governance, the management level must be engaged as well. Each and every successful project has had a steering committee, chaired by a company executive or senior staff member who was responsible for the outcome of the project. They provided guidance to the project, reviewed the status of the project and helped keep the whole team involved in the project, so that it stayed on track and with the best possible results. Without the steering committee, projects tend

to run longer, have lower attendance at workshops, go over budget and return results that are inferior. Additionally parts of the organization have the ability to say "We were not involved and that is not what we want". Without a steering committee the project manager in the utility is climbing steep hill with a heavy load.

Cross-Functional Teams

Many of the utilities that participated in the Roadmap process began to immediately realize tangible benefits in having active cross-functional teams working together to solve common utility challenges. However, to be most effective, this 'silo-busting' objective must almost always require the critical requirement for organizational buy-in and leadership from top management across all departments.

Responsibility

To be successful, roadmap projects need to touch most of the organization. In a typical utility the roadmap touches more than 70 percent of the jobs. Creating a project responsibility matrix and getting buy in from the whole organization is important. Typically a responsibility matrix includes four roles:

1. Responsible – no matter what happens, "the buck stops here." Typically this is the role of the senior executive leading the steering committee and the steering committee.
2. Authorized – these are the people who day-to-day are doing the work.
3. Consulted – these are the people who are expected to be in the meetings, providing input, reviewing documents and commenting. This is an active role in the project and people are expected to make time for this project.
4. Informed – people who will be impacted by the result and so they should know what is going on. However, they are not actively involved in the activity.

In most cases this kind of a matrix lets people know the expectations the project has and how active they are expected to be. Doing this up front and making sure that the people in the roles are keep fully informed means at the end of the project there should be no "Wait, wait, I did not know that was happening" from the organization.

Regulatory

The regulator is a key stakeholder in the roadmap process. They need to be informed and even consulted on what they see as key capabilities that the organization should have as it moves forward.

Review and Updates

A roadmap is never really done, if it is, then it is just a report. Setting a regular review of the roadmap and updating on a regular basis is fundamental to keeping the organization on track. Quarterly reviews on technology changes, regulatory changes, and other items and making updates to the roadmap are important. However a major refresh effort two or three years down the road is usually required.

Benefits Are Not Magic

You don't have a magic wand to make benefits appear on the first day of implementation; in fact benefits typically lag deployment by about a year. Outputs from the roadmap project should be realistic about the lag in benefits. During any major deployment, no one is going to lose a job, in fact in most cases the payroll (including temps, contractors and consultants will rise sharply).

Consumer Involvement

As some prominent utilities found out through negative press coverage and others are also finding out, consumers, both large and small have clear ideas of what they want the grid to be able to do for them. Getting this input early in the process can help calibrate how the public feels about the organization and what needs to be strengthened as part of the modernization effort.

Common Internal and External Drivers:

There are a number of common drivers that underlie the need to modernize the grid. They are:

1. availability / reliability
2. Increasing failures or decreasing performance linked to aging assets
3. changing load profiles and consumption
4. demographic changes
5. regulatory compliance
6. emergence of new technologies including DER and EV
7. operational efficiency
8. asset utilization
9. fiscal responsibility
10. real-time situational awareness for both transmission ***and distribution***
11. cyber security
12. workforce readiness
13. intuitive interfaces / simpler training needs
14. comprehensive cost recovery metrics

Not every utility has all of these drivers at the top level. The prioritization of these drivers changes from utility to utility. It is critical that all of the key drivers get reviewed and an agreed to prioritization happens. Spending 70% of the roadmap effort on the 14th most important driver leads to a roadmap that will not be implemented; this is where the steering committee has to make hard choices about priorities.

Technology is a Big Issue

Regardless of the background of the team, the amount of technology involved in a roadmap is tremendous, typically an order of magnitude more than the team thinks when they start the project. It is not unusual to look at more than 200 technology categories over the development of the roadmap.

Technology is a trap for most teams, they have strong technical people and technology is easier to deal with that the messy regulatory issues. Technology should be discussed at the general level (e.g. HAN) until the final stages of the roadmap. Getting too technical and too specific too early will lead to compromises in other areas of the roadmap that the team is not even aware they are making.

If you are not at the point where you are working on the very bottom row of Figure 7-1 below, you should not be having technology discussions, that go beyond the "we need a two way meter that…".

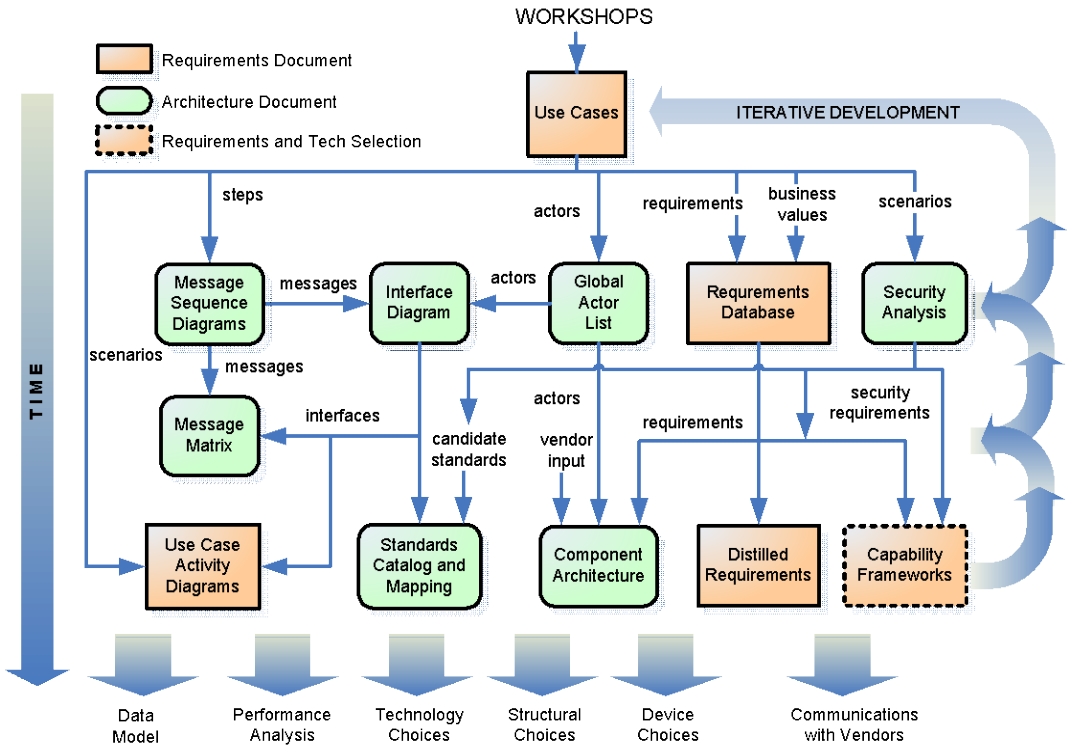


Figure 7-1
The IntelliGrid Architecture Methodology

Current State Knowledge

Knowing the current state of the organization, its equipment and processes is very importation to the use case workshops and how the roadmap is going to impact the organization.

It cannot be stated strongly enough, you need the experts on how it works today in the workshops. That knowledge is critical to determine what the impacts of the changes are whether they will fit.

Walking into the workshops with detailed knowledge of the current processes and the issues with those current processes is important. Similarly knowing what the issues are with the current equipment in the field is critical to the discussions. This includes root-cause analysis of those issues. Spending an hour debating why the System Average Interruption Duration Index (SAIDI) "is what it is" is not a productive discussion. Doing the homework before the meeting and having this information in hand is critical to the workshop. Ideally the "go to" person in the organization should start the workshop off with some facts about where the topic under discussion stands from a key metrics standpoint. Similarly having any regulatory mandates stated clearly up front also helps to frame the discussion.

In short know what the problems are, how big they are and how much it is costing. Creating a $1 billion dollar fix to a $20 million problem seldom gets the green light from either the regulators or senior management.

Communications Technology Assessment Matrix

Communication is a much bigger part of this project than most; not only communication to people about the project (which is not the theme of this discussion) but also the communications with the equipment in the grid and the people working on the grid.

The creation of a matrix that captures all of the requirements as the project progresses for communications and where the communications needs to happen will facilitate technology assessment later in the project. Some of the key communications areas that are common to a roadmap are:

1. Field and Enterprise Communications Infrastructure and Architecture
2. Customer Systems
3. Grid Operations and Control
4. Renewable and Distributed Energy Resources Integration
5. Grid Planning and Asset Efficiency
6. Workforce Effectiveness

When the technology assessment was done, the key evaluation criteria typically included:

1. Maturity
2. Self-description
3. Security
4. Scalability
5. Manageability
6. Standards
7. Openness
8. Users groups
9. Object modeling
10. Power industry reference implementations and support

For a project manager putting each of these criteria into the evaluation sheet ahead of time as categories is useful to make sure all the requirements are captured in workshops and discussion sessions.

Additional evaluation criteria also have emerged in the roadmaps and are found to be useful for communications:

1. Increase reliability
2. Cost
3. Security/safety compliance (risk mitigation, minimize/avoid negative public relations)
4. Risk of obsolescence
5. Regulatory concerns
6. Customer acceptance
7. System integration
8. Ease of interpreting information
9. Maturity
10. Capability
11. Work force requirements
12. Implementation
13. Training and support

System Integration is HUGE

Not only is it huge but it is a specialized topic. Don't try to wrestle it to the ground in the workshops or in the roadmap. Indication that system "A" needs this kind of information (e.g. Customer) from system "B" is the level that is productive. Anything deeper than that in any workshop or group discussion (unless it is the system integration team) will turn off much of the audience and slow the process down. Remember, save those discussions for when the project reaches the bottom row of the IntelliGrid Architecture Process diagram above.

Don't Just Add

Many teams talk about "additions to the technology, new IT systems, new communications systems, new…"

The problem is there are old systems out there too. The roadmap needs to talk about replacement and transition as well as additions. This can be a hard discussion, since no new system will work exactly like an old system and people are used to how the old system works.

Supporting Items

The roadmap by itself is not enough to succeed. Nor is a business case enough support to make the roadmap succeed in implementation. There are several other items that need to happen, that the roadmap can be a catalyst for. They include:

1. Organization-wide integration policy
2. Organization-wide security policy
3. Organization-wide privacy policy
4. Asset-management policy

Training and Change Management

Regardless of the technologies chosen or the timelines developed or any other aspect of the roadmap, one item is constant across all of the roadmaps. Training of the existing workforce has to happen for the deployment to be successful and the organization has to change to meet the new technology half way.

It will be people that will make or break the success of the roadmap and its implementation!

Section 8: Conclusions

The EPRI Smart Grid Roadmap methodology has been found to be an effective tool in assisting utilities to move forward in their grid modernization efforts.

The Smart Grid vision that these Roadmaps embrace should link electric operations, communications, and automated control systems to create a highly automated, responsive, and resilient power delivery system that should both improve services and empower customers to make informed energy decisions. A Smart Grid with these characteristics would support a wide range of current and evolving energy policy goals, including increased penetration of renewable resources, reduced greenhouse gas emissions, increased energy efficiency, implementation of demand response, increased use of distributed energy resources, maintained and/or enhanced grid reliability, and advanced transportation electrification.

Integrated systems introduce more complex cyber security issues, but support a wider range of system options that exhibit lower costs, greater price vs. feature flexibility, and ensure continued improvement in the security of power supply. Therefore, the Smart Grid should place an emphasis on greater protection from cyber security attacks and safeguard customer privacy and worker safety.

The Roadmap process has also illuminated some of the challenges associated with Smart Grid development and deployment—such as maintaining and/or increasing reliability in the face of increased grid complexity and managing technologies.

Appendix A: Bridging from the NIST Catolog of Standards to the IntelliGrid Methodolgy

The NIST Framework - Background

In the Energy Independence and Security Act of 2007 (EISA) made it the policy of the United States to modernize the nation's electricity transmission and distribution system to create a smart electric grid and The American Recovery and Reinvestment Act of 2009 (ARRA) accelerated the development of Smart Grid technologies, investing $4.5 billion for electricity delivery and energy reliability activities to modernize the electric grid and implement demonstration and deployment programs, as part of that investment, The National Institute of Standards and Technology (NIST) received funding to support standards development for smart grid.

To this end NIST held a series of workshops starting with the creation of the Domain Expert Working Groups (DEWG) starting in 2008. The workshops included an architecture workshop in May of 2009 that resulted in the characterization of 7 domains that comprise the overall industry which is shown in the figure below.

The framework uses this diagram and the supporting definitions to help structure the work of the Smart Grid Interoperability Panel (SGIP) that NIST helped form in late 2009. In 2012 NIST published the second version of the framework document "NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 2.0 (NIST Special Publication 1108R2) which is available to the public on the NIST website (nist.gov).

What is the Framework?

The framework in laid out in some detail in the NIST document. NIST talks about the framework this way:

"The expedited development of an interoperability framework and a roadmap for underpinning standards, such as those outlined in this document, is a fundamental aspect of the overall transformation to a Smart Grid infrastructure.

Although electric utilities are ultimately responsible for the safe and reliable operation of the grid, many other participants will be involved in the evolution of the existing electric power infrastructure. Technical contributions from numerous stakeholder communities will be required to realize an interoperable, secure Smart Grid.

Because of the diversity of technical and industrial perspectives involved, most participants in the roadmapping effort are familiar with only subsets of Smart Grid-related standards. Few have detailed knowledge of all pertinent standards, even in their own industrial and technical area. To facilitate broad and balanced input from all Smart Grid stakeholders, the SGIP28 was established:

- To create a forum with balanced stakeholder governance that would bring together stakeholders with expertise in the many various areas necessary for the Smart Grid, including areas such as power engineering, communications, information technology (IT), and systems engineering;
- To support development of consensus for Smart Grid interoperability standards; and
- To provide a source of expert input for the interoperability standards framework and roadmap.

This report contributes to an increased understanding of the key elements critical to realization of the Smart Grid, including standards-related priorities, strengths and weaknesses of individual standards, the level of effective interoperability among different Smart Grid domains, and cybersecurity requirements."

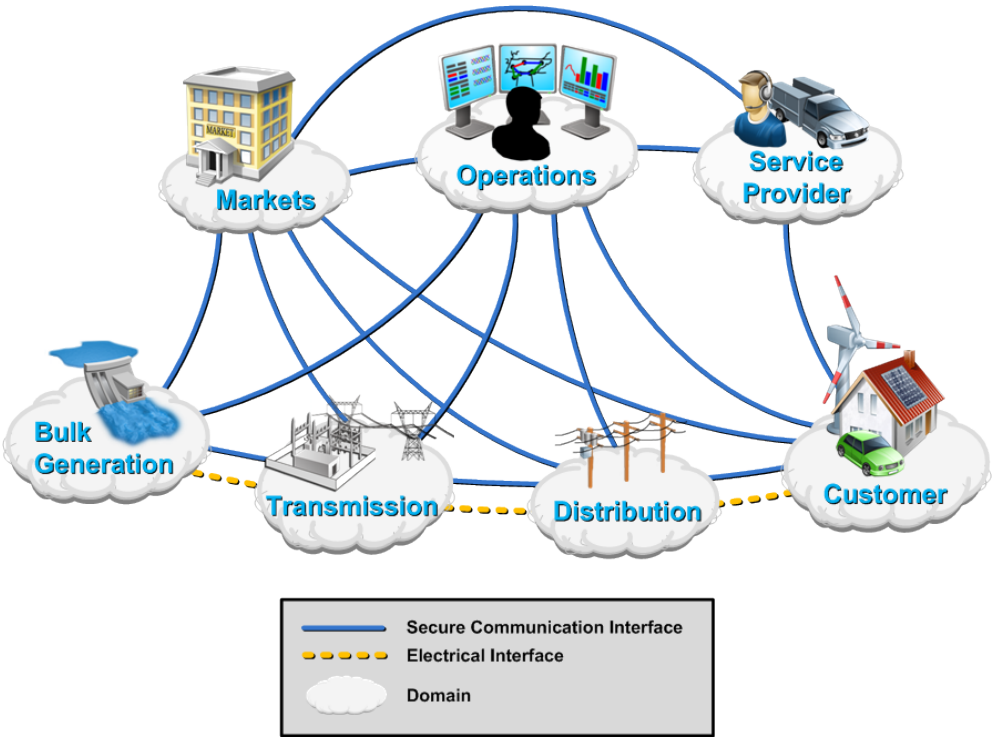
This framework is being used not only by NIST, but the rest of the US government, many utilities, most of the major standards bodies, and many other countries.

One of the components of the framework is the 7 domain model, which graphically lays out the overall picture of grid and its major components. The seven domains are:

- Generation – where the majority of electricity is created for consumption by customers.
- Transmission – where the majority of the high voltage long distance movement of electricity happens
- Distribution – a lower voltage portion of the grid which connects most of the customers to the transmission network and through that to generation.
- Customer – end users and their energy consuming and producing devices
- Markets – matching wholesale buyers and sellers of electricity to help balance the overall supply and demand.
- Operations – controlling the creation, flow and consumption of electricity to keep the system in balance.

- Service Providers – providing supporting services to the members of the other domains

The diagram is shown below:



This domain model has been used thousands of times to help explain what grid modernization is all about. Internationally it is probably the most recognized diagram ever created to illustrate what happens with electricity.

The SGIP continues to meet and work on interoperability and improve the framework. There are a number of international working groups that are working to harmonize how standards work, what the overall architecture should be, how testing and security should be structured. The overall document runs to more than 200 pages including a section on standards. The document fits well within the overall Intelligrid methodology and should be used as a supplement to the process of developing a roadmap. It provides an overview of many of the key standards that are useful when developing a roadmap or starting the process of implementation.

SGAC Framework Additions

As part of the work that the SGAC did a series of workshops were held to review all of the Intelligrid and other publically available use cases. This work was done to compile a complete list of available use cases as a first step in the process of cataloging all of the possible grid modernization requirements and actors. In this

first step over 700 existing use cases were reviewed, categorized by domain and level of completeness – based on the draft IEC standard for use cases. The SGAC team then reviewed each use case and pulled out a list of approximately 16,000 raw requirements from the use cases, as well as over 200 raw actors. In additional workshops, the requirements were grouped into higher level requirements and duplicates were eliminated from the list. This work reduced the list of high level requirements to approximately 500 and the actors to approximately 80. The requirements were again sorted by domain making it easy for someone focused on a pure distribution roadmap to review only the requirements that applied to distribution. Because the requirements can be traced back to the use cases they came from, this review can allow someone to segment the use cases they want to review, based on requirements they think they might need in the Intelligrid roadmapping process, say from a regulatory hearing or other required mandate. This can save significant time in deciding which use cases are good inputs to the Intelligrid process. Additionally the requirements list can serve as a double check coming out of the Intelligrid requirements process – allowing the team to have a standard reference list do review against what was developed in the workshop. Because all of the low level raw requirements are also traceable to the higher level requirements, it is possible to look at very low level engineering requirements that can be used as a starting point for the RFP process. At the end of this chapter, the places that this work can be used in Intelligid process are marked on the diagram with arrows to provide a visual cue on where to use the work.

Catalog of Standards

The Catalog of Standards was established by the SGIP Governing Board in May 2011, and the first six standards to be included in the catalog were approved by the SGIP Plenary in July 2011. As of May 2012, the number of standards or standards components added to the Catalog of Standards stands at 28. It is anticipated that the catalog will eventually contain hundreds of these consensus documents.

The Catalog of Standards provides a key—but not exclusive—source of input to the NIST process for coordinating the development of a framework of protocols and model standards for an interoperable Smart Grid. (See Section 4.5 of NIST Framework 2.0 for further details on the NIST Smart Grid standards identification process.) To better understand the relationship between SGIP's "Catalog of Standards" and NIST's "Identified Standards" list, please use this link.

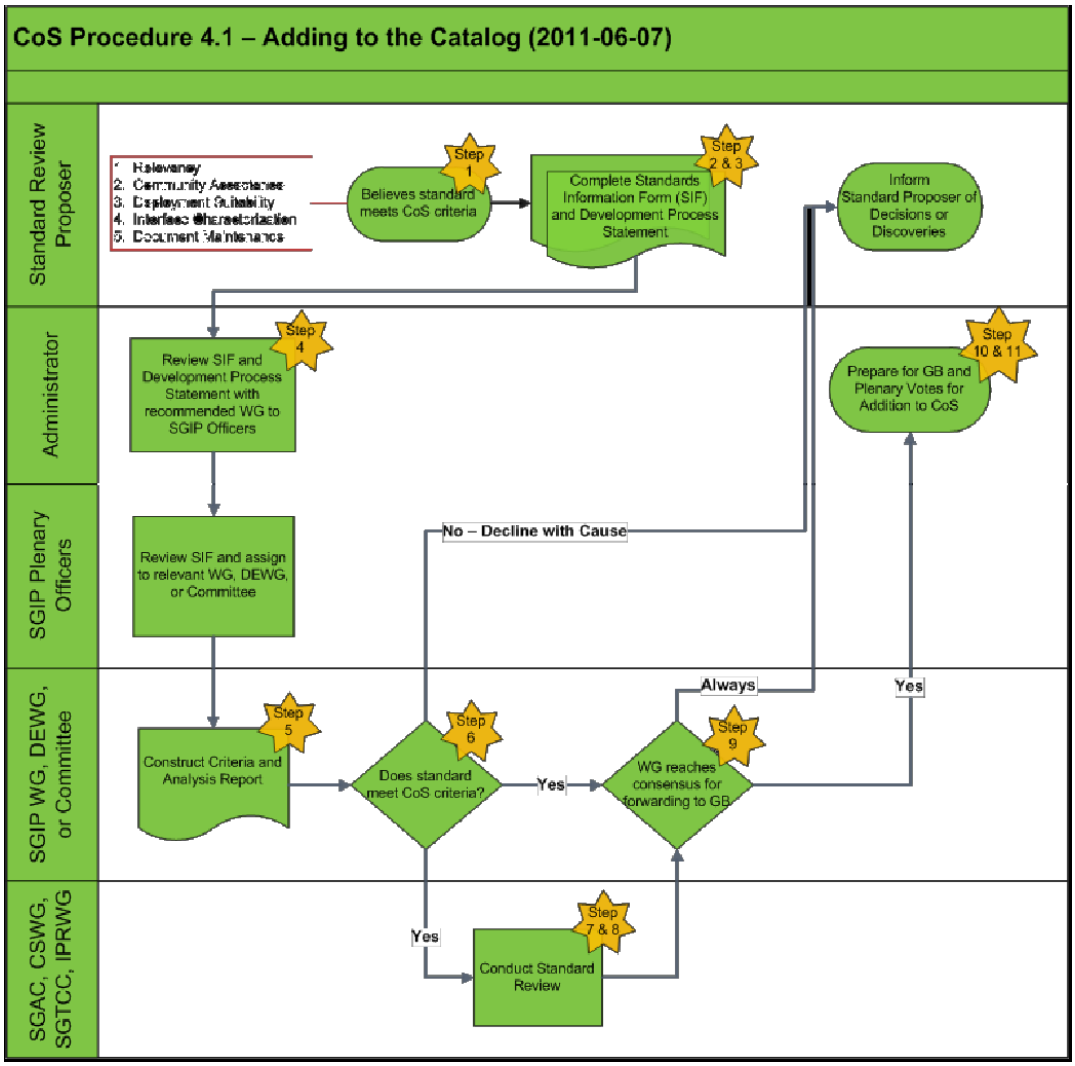
The process for adding standard to the Catalog of standards is shown below. While the framework document lists 97 that NIST recommends, few of those standards had been through the review process for the catalog of standards prior to publication of the framework document. The process to get a standard into the catalog can take several months it is one of the most rigorous processes to review an existing standard that exists today. The process includes a full review of the security implications of the standard, and a review of the architectural implications, primarily focused on interoperability, as well. Review documents

are completed and included in the catalog of standards showing the scope, expected use, status, open issues, and other aspects of the reviews. In most cases the standards are reviewed with the participation of one or more of the authors of the standard and the authors often take the recommendations back to the standards bodies for inclusion on future versions of the standard. In practice approximately 20 percent of the standards that have started the review process have been put on hold while the standards body makes changes recommended during the review process. Also during this process the Smart Grid Testing and Certification Committee (SGTCC) looks at the standard to see if testing exists and if there is a supporting user group or certification process for the standard. If there is they review the testing and certification supporting the standard and complete at testing and certification checklist, similar to the checklists completed by the architecture and security reviews.

At a deeper level the architecture committee's review checklist includes each of the levels in the GWAC stack and questions about those levels. The CSWG has a checklist that looks at each of the major elements in the NISTIR 7826 that was written by the CSWG to deal with grid security issues. So each review sheet provide a basis for a high level overview of what the standard covers. In addition the architecture committee review sheet has each of the 7 layers of the ISO stack included, so that someone working on an architecture project can understand which standards deal with the physical communication layer and which with the application layer. This allows a very rapid first pass review to determine if two standards compete or complement each other. The same is true with the GWAC stack, again allowing for a rapid review. Because the applicability to the 7 domains is also reviewed it is possible to quickly determine if the project someone is reviewing should take a deeper look at the standard or not. Technical and security issues are listed on the checklists, so that when reviewing the checklist, it is clear what gaps or issues might exist in the standard.

On their website NIST has posted the follow introduction to the catalog of standards:

"One of the most useful sources of information about Smart Grid standards is the Catalog of Standards, which is produced and maintained by the Smart Grid Interoperability Panel (SGIP). As described in the NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 2.0 (see Sections 4.2 and 5.3), the Catalog of Standards will serve as a compendium of standards, practices, and guidelines considered relevant for the development and deployment of a robust and interoperable Smart Grid. The extensive information included for each entry in the Catalog of Standards will be a very useful resource for utilities, manufacturers, regulators, consumers, and other Smart Grid stakeholders. The SGIP is assembling this set of reference documents as a resource for the Smart Grid community."



The diagram is full of acronyms that are unique to the SGIP (Smart Grid Interoperability Panel):

- SGAC – Smart Grid Architecture Committee
- CSWG – Cyber Security Working Group
- SGTCC – Smart Grid Testing and Certification Committee
- IPRWG - Intellectual Property Rights Working Group
- DEWG – Domain Expert Working Group
- CoS – Catalog of Standards
- GB – Governing Board

The process in each working group has its own process diagram, procedure and forms. In each working group from the time a standard enters the process to completion is no less than 90 days.

All of the major standards development organizations (SDOs) [e.g. IEEE, IEC, NAESB, etc.] are actively participating in this activity, providing access to authors and support as needed to complete the reviews of the standards.

The overall goal is to have a single location where professionals working in the industry can go to find standards that are relevant to their needs. The Catalog of Standards does not mean that the standard can be blindly applied to a project and it does not mean that the standard is without flaws, but it does mean that from an interoperability and an interoperability security point of view that the standards have received a review and issues that have been found have been discussed with the SDO that created the standard.

Again from the NIST Framework document NIST has the following comment about the Catalog of Standards:

"Note that the SGIP CoS is anticipated to provide a key, but not exclusive, source of input to the NIST process for coordinating the development of a framework of protocols and model standards for the Smart Grid under its Energy Independence and Security Act of 2007 (EISA) responsibilities.

The CoS is a compendium of standards and practices considered to be relevant for the development and deployment of a robust and interoperable Smart Grid. The CoS may contain multiple entries that may accomplish the same goals and are functionally equivalent; similarly, a single CoS entry may contain optional elements that need not be included in all implementations. In general, compliance with a standard does not guarantee interoperability due to the reasons given above. Though standards facilitate interoperability, they rarely, if ever, cover all levels of agreement and configuration required in practice. As a part of its work program, the SGIP is defining a testing and certification program that may be applied to the equipment, devices, and systems built to the standards listed in the CoS and that, if applied, will substantiate that implementations designed to the respective standards not only have compliance with the standards, but are also interoperable with one another. The CoS entry will indicate when test profiles have been defined and testing organizations identified for a particular standard; this will be indicated in the Catalog entry."

Where do they fit in the Intelligrid Methodology?

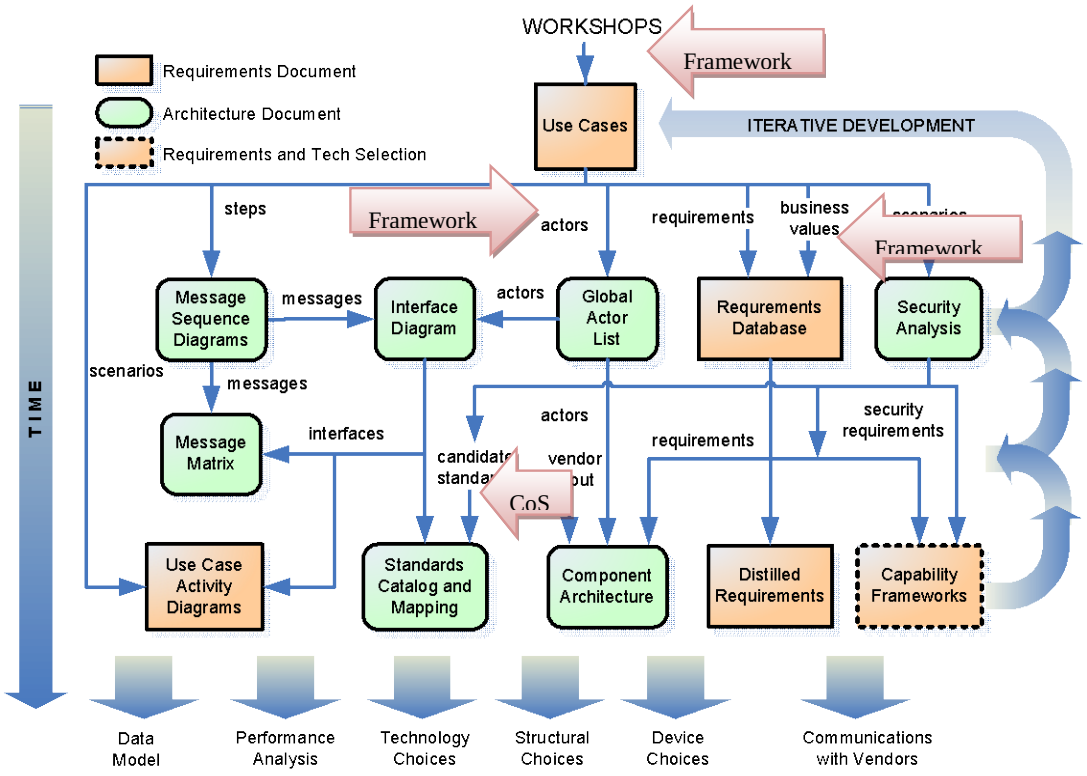
Going back to the Intelligrid diagram – it is possible to see where these two items fit. The Framework, and especially the work done by the SGAC fits into the diagram in three locations:

1. In selecting use cases for the workshops. The complete list of public use cases developed by the SGAC can be used either directly to find candidate use cases or the high level requirements list can be used to determine which use cases to look at to support specific business requirements.

2. The SGAC requirements list can be used as a double check on the requirements data base that comes from the use cases developed or modified in the workshops.
3. The SGAC actor list can be used as an input to the actor list or it can be used as a double check on the list of actors developed in the workshops from the use case work.

The Catalog of Standards (CoS) is useful in providing information on the standards to review and also providing a high level overview of what the standards might cover and any known gaps when the review was completed.

All four of these uses are marked on the diagram with the red arrows.



Appendix B: Communications Technology Assessment

This section is an updated version of the Communications Technology Assessment chapter or annex provided in most of the Smart Grid Roadmaps.

The Communications Technology Assessment provides an overview of technologies to be considered for use in utility communications infrastructure and in integrated vender and utility communications system architectures. It includes a discussion of important trends associated with the communication technologies.

Scope: What is a "Technology"?

The purpose of the assessment is to review, evaluate and recommend a set of communications "technologies", where the term "technology" refers generically to any of the following:

- Individual communications protocols
- Suites or profiles consisting of several protocols
- Media (i.e. physical links) used for communications
- Classes of networks, protocols, or devices
- Communications services
- Standards that enable communications, such as standard file formats

The reader should note the following additional restrictions on the scope of the technology assessment:

- The assessment evaluated communications infrastructure and architecture technology only. It does not evaluate other types of technologies that might be used for T&D automation such as Intelligent Electronic Devices (IEDs), application software or network components such firewalls and routers.
- The assessment does not recommend the final list of suitable technologies for an integrated grid communications and automation systems architecture, but provides a list from which specific choices may be made and a list of core technology proposals.

- In some cases particular technology choices will not be specified because one of the goals of the Reference Design is to be independent of the lowest layers of communications technologies.

Overall Integrated System Infrastructure

The role of technology is central in enabling utilities to address the four fundamental objectives of reliability, cost-effectiveness, customer service and regulatory compliance. To achieve these objectives, utilities should identify priority applications in terms of business objectives and determine a target implementation order as well as target schedule. The purpose of the technology assessment is to objectively evaluate the technology options available to support the priority applications.

Technologies must be ultimately selected as part of an informed decision making process that starts with determining the overall system architecture. Figure C-1 shows a sample reference system architecture.

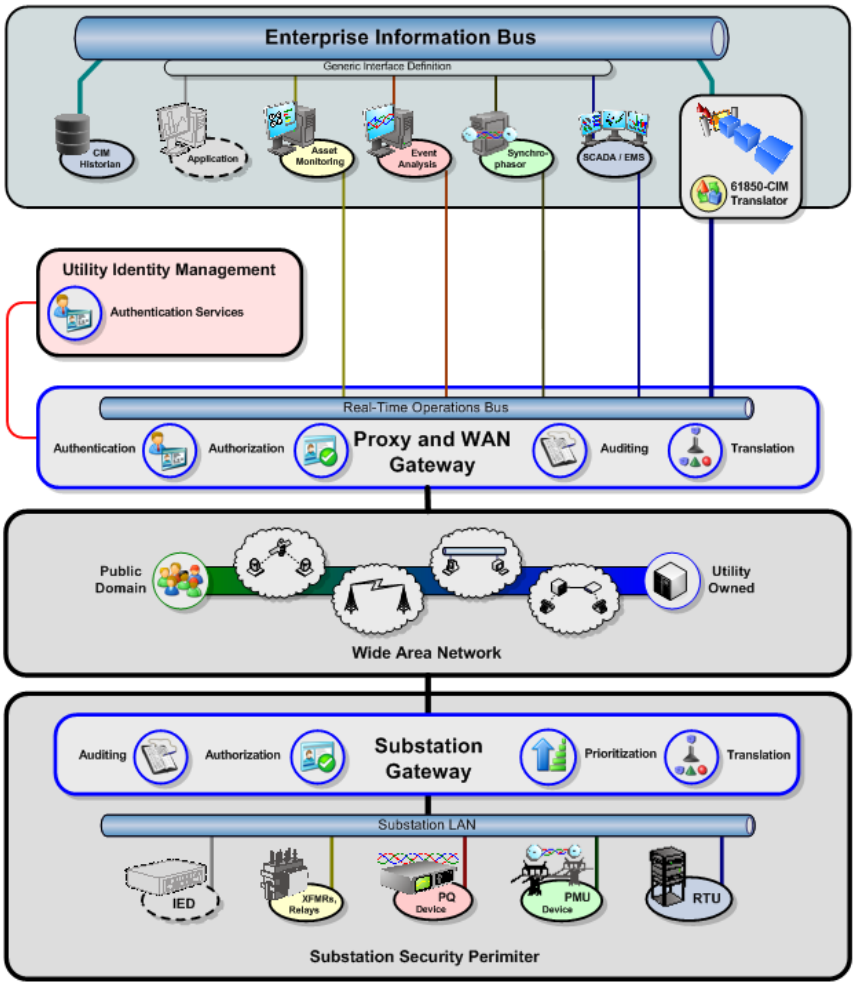


Figure B-1
Integrated Utility Systems Architecture

Organization and Approach

The Communications Technology Assessment is organized into the following three main areas:

- An overview of ***communications system architecture*** that summaries the major components that are needed to provide an integrated communications system.
- A list of technology ***evaluation criteria*** that to assist utilities as they continue to invest in the integrated systems including enterprise-level systems. The evaluation criteria are derived from the IntelliGrid principles and recommendations.
- The ***technology assessments*** themselves. Each technology is described and assessed with respect to the evaluation criteria. In addition, a section is dedicated within each assessment to five different areas:
  - Application to utility systems – how the technology would be used in utility system environment.
  - Strengths – what the technology does well.
  - Concerns – reasons why the technology may be less suitable.
  - References – a list of web sites where the specifications for the technology and more information can be found.
  - Layers – the OSI layer or layers that the technology implements.

The reference architecture includes new and improved functionality for AMI meters, renewable energy generation, electric vehicles, advanced distribution, remote device and data analytics. The reference architecture can provide a common, unified network for all remote devices. Traditionally, asset owners might be solely responsible for determining field devices and communication mechanisms used to acquire remote data on an application-by-application basis. As a result, communications infrastructure was unnecessarily bound to business function.

A primary benefit of the reference architecture is to rectify the unnecessary application-by-application communications solution and consolidate all system communications into a single integrated network. By standardizing on IP-based communications, utilities can leverage a wide range of industry-standard solutions, addressing everything from network management to endpoint security. A standardized IP-based communication system allows transport mechanisms to be selected according to data needs and environmental constraints and independently from each application.

Figure C-1 is a high level architecture diagram and assumes the following core functions:

- **Enterprise Integration/Information Bus**
  - Flexible message-based communications bus which simplifies integration of new applications and web services using a unified data and messaging model.
- **Operations Applications**
  - Energy Management Systems
  - Advanced Distribution Automation
  - Substation Automation
  - Geographic Information System (GIS)
  - Outage Management System (OMS)
  - Work Management Information System (WMIS)
  - Database
  - Data Historian such as OSIsoft PI
- **Smart Meter Systems**
  - Advanced Meter Infrastructure (AMI) Meter
  - Meter Data Management System (MDMS)
  - Automated Data Collection System (ACDS)
  - AMI Back Office System
  - Billing Usage System
- **Real Time Operation Bus**
  - Unified communications bus for data transfer between EMS/DMS/OMS applications and front-end data gathering equipment retrieving data for real time applications.
- **Utility Identity Management Server**
  - The credential management application to maintain access control (authentication) and authorization information. The Proxy and WAN gateways and Substation Gateways obtain updated information from the identify management server.
- **Proxy and WAN Gateway**
  - Designed to abstract the authentication, authorization and addressing for all remote devices and data access. It resides in the demilitarized zone between the substation and the enterprise, and integrates with the utility's identity management server, eliminating the need for community logins and published IP addresses for individual IEDs.
- **Cyber Security**
  - Utilities must deal with a wide range of applications, equipment and communications media, some or many of which are classed as cyber assets. Many of these assets will be monitoring or controlling critical assets so will be classed as cyber critical assets and subject to NERC CIP

requirements. It is critical to build security measures into the communications systems from the very beginning.
- NISTR 7628, Guidelines for Smart Grid Cyber Security, Volumes 1 – 3 are an excellent source of information on cyber security architecture and implementation strategies. Volume 1 is located at csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol1.pdf.
- In terms of security architecture the defense-in-depth strategy recommended by NISTR 7628 should be implemented. In order to mitigate risk, security should be applied in layers, with one or more security measures implemented at each layer. A defense-in-depth approach focuses on defending the information, assets, power systems, communications and IT infrastructures through layered defenses including firewalls, intrusion detection systems (IDS), antivirus software, and cryptography.

- **Wide Area Network (WAN)**
  - The WAN must be selected to meet the demanding requirements that the wide range of utility applications require. Figure 6-1 above assumes a hierarchical architecture which accommodates all data for transmission substations, distribution substations, feeder based devices, distributed generation/ Independent Power Producers (IPPs), commercial metering and consumer portal/metering.
  - Because of the large number of devices involved in utility networks, it is vital that standard technologies be used for managing the network. Example functions include collecting statistics, alarms and status information on the communications network itself.
  - A key principle of the IntelliGrid Architecture is the use of "meta-data" for formally describing and exchanging device configuration and data reporting. Utility projects will benefit from a metadata capability to manage the large numbers of devices involved.

- **Substation Gateway**
  - Functionality may be performed by multiple devices.
  - Designed to abstract the authentication, authorization and addressing for all remote devices and data access. The gateway resides at the substation and will integrate with a utility's identity management server, eliminating the need for community logins and published IP addresses for individual IEDs.
  - Supports all substation LAN media, protocols and data formats.
  - Supports all serial and LAN protocols for legacy devices to enable a migration strategy of hybrid mixtures of old and new devices.
  - Supports cyber security applications including auditing, credential storage, access control.
  - Capability for local intelligent applications such as equipment monitoring applications, volt/var control, auto-reconfiguration, auto-restoration.
  - Future support of super-calibrator (local state estimator) function.
  - Integrated local data logging with future support for local data historian.

- Integrated automation application programming.
- Supports local human machine interface.
- Supports legacy IED configuration templates.
- Supports IEC 61850 Substation Configuration Language (SCL) for substation and IED configuration.

- **Substation Local Area Network (LAN)**
  - Copper or fiber Ethernet
  - 10/100/1000 Mbps
  - Wireless LAN (secured) for select data types
- **Substation IEDs**
  - Support optimized integration of functions (e.g. protection with fault/event recording)
  - Supports all defined substation LAN media, protocols and data formats
  - Applicable secure device requirements
  - Support of remote configuration and firmware download.
  - Support of local on-line configuration.
  - Equipped with high resolution time synchronization.
  - Optional integrated phasor measurement.
  - Integrated automation programming.
- **Feeder IED and Other Devices**
  - IEDs installed on the feeder such as reclosers, RTUs and capacitor controllers that communicate via a local or regional substation in a hierarchical architecture.
- **Mobile Work Force**
  - Mobile access to historian data, and substation data for local and remote equipment.
  - Utilization of short range communication technologies such as Bluetooth or infrared to perform maintenance tasks on local devices for example retrieving log data and updating configuration or firmware on pole-mounted devices.
  - Mobile access to substation drawings.
  - Mobile access to GIS information and asset information.
  - Mobile access to up-to-date OMS information integrated with coordinated fault location applications.
- **Customer Facing Systems**
  - Electrical metering is the application that most people associate with a consumer application. In addition various aspects of building automation are also fundamental to the consumer concept, and are therefore discussed.
    - Customer Communications System
    - Customer Web Portal
    - Customer Service System (CSS) or Customer Information System (CIS)

- Demand Response Availability and Control System (DRAACS)
- Home Area Network (HAN)
- HAN Display
- Programmable Controllable Thermostat Unit (PCTU)

Architecturally Significant Requirements

The following are considered to be the core applications that exhibit the most architecturally significant requirements for communications systems. The requirements defined here are can be used as inputs to communications architecture definition and procurement tasks. For example, bandwidth requirements can be used to develop network communications systems as well as servers which receive and process communications messages. For procurement purposes, these requirements can be used as a starting point for utilities developing Request for Proposals (RFPs).

- **Fault/Event Capture and Reporting Application**
  - High bandwidth due to 2 minute requirement for fault event notifications
  - Modest point count – all substations
  - Enterprise data management implications
- **Phasor Measurement and Communications Application**
  - Modest bandwidth at station
  - Minimal point count – selected stations initially (potentially large point count in the future)
  - High bandwidth after concentration
  - Very low latency
  - High reliability if used for state estimator / control
  - High determinism (i.e. narrow range of allowable latency, bandwidth, and reliability)
  - Enterprise data management implications
- **Asset Management**
  - Low bandwidth
  - Reliability (up time) less of a concern if store and forward architecture used (recommended)
  - Two communication pieces – sensor to sensor gateway/IED – and sensor gateway/IED in substation back to enterprise
- **Advanced Distribution Automation**
  - Modest bandwidth
  - Low latency
  - High determinism (i.e. narrow range of allowable latency, bandwidth, and reliability)
  - Peer-to-peer
  - High security

- **AMI**
  - Modest bandwidth
  - Latency is an issue if same day/current usage data reporting is desired for customer display purposes
  - Two way communications path to/from the meter
  - High security
  - Water and electric meter reading
  - Real time data path to HAN display
  - Meter reading scheduling and on-demand meter reading
  - Meter reading for Critical Pricing events
  - Meter data can include peak demand, peak generation, power quality data, volt/VAr data and temperature
  - Tamper Detection
  - Remote disconnect/reconnect/service limiting
- **Renewable Energy Integration**
  - Modest bandwidth
  - Low latency
  - Two way communications to/from renewable generation systems

Service Groups

The technology assessments are organized in sections according to ***service groups***, as illustrated in Figure C-2. The concentric rings in the figure indicate more generic, shared or common technologies toward the center, and more specialized, project-specific or application-specific technologies toward the outside. When selecting technologies for a particular project, a system engineer should start at the center and work outwards. A figure at the beginning of each chapter illustrates the service group addressed by that chapter.

Figure B-2
Communication Service Groups

Service Groups and Protocols

The following is a list of the service groups and the associated protocols for core technologies within each group. For each service group, noteworthy communications technologies are briefly discussed. More detailed material on each service group can be found in the subsequent sections. It is important that all of these service groups be represented in any utility implementation.

- **Core Networking** – The Internet suite of protocols are strong contenders as the core protocols for basic communications in projects because of their low cost, widespread availability and interoperability with a variety of networks and devices including hardened substation compatible switches and other network devices that support current and future capabilities such as IEEE 1588.
- **Security** – A variety of technologies are commercially available for securing IP-based networks. Key decisions in the security area relate to methods of securing wireless networks, and the choice of Transport Layer Security (TLS) or IP Security (IPsec). These two technologies are roughly equal in the level of security they provide. The key factor appears to be ease of use, in which TLS is perceived to have the advantage.
- **Network Management** – Leaders in the network management area include Simple Network Management Protocol (SNMP) and Common Management Information Protocol (CMIP). Before a technology can be chosen, a major concern will be the definition of standard objects for managing all devices and networking hardware. Such definitions should be independent of the technology used.
- **Data Structuring and Presentation** – A number of commercial computing technologies are available that address data presentation, including Extensible Markup Language (XML), and HyperText Markup Language (HTML). The key issue here will be how to apply these technologies to the power industry, using specialized schemas similar to IEC 61850-6 Substation Configuration Language (SCL) and the new DNP XML Schema.
- **Wide Area Network (WAN) Technologies** –A fundamental principle continues to apply in that a successful reference design will allow devices to be implemented independently of WAN technologies. In the future some applications may benefit from wireless WAN technology options that hold increasing promise for back haul from aggregation sites. Existing WANs with Frame Relay and ATM switches will continue to be used, with new WAN hardware typically using gigabit Ethernet.
- **Local Area Network (LAN) Technologies** –A good reference design should be independent of LAN technology, but the leader is clearly copper and fiber Ethernet within larger field installations with potential for wireless within the substation for select applications such as equipment monitoring devices. LANs appear in several locations in the reference design: in the substation, at customer sites, in utility offices and for mobile work forces.

For communications to feeders Multiple Access (MAS) radio, fiber, WiFi (IEEE 802.11a,b,g, n) and WiMax (IEEE 802.16) are the candidate technologies. For AMI communications ZigBee, PLC, BPL, cellular, wireless including WiFi and WiMax are the candidate technologies for point to multi-point configurations. Meshed peer to peer networks also offer significant potential. For mobile workforce leased cellular, WiFi and WiMax are the leading technologies.

- **Power System Operations** – The best choice for power system communications will likely depend on which technology a particular utility has already installed. The leading substation and Telecontrol (SCADA) protocol suites are identified here, including DNP3, IEC 60870, IEC 61850, and the Common Information Model (CIM). The leading phasor measurement communications protocol is IEEE C37.118-2005. Event record formats should be in IEEE COMTRADE.

Service Groups versus OSI Layers

The seven-layer Open Systems Interconnect (OSI) model, illustrated in **Error! Reference source not found.**, is traditionally used to design communications technologies. Many of the candidate technologies cross multiple OSI layers. For instance, DNP3, IEC 61850, BACnet, and even some paging systems use portions of all seven OSI layers. Many of the problems the OSI network layers were designed to solve have been well-described and fairly well addressed over the years. As a result, most of the technologies evaluated have well-defined layered interfaces and therefore can co-exist within a device and on a network. (Whether they can work *together* properly is another issue to be addressed separately.)

The applications interoperability problems that are most likely to cause concern in utilities are best described as either being "above" the topmost OSI layer – in the realm of application object models and process orchestration or as using communications protocols for which no IP interface has yet been developed. In the technology assessment, communications technologies are assessed by the services they would provide.

The technology groupings are complimentary to the OSI model; with a given technology existing simultaneously in a particular set of layers and in a particular service group. In the technology assessment, the layers implemented by each technology are listed as part of the discussion for that technology.

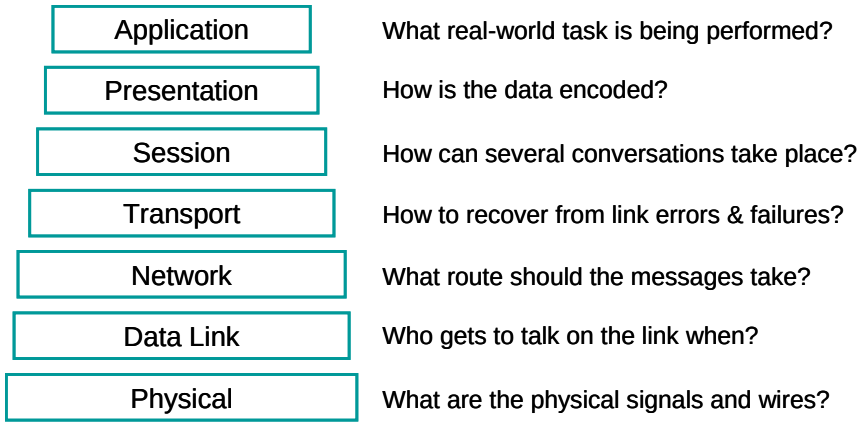


Figure B-3
Open Systems Interconnect (OSI) Reference Model

WANs, LANs and Other Networks

The communications requirements for different types of networks may vary widely. They are therefore discussed in separate chapters within the technology assessment.

There are a number of other methods and terms for classifying networks. For instance, some of the wireless standards distinguish between a WAN and a Metropolitan Area Networks (MAN) or between a LAN, a Home Area Network (HAN) and a Personal Area Network (PAN). Telecommunications standards typically distinguish between Transport (long-distance) and Access (to the home) networks.

The technology assessment does not make distinctions between all the many different types of network scope that have been proposed. It uses only the two classifications, WAN and LAN, to distinguish between communications networks used to reach a substation or site, and networks used *at* the site. A few technologies, notably Ethernet, WiFi and IEC 61334-4, can be used in *both* areas. In those cases, the technology has been placed in the most convenient category, with a note to explain it may belong in both.

Clients and Servers

It is worth noting that a number of the technologies discussed here use the concept of a **client** and a **server**. Readers unfamiliar with client server terminology need only to understand that a client makes a request to a server to provide some kind of **service**, e.g. make a connection, authenticate a user, set the time, or operate a switch. Servers service, that is provide the function requested in response to the requests made by clients.

Subscribers and Publishers

In the client server model, the publish/subscribe model permits an entity to request an update "when deemed appropriate" by the publisher. The publisher may or may not have knowledge of the specific subscribers. Typically subscribers request the publisher send an update either periodically or asynchronously when a value changes. Publish/subscribe models are sometimes implemented using broadcast or multicast protocols to allow mass transmission of information, e.g. publishing the present price of energy.

General Observations

- It is important that any reference design or implementation include technologies from *each* of the service groups. Individual projects may choose to emphasize one service group over another, but for a good design, all service groups are necessary.
- In each service group, there are typically two or three candidate technologies, each of which may be nearly equally suited for use compared to the other. For example, IPSec and TLS, SNTP and CMIP, or ANSI C12 and DLMS/COSEM. The success of a reference design may rely on how communication protocols can work together that is interoperate, rather than choosing one protocol over the other.
- There are liable to be overlaps even between technologies in different service groups. Therefore a reference design will need to clearly identify roles and options that will permit protocols to interoperate properly, and not just define a "shopping list" of technologies.
- It is vital that any reference design be completely independent of the local-area or wide-area networking technologies available.
- Many of the technologies support mechanisms that would allow their data to be "tunneled" or transported through an IP network. One possible strategy for harmonization of these various technologies would be for the LAN/WAN to simply act as a gateway for such tunnels, "wrapping and unwrapping" messages in IP "envelopes" from clients at the utility site to equipment on the customer premises and vice versa.

NIST Recommended Smart Grid Standards

Under the Energy Independence and Security Act (EISA) of 2007, the National Institute of Standards and Technology (NIST) has "primary responsibility to coordinate development of a framework that includes protocols and model standards for information management to achieve interoperability of smart grid devices and systems…" Thus NIST is tasked with the role of recommending Smart Grid standards to achieve interoperability.

In October 2010, NIST recommended 5 sets of standards as the initial set of Smart Grid standards. The protocols specified in the 5 NIST-recommended standards should be considered front runners when selecting protocols for interoperability. The initial 5 sets of standards are:

- Common Information Model (CIM) specified in IEC 61970 and 61968 for transmission and distribution systems data exchange between applications such as EMS, DMS, GIS and OMS
- IEC 61850 for substation automation and field device communications including protocols, information model, and data
- IEC 60870-6, the Inter-Control Center Communications Protocol, for data exchange over wide area networks (WANs) between utility control centers, utilities, power pools, regional control centers, and non-utility generators
- IEC 62351 for cyber security of the communication protocols listed above

NIST has defined a conceptual model with 7 domains as shown in **Error! Reference source not found.**. The NIST model describes a high level reference architecture including the communications networks. The NIST high level reference architecture is a good starting point for architecture development for future utility enterprise-level systems.

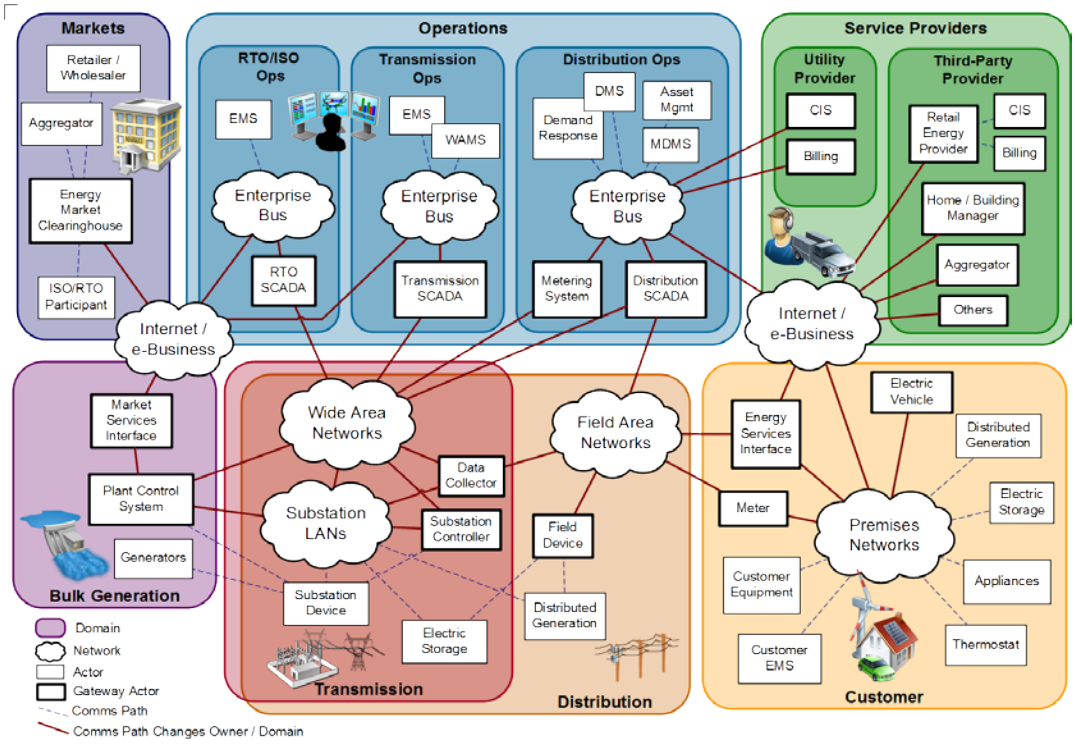


Figure B-4
NIST Domains and Reference Architecture

SGIP Recommended Standards

The Smart Grid Interoperability Panel (SGIP) maintains a data base of recommended standards called the Catalog of Standards (CoS). The Catalog is a compendium of standards and practices considered to be relevant for the

development and deployment of a robust and interoperable Smart Grid. The SGIP recommended standards in the CoS are good candidates to consider in terms of future interoperability between utility systems.

The current list of standards in the CoS is shown below:

Standard	Version	Title	Description
IEC 61850-10	ed1.0, 2005	Communication networks and systems in substations - Part 10: Conformance testing	Specifies standard techniques for testing of conformance of implementations, as well as specific measurement techniques to be applied when declaring performance parameters
IEC 61850-3	ed 1.0, 2002	Communication networks and systems in substations - Part 3: General requirements	Provides the general requirements for the entire 61850 set of standards for automating substations.
IEC 61850-4	ed 2.0, 2011	Communication networks and systems for power utility automation - Part 4: System and project management	Provides project management suggestions and requirements for the entire 61850 set of standards for automating substations.
IEC 61850-5	ed 1.0, 2003	Communication networks and systems in substations - Part 5: Communication requirements for functions and device models	Provides communications requirements for substation functions for the entire 61850 set of standards for automating substations.
IEC 61850-6	ed 2.0, 2009	Communication networks and systems for power utility automation - Part 6: Configuration description language for communication in electrical substations related to IEDs	Provides communications requirements for substation functions for the entire 61850 set of standards for automating substations.
IEC 61850-7-1	ed 2.0, 2011	Communication networks and systems for power utility automation - Part 7-1: Basic communication structure - Principles and models	Provides an overview of and an introduction to the abstract models and services in IEC 61850-7-4, IEC 61850-7-3, IEC 61850-7-2, IEC 61850-6, and IEC 61850-8-1

Standard	Version	Title	Description
IEC 61850-7-2	ed 2.0, 2010	Communication networks and systems for power utility automation - Part 7-2: Basic information and communication structure - Abstract communication service interface (ACSI)	Provides communications requirements for substation functions for the entire 61850 set of standards for automating substations.
IEC 61850-7-3	ed 2.0, 2010	Communication networks and systems for power utility automation - Part 7-3: Basic communication structure - Common data classes	Specifies the hierarchy of abstract classes. In particular, the names and structures for: Standard data types; Attribute types; CDCs for status information; CDCs for measured information, control, status settings, and analog settings
IEC 61850-7-410	ed 1.0, 2007	Communication networks and systems for power utility automation - Part 7-410: Hydroelectric power plants - Communication for monitoring and control	Specifies the additional common data classes, logical nodes and data objects required for the use of IEC 61850 in a hydropower plant. Includes electrical/mechanical/hydrological functions as well as sensors.
IEC 61850-7-420	ed 1.0, 2009	Communication networks and systems for power utility automation - Part 7-420: Basic communication structure - Distributed energy resources logical nodes	Defines the information models to be used in the exchange of information with distributed energy resources (DER), which comprise dispersed generation devices and dispersed storage devices
IEC 61850-7-4	ed 2.0, 2010	Communication networks and systems for power utility automation - Part 7-4: Basic communication structure - Compatible logical node classes and data object classes	Specifies abstract information model of devices and functions, consisting of data objects contained in Logical Nodes (LNs).
IEC 61850-8-1	ed 2.0, 2011	Communication networks and systems for power utility automation - Part 8-1: Specific communication service mapping (SCSM) - Mappings to MMS (ISO 9506-1 and ISO 9506-2) and to ISO/IEC 8802-3	Provides inter-device operation of a variety of substation and other field devices to create and exchange concrete) communication messages by mapping the abstract services and the abstract logical nodes and common data models to the Manufacturing Messaging Specification (MMS) over Ethernet.

Standard	Version	Title	Description
IEC 61850-9-2	ed 1.0, 2004	Communication networks and systems in substations - Part 9-2: Specific Communication Service Mapping (SCSM) - Sampled values over ISO/IEC 8802-3	Provides a comprehensive overview of the different aspects to consider while using IEC 61850 for information exchange between substations and control centers or other system level applications
IEC/TR 61850-1	ed1.0 (2003-04)	Communication networks and systems in substations - Part 1: Introduction and overview	The IEC 61850 series of standards define object models, abstract services, and mappings to communications protocols for field devices and systems. The scope of IEC 61850 includes information exchanges within substations, for protective relaying, between substations, between substations and control centers, within hydro power plants, for distribution automation, for managing distributed energy resources (generation and storage), and for managing charging of electric vehicles. Part 1 is an introduction to the substations domain since it was the first domain to be developed.
IEEE 1815-2010	July 2010	Standard for Electric Power Systems Communications - Distributed Network Protocol (DNP3)	Specifies the DNP3 protocol structure, functions, and application alternatives for power system communications. In addition to defining the structure and operation of DNP3, the standard defines three application levels that are interoperable.
IEEE C37.238-2011	2011	IEEE Standard Profile for Use of IEEE 1588 Precision Time Protocol in Power System Applications	Specifies a common profile for use of IEEE 1588-2008 Precision Time Protocol (PTP) in power system protection, control, automation and data communication applications utilizing an Ethernet communications architecture.

Standard	Version	Title	Description
IEEE C37.239-2010	2010	Standard for Common Format for Event Data Exchange (COMFEDE) for Power Systems	A common format for data files used for the interchange of various types of event data collected from electrical power systems or power system models is defined. It doesn't define what is transferred via communications. It is only a file format for offline analysis and data exchange. COMFEDE represents a subset of what is in IEC 61850.
IETF RFC6272	Informational only 2011	Internet Protocols for the Smart Grid	Identifies the key infrastructure protocols of the Internet Protocol Suite for use in the Smart Grid. The target audience is those people seeking guidance on how to construct an appropriate Internet Protocol Suite profile for the Smart Grid. In practice, such a profile would consist of selecting what is needed for Smart Grid deployment from the picture presented here
NAESB REQ 18/WEQ 19	REQ18,WEQ19	PAP10 Energy Usage Information	Defines an information model of semantics for the definition and exchange of customer energy usage information. The actual exchange standards are anticipated to be derivative from this seed standard.
NEMA SG-AMI 1	1-2009	Requirements for Smart Meter Upgradeability	NEMA Smart Grid Standards Publication SG-AMI 1 defines requirements that include secure local and remote upgrades of Smart Meter: Metrology; AMI applications; AMI communications; HAN applications; and HAN communications.
NISTIR 7761	Updated 2011	Guidelines for Assessing Wireless Standards for Smart Grid Applications	Key tools and methods to assist Smart grid system designers in making informed decisions about existing and emerging wireless technologies. An initial set of quantified requirements have been brought together for advanced metering infrastructure (AMI) and initial Distribution Automation (DA) communications.

Standard	Version	Title	Description
OASIS EMIX	1.0	Energy Market Information eXchange	OASIS EMIX defines an information model and XML vocabulary for the interoperable and standard exchange of prices and product definitions in transaction-based energy markets. Information covered includes price, bid, times for use or availability, units and quantity to be traded.
OASIS Energy Interop	1.0	Energy Interop	OASIS Energy interoperation describes an information and communication model to enable collaborative and transaction-based use of energy for the interoperable exchange of: dynamic price signals; reliability signals; emergency signals; communication of market participation information (bids); load predictability and generation information exchange of signals for dynamic pricing, reliability, and emergencies; and generation information
OASIS WS-Calendar	v1.0 in process	Web Services Calendar	The anticipated use of WS-Calendar as a component within other specifications provides a common model for scheduling diverse interactions in different domains.
SAE J1772	Revised 2010	Electrical Connector between PEV and EVSE	SAE Recommended Practice J1772 covers the general physical, electrical, functional and performance requirements to facilitate conductive charging of EV/PHEV vehicles in North America.
SAE J2836/1-3	2010-04-08	Use Cases for PEV Interactions (in development) [Part 1, Part 2, Part 3]	SAE Information Report J2836 establishes use cases for communication between plug-in electric vehicles and the electric power grid, for energy transfer and other applications.

Standard	Version	Title	Description
SAE J2847/1-3		Communications for PEV Interactions (in development) [Part 1, Part 2, Part 3]	SAE Recommended Practice J2847 establishes requirements and specifications for communication between plug-in electric vehicles and the electric power grid, for energy transfer and other applications. Where relevant, this document notes, but does formally specify, interactions between the vehicle and vehicle operator.
SGIP 2011-0008_1	1.0	PAP 18: SEP 1.x to SEP 2.0 Transition and Coexistence White Paper	SEP 1.x to SEP 2.0 Transition and Coexistence was created to specifically address SEP 1.x to SEP 2.0 migration and coexistence.

Technology Ratings

Ratings are given to each of the technologies analyzed using the defined evaluation criteria. After reading the evaluations in the rest of the documents, and assuming the criteria have been fairly quantitatively defined, the reasons any particular rating was given will hopefully be obvious. However, it is reasonable to expect that any two people's opinions may differ by about 1 point for any given criterion and technology.

Purpose of the Ratings

The purpose of the ratings is not to suggest that any particular technology is "the best", even within its service group. The Reference Design may identify other key criteria for evaluation. Furthermore, any particular project may have its own priorities. The ratings assume an equal weight for all criteria, but a particular project may choose to perform a weighted average. It has been noted, for instance, that perhaps the "applicability to…" criteria may have been given excessive weight, and advocate a "not invented here" philosophy. The purpose of providing the ratings is to give an overview of the capabilities of the technologies and to show how the evaluation criteria could be used in the future.

Visible Trends

Technologies selected for evaluation were pre-selected based on the result from previous technology assessments. The intent of the assessment is to provide a "short list", not a comprehensive discussion of all technologies. For instance, the ISO suite of protocols is not included in the ranking table. Not too surprisingly, most of the technologies listed here were rated fairly high; averaging about 35 out of a possible 55 points For a more comprehensive (but less detailed) list of technologies, please refer to the IntelliGrid Architecture documentation.

It is interesting that the highest rated technology received only a 43, less than 80% of the maximum. One reason for the lack of high scores is, of course, that no technology is "perfect". Another reason is that any given technology tends to specialize in a particular area, and so none of them are will be a "jack of all trades".

Criteria Not Included

Lastly, it should be noted that one criterion that is missing is how well the protocol does its job. For instance, CMIP is generally acknowledged to be a better network management protocol than SNMP – it was designed to be such. However performance is not shown in the table because it is extremely difficult to find a non-subjective metric for such a quality. For that kind of information, the reader should look at the Strengths and Concerns sections for each technology. The Level of Adoption, Applicability to the Power Industry, and Applicability to the utility metrics may also provide relevant information in regards to performance.

Commentary on Highs and Lows

Some readers may find it surprising that their favorite technology does not rate highly. One noticeably low rating is Access BPL. For example, X10 has problems both with licensing and with its limited technical capabilities. These factors do not; however, seem to affect its popularity.

SSH is a similarly promising technology that has had problems with licensing, affecting its rating.

The leaders, for their part, tend to be well-established, popular standards that are also used in other industries. One exception is DLMS/COSEM which edges out ANSI C12, largely because of the latter's lack of security and users' group support. This area sorely needs some harmonization efforts to prevent two different standards being used in different areas of the world. WiMAX gets a fairly high rating despite not being very mature. It will be very interesting to watch what happens if it becomes as more widely implemented.

Application of Weightings

It is possible to apply weightings for each category of the assessment to develop an overall comparison of the available technologies in one of the service groups. A row for weightings is included in the spreadsheet for each service group. For purposes of the overview analysis, the different categories are given equal weightings. The original spreadsheet is available for modification or evaluation with different weightings. Utilities may also be interested in refining one of the categories, such as "Adoption" to represent the level of adoption at their utility rather than adoption in the industry as a whole.

Table B-1
Technology Ratings

	Standardization	Openness	Adoption	User's Group	Security	Manageability	Scaleability	Object Modeling	Self-Description	Power Industry	Utility Applicability	TOTAL	**Percentage**	Bar Graph
Core Networking														
IPv4	5	5	5	4	2	4	5	1	2	3	3	39	**71%**	
IPv6	5	5	2	4	4	4	5	1	5	3	3	41	**75%**	
TCP	5	5	5	4	2	4	5	1	2	3	3	39	**71%**	
UDP	5	5	5	4	1	4	5	1	1	3	3	37	**67%**	
HTTP	5	5	5	5	2	3	5	2	4	3	3	42	**76%**	
Security														
TLS	5	5	5	4	5	3	4	1	3	3	2	40	**73%**	
IPSec	5	5	5	5	5	3	5	1	3	3	3	43	**78%**	
HTTPS	5	5	5	5	4	2	4	1	4	3	3	41	**75%**	
SSH	3	4	4	3	5	2	2	1	2	2	2	30	**55%**	
X.509	5	4	4	1	5	5	3	1	4	3	2	37	**67%**	
IEEE 802.11i	5	3	2	5	5	4	2	1	2	2	3	34	**62%**	
Management														
Basic IP	5	5	5	4	1	5	4	1	3	3	3	39	**71%**	
SNMP	5	5	5	4	2	5	3	4	2	2	2	39	**71%**	
CMIP	5	3	2	1	3	5	3	4	2	1	1	30	**55%**	
NTP/SNTP	3	5	5	4	1	5	4	1	2	3	3	36	**65%**	
IEEE 1588 (PTP)	5	3	3	4	1	5	3	1	2	4	4	35	**64%**	
Presentation														
HTML	5	5	5	4	2	5	5	4	4	3	3	45	**82%**	
XML	5	5	5	4	2	5	5	5	4	3	3	46	**84%**	
BNF	2	5	3	1	1	1	5	5	3	3	3	32	**58%**	
ASN.1	5	5	5	1	1	1	5	5	3	3	2	36	**65%**	
IEC 61850-6 (SCL)	5	5	2	5	2	5	2	4	4	4	2	40	**73%**	
SOAP and Web Service	3	5	4	4	2	5	3	4	5	3	2	40	**73%**	
ebXML	5	5	3	4	2	5	3	4	5	2	3	41	**75%**	
LANs														
Ethernet	5	5	5	2	3	4	5	2	5	3	3	42	**76%**	
Wi-Fi	5	4	5	5	3	4	4	1	5	2	3	41	**75%**	
ZigBee	5	4	3	5	4	4	3	1	5	4	4	42	**76%**	
Bluetooth	5	4	4	5	2	4	3	1	5	1	1	35	**64%**	
HomePlug	3	3	2	5	3	3	3	1	5	2	3	33	**60%**	
X10	1	4	5	2	1	1	1	1	5	4	4	29	**53%**	
WANs														
SONET/SDH	4	4	4	5	5	4	5	3	3	5	3	45	**82%**	
MPLS	5	5	5	5	4	5	5	3	3	3	2	45	**82%**	
Frame Relay	5	5	5	5	4	5	4	3	3	2	2	43	**78%**	
DSL	5	4	5	5	4	4	4	3	3	2	2	41	**75%**	
Cable	5	5	5	5	4	4	4	3	3	2	2	42	**76%**	
WiMAX	5	4	2	5	4	3	3	3	5	1	1	36	**65%**	
Access BPL	1	2	2	2	3	2	4	1	2	4	4	27	**49%**	
IEC 61334-5 PLC	5	3	4	1	1	2	3	1	1	5	4	30	**55%**	
Paging	3	2	5	1	1	2	4	1	5	3	3	30	**55%**	
Satellite	2	3	2	1	4	4	3	1	1	3	3	27	**49%**	
Cellular	5	3	5	2	3	4	4	3	5	3	3	40	**73%**	
FTTH	5	3	2	2	4	4	4	3	3	1	1	32	**58%**	
Power System Operations														
DNP3	5	4	5	5	2	1	3	2	3	4	3	37	**67%**	
IEC 60870-5-104	5	4	5	3	2	1	3	2	3	5	3	36	**65%**	
IEC 61850	5	3	2	5	3	1	3	4	5	5	3	39	**71%**	
IEC 61968/61970	5	3	2	4	2	1	2	5	5	5	3	37	**67%**	
IEC 60870-6 TASE.2	5	4	5	4	2	1	2	2	2	5	3	35	**64%**	
IEEE C37.118	5	3	4	3	2	3	5	3	3	5	4	40	**73%**	
IEEE COMTRADE	4	4	5	2	2	2	3	2	2	5	1	32	**58%**	
Consumer Application														
ANSI/IEEE C12	5	4	3	2	2	1	4	4	3	5	5	38	**69%**	
DLMS/COSEM	5	4	3	5	3	1	4	4	3	5	5	42	**76%**	
BACnet	4	4	4	5	2	1	2	2	2	4	4	34	**62%**	
EIA 709 (LONWorks)	4	2	3	5	2	2	3	2	3	3	3	32	**58%**	
KNX (EN 50090)	4	4	3	5	1	4	2	3	5	3	3	37	**67%**	
OpenADR	3	5	1	3	3	1	2	3	3	3	1	28	**51%**	

Technologies have been pre-selected according to the IntelliGrid Architecture

Evaluation Criteria

The evaluation criteria used in to assess the technologies for utility implementations were based on criteria recommended by IntelliGrid methodology. The criteria are based on the Integrated Energy and Communications Systems Architecture, Volume I: User Guidelines and Recommendations, in particular those directed at Chief Information Architects and Energy System Engineers.

The evaluation criteria are interrelated and desirable characteristics from one aspect of the assessment may conflict with other assessment criteria. For instance, open standards are preferred, but a solution that is partly proprietary and solves a problem of scalability or security may end up being the best choice if it provides well-defined and published interfaces that can be integrated with other systems.

Each of the following sections explains the need for a particular criterion and describes how the criteria were evaluated in qualitative terms. A table lists and explains how the technologies were evaluated for each criterion. Although each criterion is arguably a multi-dimensional measurement, it was necessary for simplicity's sake to normalize ratings to a number from one to five.

Level of Standardization

Technologies used for utility implementations should be both open and standardized. Standardization refers to how well-defined the technology is, and how well it is recognized by its potential user community as a viable alternative. Table C-2 lists commonly accepted levels of standardization, in order of their preference for se by IntelliGrid. Some technologies may be recognized by multiple standards levels at once.

Table B-2
Levels of Standardization

Level	Defined by	Recognized	Example
International Standard	International standards body	Worldwide	ISO, IEC, IEEE
National Standard	National standards body	Within one country or group of countries	ANSI, CEN, CSA
Consortia / Industry Standard	Group of vendors and/or users representing an industry or market segment	Members of the consortium	ASHRAE, IETF, EIA, DNP
Proprietary / de Facto Standard	Single vendor or user	Market dominance	Microsoft

Standardization is vital to prevent utility implementations from becoming victim to the "pilot syndrome", in which a number of vendors manage to make their equipment work together for a particular project, but cannot communicate with other devices in the industry. It also ensures that the technology is well-defined and has been reviewed by industry experts.

Table B-3
Normalized Rating of Level of Standardization

Rating	Title	Description
1	Proprietary	Not a standard
2	de Facto	Not a standard, but published and widely used
3	Consortia	Standardized by a group of vendors or an industry
4	National	Standardized by a national or regional organization
5	International	Standardized by an international organization

Level of Openness

The term *openness* indicates a measure of how easy it is to obtain and use the technology. It may be well-defined (high level of standardization) and widely used (high level of adoption), but still not be open, if it can only be used through a license agreement with a particular vendor.

Openness is important for utility systems because it will reduce barriers for new vendors to enter the market, and therefore will help to create economies of scale. A checklist for the level of openness of a technology is shown in Table C-4. The more boxes that can be checked for a given technology, the more open it can be considered. Less likely combinations are shaded. The normalized rating described in

Table C-5 is a simplification of the openness checklist.

Table B-4
Technology Openness Qualitative Checklist

Indicator	Should ideally be...					
	Published	Low Cost	Non-Profit	Multi-Vendor	On-Line	Reviewed by Users
Specification						
Source code						
Tools						
Hardware						
Right to Use						
Support						

Table B-5
Normalized Rating of Openness

Rating	Title	Description
1	Licensed Only	The technology can only be obtained using a license from a single source
2	Locked-In	The technology may be obtained from multiple vendors, but using it requires the user to "lock in" with a particular vendor and be unable to change vendors without significant cost.
3	More Than One	The technology is available from more than one vendor.
4	Many Vendors	The technology is available from many vendors
5	Open Source	The technology is available as open source software

Level of Adoption

Regardless of how well-defined, recognized or open a standard is, the primary measure of its success is how widely it is used. The Internet standards, for instance, are not International Standards recognized by ISO or the IEC; however, they are some of the most widely used communications protocols in the world. It is important that technology chosen for use be widely used, because a large user base ensures:

- **Usefulness.** Problems with the technology will be more quickly identified and corrected.
- **Stability.** It will be more likely to evolve rather than become obsolete (e.g. Ethernet)
- **Longevity.** More people will have a stake in its continued use.

These factors will make it less likely that a wholesale upgrade of equipment will be necessary in the future. Table C-6 provides a normalized rating from one-five (1-5) of adoption.

Table B-6
Normalized Rating of Adoption

Rating	Title	Description
1	Not Released	Products are not yet available.
2	Early Adopters	A few products are available to early adopters but the technology is not yet well known.
3	Well-Known	Most users know of the technology but many have not decided to acquire it yet.
4	Common	Most users in the target group are using the technology
5	Pervasive	The technology is considered part of the minimum feature set for the type of products that might use it.

Level of Users' Group Support

A contributing factor to the acceptance of any technology is whether a users' group exists to help maintain it. Some standards end up being abandoned after they have been published because the standards organizations that created them are not designed to help them thrive. A users' group usually provides one or more of the following services that help the promotion and continuation of the technology:

- Web Site
- Up-to-Date List of Members/Vendors/Users
- Frequently-Asked-Questions (FAQ) List
- Access to the Specifications
- Discussion Forum
- Mailing List
- Trade Show Booths
- Vendor Advertisements
- Help Line
- Newsletter
- Conformance Test Procedures
- Conformance Test Labs or Lab Certification Program
- Quality Program
- Interoperability Test Procedures
- Interoperability Test Labs or Lab Certification Program

All of these measures help prevent the technology from becoming obsolete and reduce the cost of implementation. Technologies with existing users' groups are therefore preferred for utility implementations. Table C-7 provides a normalized rating for user group support.

Table B-7
Normalized Rating of Users' Group Support

Rating	Title	Description
1	None	There is no Users' Group which supports the technology.
2	Marketing Only	A Users' Group exists but it mostly markets the technology
3	Technical Forum	The Users' Group provides a mailing list or forum for discussing technical issues, which may not have any impact on the standard.
4	Updates Standard	Concerns raised within the Users' Group can cause the standard specification for the technology to be modified.
5	Provides Testing	The Users' Group provides a certification testing process, procedures, and/or facility.

Security

Security is vital to utility implementations for NERC compliance and to address the following partial list of possible threats:

- An inside or outside attacker gaining unauthorized control of a piece of substation equipment.
- An inside or outside attacker cutting off access to equipment data.
- An inside or outside attacker compromising the integrity of equipment data.
- An inside or outside attacker gaining unauthorized access to equipment data.
- An inside or outside attacker using a utility LAN/WAN as a staging area for an attack on a connected network.

An essential action required by utilities is to review the comprehensive security policy covering all key elements of their communications system as well as the operating practices of all internal groups that interact with the communications system. Key requirements that will be a part of the security policy include logging, audits and risk analysis that are not specifically technology solutions. As far as technology areas are concerned the following are some of the key methods used to address security threats:

- Access Control and Authentication
- Authorization
- Port and Protocol Selection and Management
- IP Address Management
- Software and Data Integrity
- Proxy Servers

- Virtual LANs for Isolation
- Encryption

All technologies used in utilities should therefore be easy to integrate with common security technologies.

As noted in the report *A Strawman Reference Design for Demand Response Information Exchange*, security is part of a larger aspect of systems known as **trust**. The measure of trust in a system includes, in addition to the quality of its security, its level of integrity (reliability) and its performance. Trust factors are not discussed in the assessment primarily because of the lack of good measurements that are specific to any particular technology.

The security industry is unique in that it is constantly "fighting a war" in which "locks" are continually being upgraded to protect against new types of "lock picks". In addition to the other criteria discussed in the security assessment, security technologies should also be:

- Easy to upgrade with new algorithms, key sizes, and credentials
- Well-reviewed, accepted, and monitored by cryptographic experts
- Able to negotiate alternate parameters and choices
- Configurable to match users' security policies

As with the other criteria, these are complex, the qualitative security requirements are simplified into a normalized rating as shown in **Error! Reference source not found.**.

Table B-8
Normalized Rating of Security

Rating	Title	Description
1	Difficult to Secure	The technology has characteristics that make it difficult to secure
2	Can be Secured	If the technology is partnered with another technology, it can be secured, e.g. TCP can be secured using TLS.
3	Secure If Used Correctly	The technology has security features than may have flaws, but if used correctly, can create a secure system.
4	Secure As-Is	The technology has built-in features that make it secure
5	Used as Reference	The technology is a dedicated security technology and is used for securing other technologies.

Manageability

To be cost-effective, an off-site network must be remotely managed. Remotely "managed" means being able to perform the following operations from a central site:

- Enable or disable the device
- Enable or disable particular communications links
- Enable or disable spontaneous alarm reporting
- Change communications configuration parameters, such as addresses, routing choices, buffer sizes, window sizes, transmission rates, and security credentials
- Gather operational statistics
- Upload or download software or firmware
- Synchronize the time at the device

These are management functions only; there may be many other similar functions a system must support in order to perform its duties. A key factor here is the **upgradeability** of each component. In the utility environment, performing any of the functions listed above manually will be prohibitive. It must be possible to upgrade components remotely because of:

- The sheer number of devices that may need to be accessed
- The distance they will be located from the utility operations center
- Changing technology that would otherwise cause "stranded assets".

All technologies used in utility implementations should therefore be easy to co-exist with, and integrate with, common network management techniques. A proposed rating for manageability is provided in Table C-9.

Table B-9
Normalized Rating of Manageability

Rating	Title	Description
1	No Management	The technology is not remotely manageable
2	Proprietary Means	The technology can be managed via means unique to a vendor or project
3	Objects Exist	Standardized objects exist for managing the technology, but may not be commonly used.
4	Commonly Managed	The technology is often managed in real networks.
5	Management Technology	The technology is used for managing other technologies.

Scalability

Utility implementations today may support connections only to a limited number of systems but could eventually support connections to literally thousands of components such as solar installations. Therefore, any technology chosen must be scalable and cost-effective for a large number of devices. Scalability is a particular concern in the case of the wide-area network technologies discussed below. The number of addresses required to specify individual devices can be a challenge for some technologies. Another important factor is the scalability of network management and security. Software, firmware, passwords and other security credentials may need to be downloaded to millions of devices. Technologies that support mass management should be encouraged. See Table C-10 below for an approach for rating scalability.

Table B-10
Normalized Rating of Scalability

Rating	Title	Description
1	Tens	Technology can be applied to tens of devices.
2	Hundreds	Technology can be applied to hundreds of devices.
3	Thousands	Technology can be applied to thousands of devices.
4	Millions	Technology can be applied to millions of devices.
5	Billions	Technology can be applied to billions of devices.

Use of Object Modeling

It is a key principle of the IntelliGrid Architecture that all utility application-layer technologies should be object-oriented or object-based. In other words, all the data transferred in utility networks should be:

- Organized into standard logical groupings, usually called objects. Objects are abstract representations of real-world functions and processes of the power system.
- Accessed using a standard (ideally human-readable) naming convention
- Arranged in a hierarchy that permits clients to perform operations on subsets of the data
- Associated as a group with standard functions or services (often called methods)
- Expandable to include vendor-specific or proprietary data
- Reducible to a standard minimum subset

Object modeling makes it possible to configure and manage the enormous amount of data provided by a network of components. A proposed rating for level of support for object models is provided in Table C-11.

Table B-11
Normalized Rating of Object Modeling

Rating	Title	Description
1	None	The technology does not have the concept of objects.
2	Simple	The technology has the concept of objects that can be operated on, but they are simple and not deeply structured.
3	Structured	The technology has the concept of structured data with several levels of nesting, and structured object names
4	Addressable	The technology permits access to "leaf" portions of the structured data.
5	Standard Methodology	The technology uses a standard object methodology, such as UML.

Use of Self-Description and Meta-data

Another two related IntelliGrid Architecture principles that should be applied to enterprise-wide implementations are the use of self-description and meta-data. Self-description is the ability for a server device, such as an IED, to describe itself to a client, such as a master station or data concentrator. The server informs the client what data it has available, what format the data is in, and how to access the data. Self-description is fairly common in commercial computing applications, and makes possible what is generically known as "plug and play". In the utility industry, data object information has typically been manually specified.

Self-description reduces the cost of deploying enterprise systems by:

- Reducing labor costs during installation and configuration by automating a human process.
- Reducing errors in configuration due to memory errors or mistyping.
- Reducing the amount of testing that must be performed on communications paths to correct human errors.

Self-description may be performed either online or offline. When it is done online, the information is transferred within the protocol stream, usually at initialization time. When it is performed offline, the vendor or user of the server device provides a file in a standard format that describes the device's data. Offline self-description tends to be preferred because of the delay that online self-description may cause at start-up.

"Meta-data" is a term literally meaning "information about data". Meta-data includes self-description as well as other ways to organize information so it is easily identifiable and human readable, such as document markup languages (e.g. HTML, XML). Metadata technology is necessary to achieve the scale of

deployment expected for large enterprise systems. Table C-12 provides a normalized rating for the level of support of self-description and metadata.

Table B-12
Normalized Rating of Self-Description

Rating	Title	Description
1	Pre-Configured	No self-description. Endpoints using the technology must be configured by hand before their use.
2	Parameters Exchanged	Endpoints using the technology may identify key information about themselves to identify configuration conflicts, e.g. version numbers.
3	Negotiation	Endpoints using the technology may negotiate important features before communicating, permit backward compatibility, and/or provide meta-data during normal communication.
4	Offline Configuration	Endpoints may use the technology to configure themselves offline using standardized file formats.
5	Plug-and-Play	It is possible to connect two endpoints together and expect them to communicate with the full set of features found in the technology.

Applicability to the Power Industry

Table C-13 provides a rating for how applicable the technology is for the power industry. Many technologies were eliminated from consideration for use in the utility implementations because they were too specific to particular industries. There may be several protocols, for instance, that could work technically but use object models and functions that are too specific to industrial automation. Other technologies were too generic depending on where they were applied. XML, for instance, in the past was viewed to be an excellent generic presentation technology but without adaptation to the industry with a power industry specific schema. With the XML-based messages for utility protocols such as DNP XML Schema and the IEC 61850-6 Substation Configuration Language (SCL), the score for XML is higher now than it was in the past.

Table B-13
Normalized Rating of Applicability to the Power Industry

Rating	Title	Description
1	Never Used Here	The technology either cannot be used in the power domain, or has never been used in the power industry and so cannot be evaluated
2	Occasionally Used Here	The technology may be used in the power industry as a part of a few pilot projects
3	Frequently Used Here	The technology is often used in the power industry.
4	Designed for Here	The technology may or may not be often used, but is designed specifically for use in the power industry.
5	Power Industry Standard	The technology is designed for the power industry and is also a recognized standard in the industry.

Applicability to Utility Systems

Most of these technologies were selected because they addressed at least some part of the wide range of utility domains. The range of domains extends from the enterprise level communication to the feeder device and consumer meters. Due to the wide range of domains included in the utility architecture, the scores for Utility Applicability rating are similar or identical to the Applicability to the Power Industry ratings. See Table C-14 for rating definitions for the applicability of the technology for utilities.

Table B-14
Normalized Rating of Applicability to the Utility

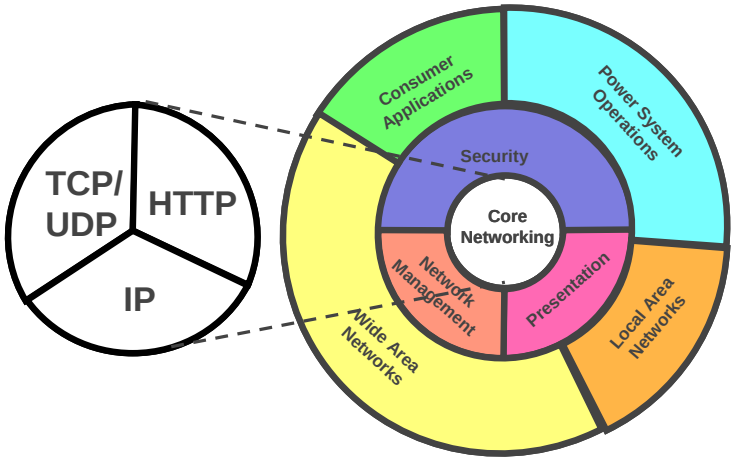
Rating	Title	Description
1	Never Used Here	The technology either cannot be used in power system domain, or has never been used in known utility environments and so cannot be evaluated
2	Occasionally Used Here	The technology was used in the utility environment as a part of a few pilot projects
3	Frequently Used Here	The technology is often used in the utility environment.
4	Designed for Here	The technology may or may not be often used, but is designed specifically for use in the utility environment.
5	Industry Standard	The technology is designed for the utility environment and is also a recognized standard.

Criteria Not Included

It should be noted that there were a few candidate criteria that were not included in the assessment, at least in the formal ratings. Where these criteria appear to be significant, they were discussed in the "strengths" and "weaknesses" sections of each technology.

- **Overall cost.** The main barrier to using the cost criterion was trying to develop a normalized rating across technologies. The technologies are so dissimilar in functionality that developing a common measure for cost was nearly impossible. Many cost factors are involved, including startup, licensing, and lifecycle costs. Because utility systems could evolve in many different ways, the discussion of cost factors occurs in the text, and cost is not an assessment criterion.
- **Maintainability.** Although partly covered under Manageability, measuring the ability of a technology to be maintained would require detailed statistics over a period of years, which were simply not available.
- **Functionality.** Evaluation of technology functional effectiveness is difficult largely because functionality is subjective measurement. It is assumed that if the technology was not acceptable for the job it was intended, it would not be widely adopted.

Core Networking Technologies



Core network technologies are basic communications protocols between devices and systems in the network.

All of the technologies described here are part of the Internet Protocol suite, administered by the Internet Engineering Task Force (IETF) and the Internet Assigned Numbers Authority (IANA).

Thanks to the popularity of the World Wide Web applications, the Internet Protocol suite is one of the most widely deployed technologies in the world

today, and can thus it be implemented at low cost. It is clear that the local and wide area networks must be IP-compatible.

The only plausible alternative to Internet protocols would be the International Organization for Standardization (ISO) suite. However, power industry experience has shown (with IEC 60870-6 and IEC 61850) that when – after considerable debate – both ISO and IP suites were specified, the ISO suite was rarely used. In the interest of preventing a repeat of that debate, the assessment therefore recommends only the IP suite.

The Internet Society (ISOC) serves as a users' group for the Internet protocol suite, providing training, marketing, news and forums on the future of the Internet. It is also the organizational home of IETF and IANA and several other Internet-related bodies. The IETF manages a large body of documentation on Internet technologies, including Requests for Comments (RFCs), Standards (STDs), Proposed Standards, and Internet Drafts. One particularly useful document is RFC 1123 (STD0003), which identifies the minimum protocol implementation for Internet host devices.

References:

- http://www.isoc.org – Internet Society
- http://www.ietf.org – Internet Engineering Task Force
- http://www.iana.org – Internet Assigned Numbers Authority
- http://www.rfc-editor.org – Request for Comments (RFC) archive (standards documentation)

IPv4

The Internet Protocol version 4 (IPv4) is the network layer for the Internet suite of protocols (RFC 791, STD0005). Its primary characteristics arise from the fact that the structure of its four-byte address space was originally intended to (and still does) provide some information on how a message should be routed. Addresses with the same prefix share a *subnet* and don't need to be forwarded; addresses with different prefixes must be forwarded elsewhere. IP's simple routing logic makes it easy to implement for end devices.

As the Internet has expanded and new high-bandwidth, low-latency applications have developed, however, the IP address structure has proven to be restrictive. Both the number of Internet addresses and the haphazard way messages were originally routed have proven to be insufficient. The Internet backbone has therefore evolved a number of ever more complex routing protocols and algorithms to work around these inherent limitations.

One of the most common mechanisms to solve the lack of address space in IPv4 is Network Address Translation (NAT), a method by which a router can make a large number of devices appear to have a single IP address on the Internet. NAT is now so commonly used it is considered a standard feature of most corporate

networks. NAT and similar techniques are enhancements that demonstrate the flexibility of the Internet protocol.

Application to utility systems: Common network layer.

Strengths: Ubiquity, ease of implementation for end devices.

Concerns: Security and quality-of-service have been added on and were not originally native to the protocol.

Layer: Network

References:

See above

IPv6

The Internet Protocol version 6 (IPv6) is the Internet Engineering Task Force's next-generation version of the Internet (RFC2460). It addresses the key limitations of IPv4, specifically:

- A 128-bit (16-byte) address space rather than the 32-bit IPv4 address.
- Automatic address configuration and inherent support for renumbering networks.
- Built-in support for guaranteed quality-of-service and security
- Greatly enhanced performance of message forwarding and route discovery

Of these enhancements, the one most discussed is the additional address space. The existing Internet uses Network Address Translation (NAT) to make a large number of network devices (like corporate intranets) appear as a small number of public Internet addresses. Key applications like peer-to-peer (P2P) file sharing, virtual private networks (VPNs), Voice Over IP (VoIP) and video on demand would work better using IPv6 rather than NAT.

The IPv6 standard has been defined for over a decade now, and it is supported as an alternate protocol stack by all major commercial communications vendors including Microsoft, Cisco, Nortel and Sun. Transition from IPv4 to IPv6 has been slow at least partially because of the capital-intensive requirement to change all equipment and network addresses. However, IPv4 and IPv6 can co-exist and be "tunneled" over each other, and a few key events indicate that IPv6 rollout may be gaining speed:

- In September 2010, federal government CIO Vivek Kundra decreed that all federal agencies upgrade their public-facing Web services to native IPv6 by Sept. 30, 2012. The 3rd Generation Partnership Project (3GPP) for wireless telephony has announced that all 3G cell-phones will support IPv6.
- In December 2010, Verizon announced that it is launching an IPv6 transition service anticipating that large organizations will soon need assistance to convert to IPv6.

IPv6 is promoted worldwide by the IPv6 Forum, which has spawned several local task forces. The North American IPv6 Task Force is sponsoring "MoonV6", a large global IPv6 pilot project, and many other local IPv6 Task Forces exist to promote IPv6.

Application to utility systems: Common network layer.

Strengths: The huge addressing space and the built-in security and network management features make IPv6 a natural fit for large networks.

Concerns: Transition to IPv6 had been slow but implementations are increasing.

Layer: Network

References: See above and the following:

- http://www.ipv6forum.com – IPv6 Forum
- http://www.nav6tf.org – North American IPv6 Task Force
- http://www.moonV6.com – Large IPv6 pilot project
- http://www.cav6tf.org – California IPv6 Task Force

TCP

The Transmission Control Protocol (TCP, RFC793, STD0007) is the reliable transport layer service of the Internet Protocol suite. Using acknowledgements and retries, it ensures IP data is delivered in the correct order with no lost packets. Most IP-based security technologies use TCP to help protect against "replay" attacks. Versions of TCP software exist that can use either IPv4 or IPv6 networks.

Application to utility systems: Common reliable transport layer for most communications.

Strengths: Ubiquity, reliability.

Concerns: Stream-oriented, rather than packet-oriented, as most utility protocols are. Timers are generally too long to detect the loss of a device or link quickly (the recommended default timeout is 5 minutes), so application layers must perform timeout and recovery logic.

Layer: Transport

References:

- See above

UDP

The User Datagram Protocol (UDP, RFC768, STD0006) is a simple transport layer "wrapper" for protocols that do not require reliability or high levels of security. Unlike TCP, UDP messages are sent on a "best effort" basis without retries, which makes it more suitable for real-time messages such as voice traffic. UDP is used with network management protocols such as SNMP and NTP, and for broadcasting messages such as announcements or the availability of certain services. Versions of UDP software exist that can use either IPv4 or IPv6 networks.

Application to utility systems: Transport layer for non-critical notifications, e.g. reporting statistics.

Strengths: Ubiquity, simplicity.

Concerns: Use should be carefully limited to non-critical data. Some technologies permit use of a UDP profile under certain restricted conditions, but vendors have a tendency to implement UDP first because it's easier. Often used for broadcast messages, use of data streaming using UDP should be limited to prevent performance problems.

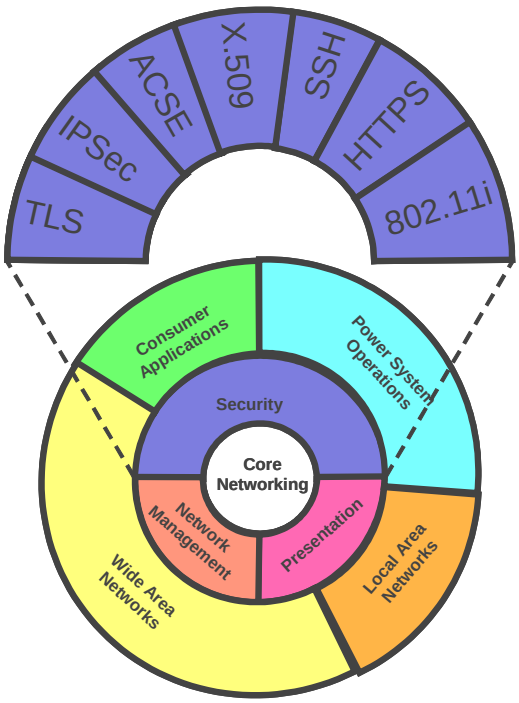
Layer: Transport

References:

- See above

HyperText Transfer Protocol (HTTP)

The Hyper Text Transfer Protocol (HTTP, RFC2616), together with the Hyper Text Markup Language (HTML), spawned the revolution known as the World Wide Web. HTTP is the mechanism for transferring pages between web servers and browsers. It is a fairly simple, text-based, request-and-response protocol that continues to be used as the content it carries evolves from static web pages to extremely interactive services.



Application to utility systems: Transferring data to and from various human-machine interfaces. It is also used as an "envelope" for other many types of web services such as SOAP.

Strengths: Ubiquity, human-readability

Concerns: Not very efficient. Some technologies that try to use HTTP and other text-based web protocols to exchange real-time data may fail because of performance problems.

Layer: Application

References:

- http://www.w3.org – World Wide Web Consortium

Security Protocols

Security is required for utility communications. The need for security measures in the utility environment includes requirements from the Federal Energy Regulatory Commission (FERC). FERC mandates compliance with eight critical infrastructure protection (CIP) reliability standards designed to protect the nation's bulk power system against potential disruptions from cyber security breaches.

The eight FERC CIP reliability standards address the following security areas:

- Critical Cyber Asset Identification

- Security Management Controls
- Personnel and Training
- Electronic Security Perimeters
- Physical Security of Critical Cyber Assets
- Systems Security Management
- Incident Reporting and Response Planning and
- Recovery Plans for Critical Cyber Assets.

The FERC reliability standards were developed by the North American Electric Reliability Corporation (NERC), which FERC has designated as the electric reliability organization (ERO). NERC is tasked with monitoring the development and implementation of cyber security standards by the National Institute of Standards and Technology (NIST). In October 2010, NIST recommended IEC 62351 as the standard to be used for cybersecurity for the communication protocols defined by the four sets of interoprability communication protocols.

Security is a major concern with smart grids, which are especially vulnerable to attack because of the two-way communication between devices and the utility grid.

Security is a very broad area of discussion. Today there are three main technical issues in applying communications security to the utility industry:

- **What layers to use?** Should security be applied at the data link, transport, network, or application layer, or some combination of those four? There are standards, proposals and valid arguments for each of these options.
- **How to manage security credentials?** Managing security credentials is a massive undertaking, especially for thousand to millions of devices, and one which technology does not help very much compared to the organizational processes and resulting costs that must be incurred. One particularly difficult issue is the revocation of authorization of a user (e.g. employee vacates company).
- **How to ensure the system adapts and evolves?** As attackers find vulnerabilities in security technologies, a network of systems must be able to upgrade to the latest solutions.

The two main candidates for IP-based security are Transport Layer Security (TLS) and Secure IP (IPsec). Although each has different vulnerabilities, in practice there is not much difference in the level of security provided between the two. The main differences between them are which protocol layer they work at, and how easy they are to implement and use. Both of them have the capability to adapt to new cryptographic algorithms.

Transport Layer Security (TLS)

Transport Layer Security (TLS, RFC4346) was originally developed under the name Secure Sockets Layer (SSL) by Netscape, as a mechanism to secure communications between web servers and client browsers. There are slight differences between SSL and TLS; TLS is now considered to be the definitive standard. Whenever the "lock" icon appears in the corner of a web browser window, it is typically because TLS that is being used to provide security.

TLS provides end-to-end authentication and encryption, operating between the transport layer (TCP) and upper layer application protocols like HTTP. When a connection is established, TLS performs authentication using X.509 certificates and automatically negotiates the cryptographic algorithms to be used for communications.

Although TLS is typically used directly between a client and a server at the transport layer, some implementations are beginning to create Virtual Private Networks (VPNs) by "tunneling" messages from one network through a TLS connection to another site.

Application to utility systems: Preventing data from being viewed or modified by attackers.

Strengths: Provides end-to-end security rather than site-to-site, so physical security within a site can be less strict – if all devices at a site are using TLS. Perceived to be easier to configure and manage than IPsec.

Concerns: Each application and each device that supports TLS must be modified to do so.

Although TLS permits authentication in both directions, its most common use is for e-commerce, in which only the identity of the server is verified. When one connects to the web-site of a bank, for instance, the web browser uses TLS to check that the site holds a certificate from an authority that the browser recognizes. The certificate confirmation authenticates the bank. However, the bank does not use TLS or certificates to authenticate the user. That direction of authentication is usually performed using a user ID and password, once an encrypted link has been established.

Deployment of TLS would require TLS authentication of ***both*** client and server. Such two-way authentication would require management and distribution of certificates at both ends of the link. Use of certificates could reduce some of the perceived ease-of-use of TLS.

Layer: Transport

References:

- See above
- http://www.openvpn.org – Use of TLS for virtual private networks

Secure IP (IPsec)

IP Security, or Secure IP, is a suite of several protocols (RFCs 4301-4309) that are used to provide authentication and encryption at the IP network layer. These protocols include the Authentication Header (AH), Encapsulating Security Payload (ESP), and Internet Key Exchange (IKE). IPsec was developed by the IETF and is a required part of IPv6.

IPsec is implemented by most major router vendors as a technology for providing Virtual Private Networks (VPNs). A VPN provides a secure "tunnel" between two locations over an insecure intervening network. IPsec can also provide end-to-end security. IPsec was developed in conjunction with IPv6 and is therefore mandatory in all standards-compliant implementations of IPv6, but because of the slow deployment of IPv6, IPsec is most commonly used to secure IPv4 traffic.

IPsec authentication can use public key certificates as with TLS. IPsec can also use a number of different types of security credentials, including simple passwords.

Application to utility systems: Preventing data from being viewed or modified by attackers.

Strengths: From a theoretical point of view it makes more sense to perform security at the network layer. By changing just the network layer software, all applications on a device can be secured. For instance, implementing IPsec on a device can secure all applications using TCP or UDP, while TLS can only secure those applications using TCP which have been modified to do so. By replacing a router at a site with an IPsec router, all devices at that site can be secured without altering any of the other devices in the site.

Concerns:

- IPsec is perceived as being extremely complex to implement, configure and use compared to TLS.
- IPsec is difficult to deploy in networks that make use of Network Address Translation (NAT) because NAT requires the using the real IP address of an endpoint. Since NAT is in widespread usage to conserve IP addresses (see above), widespread usage of NAT is a significant barrier to the deployment of IPsec.

Layer: Network

References:

- See Internet references above
- http://www.vpnc.org – Virtual Private Networks Consortium

Secure Hyper Text Transfer Protocol (HTTPS)

The Secure Hyper Text Transfer Protocol (HTTPS, RFC 2818) is the secure version of HTTP (see above), used to authenticate and encrypt file transfer between a web server and a browser. It is essentially HTTP over TLS and is the most common user of TLS. It is widely used for electronic commerce over the Internet and other applications where secure transfer of data between application and users is needed.

Application to utility systems: Interfaces between applications and between applications and users. Secure access by engineering or maintenance personnel to a web server as part of a system or a connected device.

Strengths: Widely used, thoroughly proven standard used for e-commerce and many other applications including those operating under the Health Insurance Portability and Accountability Act (HIPAA) requirements which imposes both privacy and security requirements.

Concerns: None.

Layer: Application

References:

- See Internet references above
- http://www.w3.org – World Wide Web consortium.

Secure Shell (SSH, SCP and SFTP)

Secure Shell (SSH) is a secure means of logging in to a remote device for the purpose of entering text commands (RFC4250-4256). It is intended to replace the earlier Internet standard Telnet which was extremely insecure because it transmitted unencrypted passwords across the network.

The name SSH refers both to the protocol used for communication and the program used to invoke it. Besides being used for remote login, the SSH protocol can also transfer files by invoking the Secure Copy (SCP) or Secure File Transfer Protocol (SFTP) programs, which are typically packaged with SSH.

As its name implies, Secure Shell originated on Unix systems. In addition to replacing Telnet, it is also intended to replace the Remote Shell (RSH), Remote Copy (RCP), Remote Login (rlogin) and File Transfer Protocol (FTP) programs, all of which had security problems. SSH is now available on most platforms including Windows and MacOS. Besides remote login and file transfer, SSH is sometimes also used to provide a secure "tunnel" for other less secure protocols. Tunneling is the process of carrying one or more non-secure protocols within the "envelope" of a secure protocol. Various programs exist to open these tunnels using SSH and redirect TCP connections through them, similar to Virtual Private Networks (VPNs).

SSH has an odd history. Its original version, known as SSH-1, was based on open source, but since that time companies have tried to license commercial versions of it. A newer version, known as SSH-2, was created to improve the security of the protocol and add integrity checking on the data. Recently, open source implementations of both versions, based on the original, have reappeared. Commercial, shareware, freeware and open source implementations are now all available. SSH is not yet an Internet standard, although SSH-2 has been submitted as a proposed draft standard.

Application to utility systems: Secure login to a devices and gateways and secure file transfer. Use of SSH for secure tunneling of other protocols is not recommended because of the inefficiency of the extra overhead; SSL or IPsec should be used instead. Recommend using SSH-2 because of improved key management and the message integrity checking.

Strengths: Strong user community; has been released with many versions of Unix and Linux. Can use a variety of authentication mechanisms; SSH-2 includes support for X.509 certificates.

Concerns: Odd licensing status means implementers must be careful of which version they use. Not recognized by any standards body yet.

Layer: Application, Transport

References:

- www.ssh.fi – SSH Communications Security, creators and sellers of SSH
- www.openssh.com – Open SSH project
- http://www.ietf.org/html.charters/secsh-charter.html - Secure Shell working group within the IETF, and the proposed draft standard documents.

X.509 Public Key Infrastructure

X.509 is a standard from the International Telecommunications Union (ITU-T) for defining a Public Key Infrastructure (PKI). It defines a standard format for *public key certificates* and rules governing their use, verification, and revocation.

Public key certificates are necessary because most modern security technologies (including those discussed here) perform authentication based on public key encryption, also known as asymmetric encryption. Asymmetric encryption uses two keys generated mathematically at the same time, one public and one private. The public key can only decrypt data encrypted with the private key, and vice versa. Asymmetric encryption permits the public key to be transmitted freely and openly as long as the private key is kept truly private to one of the users.

The need for certificates and PKI arises because the receiver of a message must ask the question, "How do I know that this is really the public key of the sender?"

The answer is that an organization or person known as the *certification authority* (CA), who is trusted by both sender and receiver, must attest to the identity of the sender by issuing a *certificate*. A certificate is a file containing the sender's name and public key, digitally signed by the CA using the CA's public key. The CA's public key is broadly distributed and well-known. The problem then becomes, "How do I know that this is really the CA's public key?" and so on, ad infinitum. The recursiveness of trust is why the mechanism for managing public keys is usually complex and is described as an *infrastructure*.

X.509 addresses recursive trust identification by specifying:

- A standard format for certificates
- A mechanism for establishing and verifying "chains" of certificates. These chains may be simple hierarchical trees, or more complex relationships.
- A standard format for certificate revocation lists (CRLs)

X.509 is based on the X.500 directory standard, which is very complex. The IETF has therefore taken the X.509 standard, simplified it and applied it to the context of Internet protocols. The IETF X.509 profile is described in RFC3280 and is usually the standard people mean when they say "X.509 compliant". The IETF also defines a protocol for determining if a certificate has expired, called the Online Certificate Status Protocol (OCSP, RFC2560).

Application to utility systems: A system for managing the security credentials of an network.

Strengths: Few competitors. The Pretty Good Privacy (PGP) cryptographic scheme supports the creation of certificate authorities and certificate revocation, and is widely used for email encryption. However, it does not cover the same scope as X.509 PKI and is not recognized by an international standards body like the ITU.

Concerns: Complexity and the amount of organizational and process change required to implement it properly. Because of these concerns, there has been reluctance among vendors and user to accept the complete X.509 infrastructure. While most implementations recognize the standard certificate format, for instance, many do not have the ability to check whether a given certificate has been revoked. Certificate revocation methods have not yet been widely adopted. The need to address certification revocation has been identified as part of the IntelliGrid Architecture recommendations. Further the infrastructure to manage certificates is non-trivial and many organizations must add staff to support certification functionality.

Layers: Application

References:

- http://www.ietf.org/html.charters/pkix-charter.html - IETF Public Key Infrastructure (PKIX) working group

- http://www.itu.int/ITU-T - International Telecommunication Union

Wireless Network Security (IEEE 802.11i, WPA2)

The IEEE 802.11i standard, also known as Wi-Fi Protected Access version 2 (WPA2), is the new standard method for securing the IEEE 802.11, or "Wi-Fi", wireless LAN protocols. It replaces the earlier Wired Equivalent Privacy (WEP) and first version of WPA issued by the Wi-Fi Alliance, which has known vulnerabilities.

IEEE 802.11i uses the Advanced Encryption Standard (AES) for encryption and authentication between the end device and its wireless switch. Authentication is based on the Extensible Authentication Protocol (EAP) per the earlier IEEE 802.1X standard. It may be used either with a centralized authentication server, or using pre-configured keys. Certificates are not usually used.

IEEE 802.11i is promoted by the Wi-Fi Alliance, which does certification testing of IEEE 802.11 products.

Application to utility systems: Protecting data from attack. Primary potential applications are within field installations for equipment monitoring devices.

Strengths: As the third-generation attempt at securing Wi-Fi, it has been well-reviewed. WPA2 products can be certified by the National Institute of Science and Technology (NIST) Federal Information Processing Standard (FIPS) 140-1.

Concerns: Although there is huge industry and government support for the standard, it is relatively new.

Layers: Data Link

References:

- http://www.wirelessethernet.org - Wi-Fi Alliance
- http://standards.ieee.org/getieee802/802.11.html - IEEE 802.11 standards
- http://csrc.nist.gov/publications/fips - FIPS 197-1 (AES) and FIPS 140-1

Association Control Service Element (ACSE)

The Association Control Service Element (ACSE) is worth noting in the security service group because several other key technologies in the Power System Operations and Consumer Applications service groups make use of it to provide application-layer security:

- IEC 61850 Substation Automation
- IEC 61850-7-420 Distributed Energy Resources

- The IEC 61850 series of standards was originally developed to define a set of next-generation communications protocols for substation automation. Since its initial release in 2004 its scope has been expanded to include almost every aspect of utility communications.

The core of the IEC 61850 series is the "Part 7" standards, which include:

- **IEC 61850 -7-2 Abstract Communication Services Interface.** Specifies the protocol services possible with IEC 61850 such as reading data, operating controls, spontaneously reporting data, file transfer, and the framework for defining data objects.
- **IEC 61850-7-3 Common Data Classes.** Describes the lowest-level data types used for building data objects.
- **IEC 61850-7-4 Basic and substation logical node classes and data object classes.** Describes the data objects built from the Common Data Classes and defines "logical nodes" which are functional groupings of data objects.

The IEC 61850-7-420 standard is an extension of IEC 61850-7-4 that specifically defines the data to be exchanged with DERs. It makes use of the IEC 61850-7-3/4 common data classes, data objects and logical nodes and adds those required for implementing DERs.

Application to utility systems: IEC 61850-7-420 models will applicable to the control and monitoring of renewable generation resources as well as storage systems.

Strengths: Models are easily integrated into 61850-based systems

Concerns: Limited vendor involvement has led to large, overly specific data models

Layers: Application layer.

References:

- http://www.iec.ch – International Electrotechnical Commission
- IEC 61968/61970 Common Information Model
- IEC 60870-6 Telecontrol Application Service Element (ICCP/TASE.2)ANSI Metering (ANSI/IEEE C12.19 and C12.22)
- DLMS/COSEM (IEC 62056)

ACSE is defined by the ISO as part of the OSI suite. It a relatively simple protocol dedicated to the process of setting up an association between two application layer entities (e.g. processes, tasks, etc.) on a network. It provides a mechanism for negotiating the *context* under which the two entities will communicate. The context may include such items as the version of protocol they will use, the object model, the names of software applications that may be involved, and optionally, the security credentials of the two ends.

ACSE provides a mechanism for authenticating both application entities, but does not specify the format of the cryptographic credentials or the algorithms used to build them. It essentially provides an authentication "envelope" which other protocols may use prior to beginning communications. Therefore, the level of security provided through ACSE is determined by the security choices made in the technology which uses ACSE. Because of this, ACSE is not evaluated as a separate protocol in the technology assessment.

ACSE does not provide encryption services, but may negotiate encryption services to be provided by a lower layer. It has a connectionless (datagram) version, but provides the best security over connection-oriented protocols like TCP.

ACSE does not have any users' group. It is ISO/IEC standard 8649 and 8650. It is standardized by the ITU-T as X.217, X.227, and X.237.

Application to utility systems: Used with the ISO application layer protocols listed above to provide authentication. Since all of these technologies make use of ACSE, it may be able to provide a common ground for interoperability, for instance determining which application object model is being used by a particular device.

Strengths: Many protocols do not have an "association set up" step, or provide an "envelope" for exchanging security credentials. Those technologies which use ACSE at least have the ability to provide authentication in the future, if they do not have it now.

Concerns: ACSE by itself does not guarantee security. The protocol that is using ACSE must first specify the format of the security credentials, and any given device must choose to implement them.

Layers: Application

References:

- http://www.iso.org – International Organization for Standardization
- http://www.itu.int/ITU-T - ITU-T.

IEC 62351 Series – Security within IEC TC57 standards

The 62351 series of standards defines security requirements and solutions across several distinct series of standards:

- IEC 61870-5 (SCADA standards including DNP3)
- IEC 61870-6 (TASE.2/ICCP) One of the initial set of 5 NIST recommended Smart Grid standards.
- IEC 61850 (substation and systems engineering standard)
- IEC 61970 (Core CIM Model for generation and transmission systems)
- IEC 61968 (Extends CIM model to distribution systems)

The series presently has seven parts:

- IEC 61850 Substation Automation
- IEC 62351-2 -Glossary
- IEC 62351-3 –TCP/IP security (how to use TLS)
- IEC 62351-4 –MMS Authentication (using ACSE)
- IEC 62351-5 –Security for 60870-5 and DNP3 protocols
- IEC 62351-6 –Security for 61850 reduced-stack (layer 2) protocols
- IEC 62351-7 –Network management

Application to utility systems: 62351 standards are the NIST recommended cyber security standard the CIM and substation DNP3 and MMS-based standards such as 61850 and ICCP. Additionally, 62351-3 defines a method to secure any TCP-based protocol.

Strengths: 62351 series of security standards provide a comprehensive set of expert-endorsed security measures.

Concerns: The standard provides no guidance on when security must be applied.

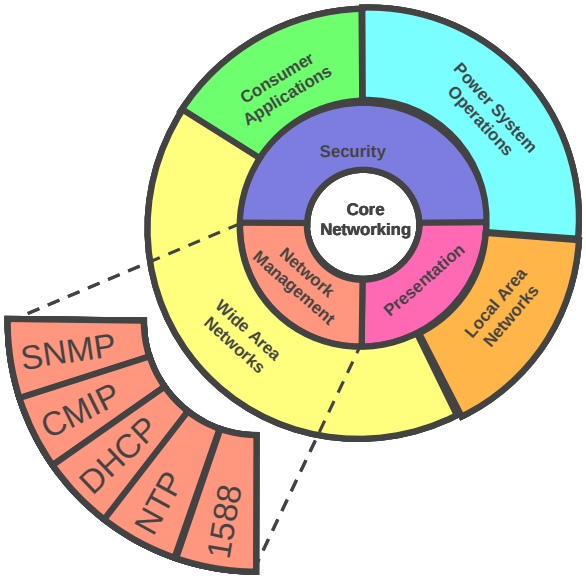
Layers: Application

References:

- http://www.iec.ch

Network Management

Network management describes the recommended technologies for managing and administering networks of utility systems and devices.



Basic IP Address Management (ARP, DNS, DHCP)

Implementations of IP are almost always accompanied by three protocols that amount to "self-description" at the network layer.

- Address Resolution Protocol (ARP, RFC826, STD0037) finds the hardware address for a particular IP address, and permits devices to announce their presence on the network.
- Domain Name System (DNS, STD0013) converts logical names to IP addresses and permits end devices to register their own logical name in the distributed database.
- Dynamic Host Configuration Protocol (DHCP, RFC2131) enables end devices to discover their own IP address and other networking parameters. DHCP has evolved from earlier protocols such as the Reverse Address Resolution Protocol (RARP, RFC903, STD0038), and the Bootstrap Protocol (BOOTP, RFC0951), both of which are still used.

IPv6 networks will support updated versions of these protocols, integrated with IPv6's automatic address configuration capabilities.

Application to utility systems: Together, these protocols make it possible for end devices to connect to a yet-unknown network and easily access services without pre-configuration. Network address resolution and configurations is a key capability for a network that may consist of thousands or millions of devices.

Strengths: Ubiquity, ease of use, scalability.

Concerns: The use of DNS and DHCP in utility networks has been the subject of some debate. Utility system engineers have been reluctant to make end devices dependent on DNS or DHCP servers, since in their minds these servers would constitute single points of failure for the network. However, the DNS and DCHP standards do provide for redundancy, so it is likely that both standards will gradually spread into utility networks as IT best practices are adopted there.

Layers: Application, Network, Data Link

References:

- See the internet references above

Simple Network Management Protocol (SNMP)

The Simple Network Management Protocol (SNMP) is the Internet standard for performing network management. There are several versions currently in use, but the IETF recognizes SNMP version 3 (RFC3411, RFC3418, STD0062) as being the definitive version.

In SNMP, each server device defines objects known as Management Information Bases (MIBs) containing measurement variables appropriate to that device.

There are a variety of standard MIBs, mostly defined for communications equipment such as Ethernet interfaces or routers. MIBs have simple text names that must be known by the client making the request. The basic SNMP operations that may be performed on a MIB are to read or write. SNMP servers may also spontaneously report alarms. Later versions of SNMP provide application layer security for management operations.

Application to utility systems: Reporting communications statistics and alarms, changing configuration parameters from all levels of the IT infrastructure.

Strengths: Ubiquity, simplicity. A variety of software tools exist for managing networks using SNMP.

Concerns: No built-in mechanism for controlling firmware upgrades or other file transfers. No meta-data or means for self-description. Standard MIBs may exist for many of the current systems and devices used in a utility; however new custom MIBs may need to be defined for new or legacy devices not currently supporting SNMP. Earlier versions of SNMP had serious security problems, although these have been solved in SNMPv3.

Layers: Application

References:

- See internet references above

Common Management Information Protocol (CMIP)

The Common Management Information Protocol (CMIP, ISO/IEC 7498-4) is the standard defined by the International Organization for Standardization (ISO) for network management. It was developed as part of the ITU-T X.700 management framework with the intention of addressing certain deficiencies in SNMP.

CMIP servers, known as Common Management Service Elements (CMISEs) define objects using *Distinguished Names*. Distinguished Names are strings of integers representing portions of a hierarchy, similar to a file structure, which must be registered either with ISO or with the operator of the network.

CMIP is designed to work with an X.500 directory for determining where in the network a given object exists. If no such directory exists, the client must be preconfigured with the names of all objects on a server that the client might need to use.

A CMISE may define any number of different services, or "methods" that can be performed on a given object, and select portions of an object to be read-only or read-write. As in classic object-oriented design, standard CMIP object classes may be expanded upon by any given CMISE with vendor-specific information. A client connects to a CMISE using the Association Control Service Element

(ACSE, ISO/IEC 8649 and 8650), which can support application layer authentication and encryption.

Application to utility systems: Network management

Strengths: Extremely flexible and able to implement almost any network management function. Unlike SNMP, it can execute tasks remotely and has a better mechanism for spontaneously reporting network problems. It has built-in security through ACSE.

Concerns: Used within the telecom industry, but otherwise not very common. It is complex to implement, requiring several different companion protocols and services (e.g. ACSE, or the X.500 directory). It was intended for use with a seven-layer ISO protocol suite, so implementations must include at least the ISO presentation and session layers, plus an RFC1006 implementation for connecting an ISO stack to TCP. RFC1189 specifies CMIP over Internet protocols, but has been rarely used.

Layers: Application

References:

- http://www.iso.org – International Organization for Standardization
- http://www.itu.int/ITU-T/ – International Telecommunications Union

Network Time Protocol (NTP and SNTP)

The Network Time Protocol (NTP, RFC1305) is the Internet standard for synchronizing time between multiple devices across a network. NTP works over UDP using a simple message format that, among other things, contains the times of transmission and reception of each message and the stratum (accuracy and precision) of the clock at each location.

Using a series of successive approximations weighted by the perceived reliability of each source, each NTP clock converges on the correct time independently. Locally, an NTP implementation uses a feedback algorithm similar to a phase-locked loop to adjust its clock. It may adjust not just the time, but the frequency of the clock, to reduce the time required to converge.

The Simple Network Time Protocol (SNTP, RFC2030 and RFC4330) is a simplified version of NTP intended to be used when there is only a single time server, and sometimes only a single client. It uses the same message format as NTP, but does not attempt to converge multiple clocks. It can be used in request/response, broadcast, or multicast modes. Mechanisms for ensuring accuracy, such as averaging or other types of statistical analysis, are considered local issues outside the scope of the standard. NTP servers must respond to SNTP requests.

Application to utility systems: Synchronizing time for a wide range of devices where GPS receivers/clocks are not available or practical and where the NTP implementation provides an adequate level of accuracy. In the future, many connected devices will need to be synchronized. SNTP may be more appropriate than NTP for applications such as consumer portals where there may be only a few (probably redundant) servers in the network. More accurate solutions may be needed such as IEEE 1588 – see below.

Strengths: NTP is widely implemented, on products having a great variety of different levels of accuracy. Software versions for Windows exist, for instance, that may provide accuracies in the 100s of milliseconds, while there are dedicated satellite servers that can get down to the sub-millisecond level if the client implementation permits it.

Concerns: The accuracy of any network time synchronization method will be greatly dependent on the hardware and software implementation on any given device. To be reliably accurate, a detailed hardware and software reference design for IED time synchronization is necessary.

Layers: Application, Data Link, Physical

References:

- See internet references above

Precision Time Protocol (IEEE 1588)

The Precision Time Protocol (IEEE 1588, IEC 61588) was developed primarily by makers of industrial drive control systems and utility protection devices who required sub-millisecond or even tens-of-microsecond time synchronization accuracy across local area networks. It was designed to be independent of LAN type, but was primarily designed for Ethernet. The National Institute for Science and Technology (NIST) was closely involved with its development.

At such levels of accuracy, the variation in the latency of an Ethernet switch, the number of Ethernet collisions, and most importantly, the non-determinism of the operating system on any given device become factors in the accuracy of synchronization

IEEE 1588 attempts to address these issues by specifying that a time server should be an integrated part of the LAN switch, and that there should be a hierarchy of servers, i.e. switches should synchronize with other switches. IEEE 1588 also discusses how best a time client can eliminate the effects of various factors on synchronization accuracy, but stops short of dictating these measures for compliance.

Note a new Power Profile for IEEE 1588 is nearing completion. Refer to IEEE C37.238, "Standard Profile for Use of IEEE 1588 Precision Time Protocol in Power System Applications"

Application to utility systems: Time synchronization for applications and devices where sub-millisecond or even microsecond time synchronization accuracy is required. Example applications are protection devices, digital fault/event recorders, phasor measurement units and phasor data concentrators.

Strengths: Can achieve extremely high time accuracy even through multiple Ethernet switches.

Concerns: Not widely adopted yet. Those vendors that support it claim they can achieve nearly the same results using SNTP. To achieve accuracy finer than hundreds of microseconds requires hardware support, which is also true of NTP. As noted for NTP, a hardware and software reference design for device time synchronization should be developed. Accuracy levels near one microsecond require the use special Ethernet switches (transparent clocks).

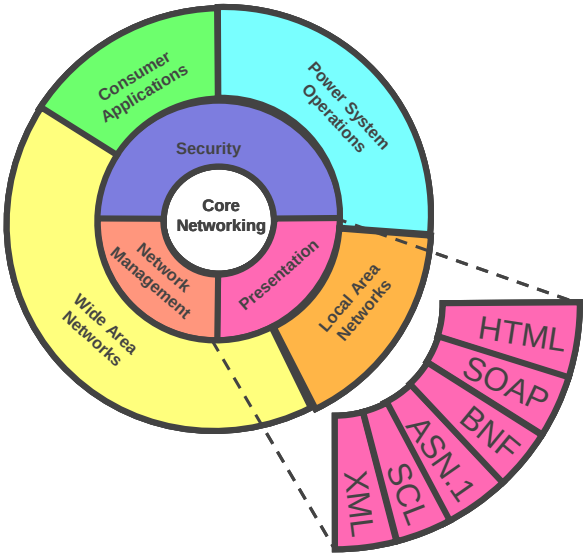
Layers: Application, Data Link, Physical

References:

- http://www.ieee.org – IEEE
- http://www.iec.ch – IEC
- http://ieee1588.nist.gov/ - NIST information site

Data Structuring and Presentation

Presentation and data structure technologies make it possible to organize data and present it in a manner that is independent of platform and implementation. Presentation technologies do not stand alone, but serve to enable other more application-specific technologies. Data structure technologies provide a standardized method of organizing and describing data. This section describes the recommended presentation technologies for networks of utility systems and devices.



The technologies described here are not the only technologies that can represent data objects; several technologies described in other groups implement the concept of data objects without using specific data structure technology. The protocols evaluated here are independent, general-purpose standards specifically designed for the purpose of data presentation and structuring.

HTML

HTML (HyperText Markup Language) was originally designed as a text formatting language that would permit people to create documents independent of how they were displayed and to embed links to other content for use by human readers. It was the first language used to define pages in the World Wide Web.

It is common for HTML files to be automatically created for use either by either human readers or other applications. The HTML language is based upon the language SGML (Standard Generalized Markup Language, ISO 8879:1986). It uses a system where portions of text are "tagged" and given specialized attributes. For example:

<body bgcolor=white>Hello</body>

In the example, the tag "body" is pre-defined by HTML. The example specifies that the text "Hello" should be displayed in white. Many networked devices already directly create HTML data in tabular format.

Application to utility systems: IEDs and networked devices already report data as human-readable HTML pages. HTML can be easily converted into other forms. Inter-system communication, e.g. gathering of LMP information from public sources.

Strengths: HTML is widely implemented. Often, the existing devices need no modification in order to communicate with other devices.

Concerns: HTML is not concerned with machine readability, only human readability. There are no standards for placement of data within the HTML file.

Layers: Presentation, application and above.

References:

- http://www.w3.org – World-Wide Web Consortium

XML

XML (eXtensible Markup Language) was designed as a replacement for HTML. It allows the markup content to be separated from the presentation. As described above, one of HTML's major shortcomings is that tags specify how data should be displayed and do not described the data itself. XML files specifically describe the data which is placed into the file. There are also provisions for describing the presentation of the data. In fact, XML files can represent anything which is representable by HTML. As an example of the markup, consider:

<address type=IP_Address>192.168.1.2</address>

As shown above, it is clear to both a human and a machine that an Internet Protocol address is being defined. XML allows an application to validate the contents, e.g. it could reject an address of "192.168.1". It should be noted that the tag "address" and the attribute "type" are NOT defined by XML, but are user-defined.

Application to utility systems: XML allows devices to clearly describe information content. Some protocols already use XML as the basis for their data transfers (such as Simple Object Access Protocol SOAP). XML will likely be the common language between enterprise-level applications.

Strengths: XML allows clear separation of content from display presentation. A variety of tools exist for viewing and modifying XML. It is becoming quite common as a mechanism for importing and exporting information from databases.

Concerns: XML is not as widely used for web pages and is more complicated to use than HTML; it requires the definition of an application-specific "schema" (or "Document Type Definition") to have meaning. XML is also inefficient in terms of processing and communication bandwidth compared to less generic communication systems.

Layers: Presentation, application and above.

References:

- http://www.w3.org – World-Wide Web Consortium

Backus Naur Format

Backus Naur Format (also known as Backus Normal Form or BNF) is a notational language first used to describe the syntax of programming languages. It allows precise definition of data placement with a file. It cannot easily describe the actual detailed representation of the file (the "bits and bytes")

A simple example illustrates the concept. A displayed decimal value could be described by the name "number" which recursively defined as either a digit or a number followed by a digit.

<number> ::= <digit> | <number> <digit>

<digit> ::= '0' | '1' | '2' | '3' | '4' | '5' | '6' | '7' | '8' | '9'

Application to utility systems: BNF can be used to describe the data objects within a device. A modified version of BNF was used to define the ANSI C12 metering standards.

Strengths: BNF allows clear definitions of the representational language (syntax) which can be machine-interpreted.

Concerns: BNF is very bulky and it does not define the semantics of the data or the procedures used to transmit it.

Layers: Presentation, application and above.

References:

- http://cui.unige.ch/db-research/Enseignement/analyseinfo/AboutBNF.html

ASN.1

ASN.1 (Abstract Syntax Notation –One) is a formal language (grammar) for abstractly describing messages to be exchanged among an extensive range of applications (ISO/IEC 8825 and 8825, ITU X.680 and X.690 series). ASN.1 is used for applications involving the Internet, intelligent network, cellular phones, ground-to-air communications, electronic commerce, secure electronic services, interactive television, intelligent transportation systems, Voice over IP (VOIP) and others. ASN.1 is designed to be machine-readable.

A simple example illustrates the usage of ASN.1. A pair of energy registers within a billing meter might be named "watt-var" and would be described as follows:

```
watt-var ::= SEQUENCE {
    watt-value      Energy-Value-Type,
    var-value       Energy-Value-Type }
Energy-Value-Type ::= OCTET STRING (SIZE (8))
```

ASN.1 is often paired with a language used convert the formal definitions into "bits and bytes". These languages are known as encoding rules. Five different encoding rules have been defined as international standards as listed below. The combination of the ASN.1 grammar and the specification of the encoding rule precisely specifies the "bits and bytes" of a protocol.

- BER (Basic Encoding Rules) was the first set of encoding rules defined. The purpose of BER is to provide a simple encoding of ASN.1 while providing self-description and optional extensions. Each object in ASN.1 is encoded on byte boundaries. BER provides multiple ways to encode the same content.
- PER (Packed Encoding Rules) was created as a means to reduce the bandwidth required for messages. It does this by discarding the concepts of self-description and byte-aligned data. PER provides a much more compact encoding than BER.
- DER (Distinguished Encoding Rules) is used in security-aware applications where the need for a unique encoding for a given set of data content.
- CER (Canonical Encoding Rules) is a rarely used rule set for encoding while it is being created.
- XER (XML Encoding Rules) allows ASN.1 content to be expressed in XML.

Application to utility systems: ASN.1 can define the syntax, semantics, and expression of the data communication. ASN.1 languages will likely be used for high-speed enterprise-level communications.

Strengths: ASN.1 allows clear definitions of the representational language which can be machine-interpreted. BER is widely used by Internet applications (such as SNMP) and IEC 61850-based applications. ASN.1/BER or ASN.1/CER self-description eases the task of integrating products. The usage of ASN.1 is generally hidden from users.

Concerns: ASN.1 is very bulky and difficult to learn. It requires a "compiler" with run-time libraries on the device it is implemented on.

Layers: Presentation, application and above. Also used in some lower layers.

References:

- http://asn1.elibel.tm.fr/en/introduction/index.htm - Tutorial
- http://www.oss.com/asn1/rules.html - Encoding Rules Tutorial
- http://www.iso.org – ISO
- http://www.itu.int/itu-t - ITU

IEC 61850-6 Substation Configuration Language (SCL)

SCL is used by IEC 61850-based system to describe the entire configuration of a substation. SCL uses XML for the configuration of electrical substation devices. The SCL language is designed to be extensible in the sense that it can be used in situations outside of the substation. Many parts of the SCL language use optional components which allow compact representation of simple configurations. SCL contains three parts: substation, communication, and product.

- The substation portion deals with the actual physical devices within the substation and the topology of the substation.
- The communication section describes the multitude of communication paths and redundancies of those paths.
- The product section describes the actual devices which communicate with the substation.

The communication and product portions of SCL are addressed by tools which provide the necessary configuration. The communication portion can be used to describe the detailed topology of the communication system at any level. For example, it could describe the connectivity of end devices to a feeder data concentrator and then describe concentration to a substation data concentrator. The product portion allows a clear description of the device itself. All services and object instances behind the device can be described in an unambiguous manner. The substation portion describes to topological aspects of the system in CIM-like terms.

Application to utility systems: SCL provides a method to produce machine-readable documentation describing both the communication paths and the actual information transfer.

Strengths: SCL allows clear definitions of the system topology at multiple levels and also defines data models of the devices.

Concerns: SCL as a whole is very difficult to learn. Software manipulation tools are required to perform configuration of the communications.

Layers: Application and above.

References:

- http://www.iec.ch - IEC

SOAP and Web Services

Web services are a generic term for protocols which communicate using Hyper Text Transport Protocol (HTTP – see above). The Simple Object Access Protocol (SOAP) is the protocol on which most web services are based. HTTP is

used as the transport mechanism for SOAP because it is included in almost every networked device.

HTTP defines only three commands: GET (retrieves a document from a server), HEAD (determine size of a document), and POST (send a document and retrieve the response). SOAP simply defines the message format used by the existing HTTP "POST" and HTTP "GET" commands as being XML content. The SOAP example below retrieves the "watt" data from a device. Prior to data exchange, both ends must agree on an XML schema to be used for the SOAP exchange.

```
GET /consumer.example.org/meteringData?code=watt  HTTP/1.1
Host: consumer.example.org
Accept: text/html;q=0.5, application/soap+xml
```

And the device response of:

```
HTTP/1.1 200 OK
Content-Type: application/soap+xml; charset="utf-8"
Content-Length: nnnn

<?xml version='1.0' ?>
<env:Envelope xmlns:env="http://www.w3.org/2003/05/soap-envelope">
 <env:Header>
  <m:metering xmlns:m="http://consumer.example.org/meteringData"
       env:role="http://www.w3.org/2003/05/soap-envelope/role/next"
           env:mustUnderstand="true">
   <m:reference>uuid:093a2da1-q345-739r-ba5d-
pqff98fe8j7d</m:reference>
   <m:dateAndTime>2001-11-30T16:25:00.000-05:00</m:dateAndTime>
  </m:metering>
 </env:Header>
 <env:Body>
  <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"
            xmlns:x="http://provider.example.org/vocab#"
     env:encodingStyle="http://www.w3.org/1999/02/22-rdf-syntax-ns#">
   <x:meteringData
 rdf:about="http://consumer.example.org/meteringData?code=watt">
      <x:watt>12345678</x:watt>
    </x:meteringData>
  </rdf:RDF>
 </env:Body>
</env:Envelope>
```

As shown above, web services require a substantial overhead for messages. The message also shows that the messages are completely encoded as text messages and are therefore very simple for human readers to understand.

Application to utility systems:

- Web services offer a simple method to leverage the existing HTTP capability already built into most network capable devices. Web services are extremely popular in the commercial computing environment and therefore may be often used in the back office devices that communicate with devices such as consumer portals. Their deployment in devices themselves will depend on

how cost-effectively the necessary processing power and bandwidth can be deployed to the customer site.

- When Web services are implemented with the other necessary applications and hardware platforms, secure remote enterprise wide access can be provided to select data and display for authorized staff. An example implementation could be a low cost substation user interface (permanent or staff laptop) displaying a single line and other data for that substation and any other substation on the system.

Strengths: Web services transparently transport data across any web-enabled communication system. The mechanism is inherently self-descriptive. Security is available through WS-Security or the Security Assertion Markup Language (SAML).

Concerns: Message overheads are very large.

Layers: Presentation, application and above.

References:

- http://www.w3.org/TR/soap - World-Wide Web Consortium SOAP page
- http://www.w3.org/TR/wsdl - World-Wide Web Consortium Web Services page
- http://www.oasis-open.org/specs/index.php - OASIS (see below) standards, including WS-Security and SAML.

ebXML

Electronic Business eXtensible Markup Language (ebXML) is a family of standards for the exchange of business messages over the internet. It is a true set of international standards (ISO/TS 15000-x). The standards stated intent is "enable anyone, anywhere to do business with anyone else over the Internet". It is based upon the concept that the each "actor" in a transaction maintains a registry (dictionary) of capabilities and the business scenario they support. The message exchange phase is very similar to that of SOAP. ebXML is developed and promoted by the Organization for the Advancement of Structured Information Standards (OASIS).

Application to utility systems: Directory-driven data exchange system allows dynamic discovery of services and objects behind the gateways and consumer portals.

Strengths: Built-in directory services.

Concerns: Directory services are bulky. Message overhead is very large.

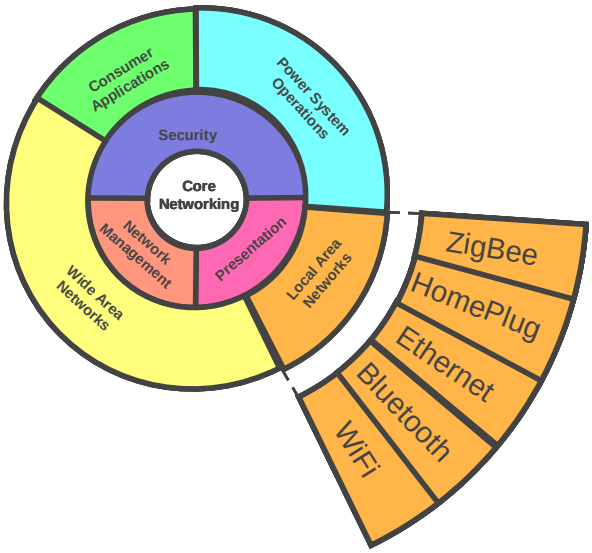
Layers: Presentation, application and above.

References:

- http://www.ebxml.org – OASIS ebXML site
- http://www.oasis-open.org/specs/index.php - OASIS standards list

Local Area Network Technologies

Local area networks provide connectivity for devices located in proximity to one another It is possible that a recommended architecture will not specify a particular LAN technology because one of the goals of the design will be independence from such technologies. However, LAN technologies are discussed as a guide for possible deployment as pilot projects.



Wired Ethernet (IEEE 802.3)

Ethernet is a LAN technology first developed by Xerox®, and refined by DEC and Intel (DIX). The Ethernet access mechanism is Collision Sense Multiple Access with Collision Detection (CSMA/CD). Ethernet was standardized by the IEEE in the IEEE 802.3 standard. Today the term Ethernet includes 10, 100 (Fast), 1000 (Gigabit) Mbps, 10GbE, 40 GbE, and 100 GbE Ethernet technologies. Ethernet is the most common LAN technology with 88% of the installed base and 98% of all new purchases being Ethernet. Ethernet is also now widely used as a WAN protocol.

Application to utility systems: An access mechanism for equipment at a utility or customer site to reach a WAN or other network. It could be used as a standardized "port" for network access. In addition, Ethernet is applicable to WAN throughout utility enterprise systems.

Strengths: Low cost, huge market support and a variety of available products.

Concerns: Most technologies are for local area network only.

Layers: Data Link, Physical

References:

- http://standards.ieee.org/getieee802/802.3.html - IEEE 802.3 page

Wireless IEEE 802.x

There are four main IEEE standards with applicability to AMI: IEEE 802.11 (Wi-Fi), commonly used for local area networks, IEEE 802.16 (WiMAX) an emerging standard for wider metropolitan networks, IEEE 802.15.1 (Bluetooth) for "personal area networks", and IEEE 802.15.4 (ZigBee), a new standard for small, low-cost networks of sensors and controls. All of them use the same Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) technology for accessing the media, and are therefore sometimes collectively known as "Wireless Ethernet". WiMAX is discussed below with other wide area network technologies. Note that all wireless technologies (those using CSMA techniques) are subject to Denial-Of-Service (DOS) attacks using simple "jamming" transmitters.

Wi-Fi

The IEEE 802.11 family of standards for wireless local area networks (LANs) supports a number of physical layers, but the most popular are 802.11a, 802.11b, 802.11g, and 802.11n which are collectively marketed as "Wireless Fidelity" or "Wi-Fi". The "b" and "g" variants are in widespread use providing Internet access points for personal computer users in small offices, cafés, airports, and other public places. IEEE 802.11a and 802.11b operate in the unlicensed 5.0 and 2.4GHz range have data rate of 55 and 11 Mbps respectively. 802.11n (MIMO) technology shows particular promise for high data rates in the face of multi-path interference. The Wireless Fidelity (Wi-Fi) Alliance promotes and certifies IEEE 802.11a, b, g, and n implementations.

Application to utility systems: Possible limited application within field installations to equipment monitoring devices. May also be used for access between wide-area networks and the field installations, particularly in the case of Access BPL (see below) to get around the problem of crossing the final distribution transformer.

Strengths: Easy to deploy, equipment costs dropping rapidly.

Concerns: IEEE 802.11 by itself is only useful within the customer site. It would be better to deploy it in conjunction with some other technology, such as WiMAX or Access BPL. Security is one of the major concerns of wireless LANs in general and of IEEE 802.11 in particular. Wi-Fi would require additional security layers in order to be used securely.

Layers: Data Link, Physical

References:

- http://www.wirelessethernet.org/OpenSection/index.asp - Wi-Fi Alliance
- http://standards.ieee.org/getieee802/802.11.html - IEEE 802.11 Standards

ZigBee

IEEE 802.15.4 (ZigBee) is a Home Area Network (HAN) technology intended to connect sensors, monitors and control devices using low data rates, low cost, and extremely low power consumption. ZigBee devices create a self-organizing mesh network that can be shared by industrial controls, medical devices, smoke and intruder alarms, building automation devices, and even toys.

ZigBee operates at much lower bit rates, and is intended to be much lower-cost, than similar technologies such as Bluetooth (IEEE 802.15.1). The network is designed to use very small amounts of power, so that individual devices might run for a year or two with a single alkaline battery. ZigBee operates in the unlicensed 2.4 GHz, 915MHz and 868MHz bands over up to 16 channels with maximum bit rates between 20Kbps and 250Kbps. ZigBee transmission range is between 10 and 75 meters. ZugBee provides security using 128-bit AES keys. ZigBee uses CMSA-CA methods like the rest of the IEEE 802 standards. ZigBee is promoted by the ZigBee Alliance.

Application to utility systems: Used by utilities for drive-by meter reading, user interface at customer site, connection of sensors and other equipment in a customer local area network.

Strengths: Low power requirements and implementation costs. It has a very active users' group. ZigBee is a good example of a successful standards effort that started small and simple. It is particularly designed for use home automation or security applications. Meters utilizing ZigBee protocol 1.0 have been deployed. .

Concerns: Limited range. ZigBee lacks upward or backwards compatibility between SEP versions 1.0 and 2.0. It has relatively low data rates, although likely to be sufficient for the type of devices that would implement it. There has been a concern about the need for more comprehensive documentation to ensure broad device interoperability however these concerns are now being addressed. Original ZigBee SEP 1.0 attempted to duplicate all 7 layers of the OSI stack, but SEP 2.0 has moved to less intertwined protocol layers.

Layers: Data Link, Application, Physical, Application

References:

- http://www.zigbee.org – ZigBee Alliance
- http://standards.ieee.org/getieee802/802.15.html - IEEE 802.15 page

Bluetooth

IEEE 802.15.1 (Bluetooth) is a specification for very short-range wireless local area networks, sometimes known as Personal Area Networks (PANs). It uses the 2.45GHz ISM (Industrial, Scientific, and Medical) band to provide a maximum data rate of 723kbps (for versions 1.1 and 1.2) or 2.1Mbps (for version 2.0, recently released). The name, "Bluetooth" refers to an early Danish king who united warring tribes of the Scandinavian countries.

Bluetooth is a short-range technology. There are three possible classes of Bluetooth with maximum ranges of 1 meter, 10 meters, or 100 meters respectively. Most available devices tend to be in the 10 meter class. Bluetooth is considered to be less expensive than WiFi to implement, but more costly than ZigBee, with corresponding differences in range and power.

Bluetooth is intended for use in consumer electronics. Typical applications of Bluetooth include wireless headsets for cellphones and car phones, wireless communication to peripherals, file sharing with music players and cameras, games between palmtop computers, and many others. Bluetooth devices form "piconets" of up to 8 devices with a single master. It has been said that if WiFi is wireless Ethernet, Bluetooth is the equivalent of wireless Universal Serial Bus (USB).

A key characteristic of Bluetooth is its ability to detect other nearby devices and exchange self-description data. A number of unusual social practices (and some hoaxes) have reportedly grown up around the fact that Bluetooth users can detect when another user is in the room and exchange information. Bluetooth was originally developed by Ericsson, but is now managed by the Bluetooth Special Interest Group, which provides certification testing.

Application to utility systems: Utility applications for Mobile workforce applications with feeder and substation IED maintenance (additional security applications required). Walk up IED configuration and maintenance for feeder devices (pole mounted etc). Also drive-by meter reading, user interface at customer site, connection of sensors and other equipment in a customer local area network.

Strengths: Bluetooth is somewhat more mature than ZigBee, with many products already available. It permits higher data rates. New 2.1Mbps version 2.0 available.

Concerns:

- Since Bluetooth has been so far used primarily as a consumer electronics technology, many of the utility and industrial devices that would be useful do not have Bluetooth implementations.
- Although Bluetooth piconets can in theory be linked together, it is rarely done, so the maximum number of devices in a network may be limited to 8.

- There have been a number of reported security vulnerabilities in the last year that might permit attackers to gain control of Bluetooth devices or listen to Bluetooth conversations. Most of the vulnerabilities seem to center around the self-description and authentication mechanism

Layers: Data Link, Physical

References:

- http://www.bluetooth.org – Bluetooth Special Interest Group
- http://www.bluetooth.com – Bluetooth Marketing site
- http://standards.ieee.org/getieee802/802.15.html - IEEE 802.15 page

In-Building Power-Line (BPL) Communications

See below for a general discussion of power line communications. Multiple power line technologies exist. The two most common technologies for use of PLC are within the customer premises: HomePlug and X10.

HomePlug

The HomePlug Powerline Alliance promotes a BPL system using the frequencies between 4.5 and 21 MHz inside the customer premises, at data rates up to 85 Mbps. It is a general-purpose LAN that uses a collision-sensing data link layer and provides an effective rate after compensating for interference of around 10-15Mbps. The HomePlug LAN very similar in characteristics to 10Mbps Ethernet. It operates over both 50Hz and 60Hz wiring.

HomePlug provides most of the features expected of a modern LAN technology. It uses a highly robust ODFM transmission system with automatic retries and forward error-correction, which is well-suited to provide reliable communications in noisy environments. HomePlug products are available for bridging directly to Ethernet or USB networks, providing a simple mechanism for interoperability and peer-to-peer operation. The specification incorporates Quality-of-Service (QoS) with four levels of priority ranging from "voice traffic" to "best effort". Encryption is available, although it uses 56-bit DES and therefore may only provide token resistance to a determined hacker.

The HomePlug specification is available to any member of the HomePlug Powerline Alliance, and products are available from several different vendors. Reference designs have been published for HomePlug routers, switches, and gateways. The HomePlug Alliance provides a certification program.

There are three different HomePlug specifications.

- HomePlug 1.0, discussed above, is a mature specification with products from multiple vendors currently on the market.

- HomePlug AV (audio-visual), was officially released in August 2005. Like HomePlug 1.0, it is a customer-premises LAN, but provides a maximum data rate of 200Mbps, with an effective rate after interference of about 50 Mbps, sufficient for transferring multiple high-definition video signals within the home. Products are expected by the end of 2005.
- HomePlug BPL is an effort by the HomePlug Powerline Alliance to develop an Access BPL technology (to be used from the utility to the consumer site). It has been standardized as IEEE P1901.

Application to utility systems: HomePlug 1.0 is well-suited for general communications between the portal and devices at the consumer site. The newer versions of HomePlug may make advanced portal applications possible, such as delivering entertainment.

Strengths: Every Portal device under consideration has some connectivity to the home wiring. HomePlug BPL can use the QoS features to guarantee timely delivery of commands and responses. HomePlug's standardization by IEEE should accelerate adoption of BPL applications.

Concerns: HomePlug 1.0 security may not be sufficient depending on the application. Presumably HomePlug AV will improve on the security level provided. Recent standardization of ITU G.hn (ITU G.9960) threatens to fragment the market for BPL solutions.

References:

- http://www.homeplug.org - HomePlug Powerline Alliance
- http://www.itu.int/ITU-T - ITU-T

X10

X10 is the earliest, and probably the most popular, power-line carrier system for home automation. It was developed in 1975 by Pico Electronics of Scotland as "experiment number 10" for British Sound Reproduction (BSR). Introduced in 1979 as "BSR System X10"and popularized through the Radio Shack chain of electronics stores, the X10 protocol remains in common use, with about a dozen manufacturers still producing devices.

The X10 protocol consists of 120kHz pulses transmitted at the zero-crossings of each phase, with two crossings (10 or 01) required to represent a single data bit. Allowing for a four-bit start sequence on each message, an eight-bit address consisting of a "letter code" and a "function code", and retransmitting every message for reliability, the system produces an effective bit rate of about 20 bits per second. X10 messages are very simple, consisting of commands like "on", "off", "dim" and "brighten". A great many home automation products have been built to the X-10 specification, from simple wall switches to sophisticated security system controllers. A wireless version of the protocol is available, operating at 310MHz in North America for products like keychain controllers. Versions of X10 operate on either 60Hz or 50Hz power networks.

Application to utility systems: A convenient mechanism for a portal to control load equipment (e.g. thermostats, pool pumps) and read simple sensors within a consumer site. It cannot be used as a general-purpose LAN for carrying other traffic, e.g. Internet Protocols.

Strengths: Very commonly used. A variety of equipment is available that is compatible with the protocol. It has an extremely low cost of implementation if the device already uses the power line.

Concerns:

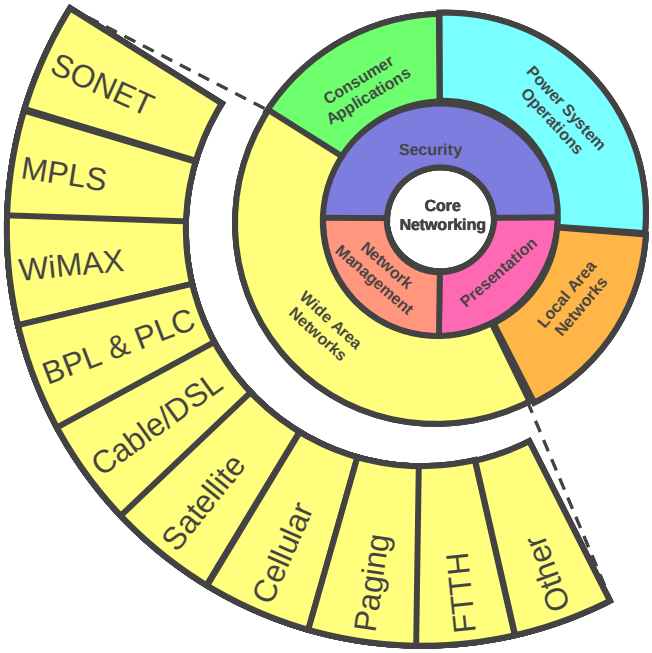
- Extremely low bandwidth and simple functionality.
- X10 is a de facto standard, not recognized by any standards body. The X10 specification is fairly easy to locate on the web, but the X10 company does not promote openness of the protocol. Although products are available from multiple vendors, many simply resell X10 company products or use their components. Various home automation web sites have a great deal of information on availability of X10 products and how to make them work, but cannot be considered users' groups for the protocol.

Layers: Application, Data Link, Physical

References:

- http://www.x10.com/home2.html - Official X10 Company Site
- http://www.smarthome.com/manuals/MAN-1136.pdf> - Early copy of the specification
- http://www.hometoys.com/htinews/feb99/articles/kingery/kingery13.htm - A tutorial on the specification

Wide Area Network (WAN) Technologies



As discussed in the technology assessment WANs are networks that are not co-located. The market for wide-area standards is very complex, and is further complicated by the intervention of governments who are attempting to foster competition.

Internet access is becoming ubiquitous for both businesses and consumers alike. Utility connected systems and devices, although they will not necessarily communicate over the Internet, will most likely use Internet protocols (IP) for some communication networks. Security is, and will to be, vital for any IP network. Today the most widely used WAN technology is Ethernet which is discussed in the earlier LAN technology section.

ATM

Asynchronous Transfer Mode (ATM) is a digital communications protocol that is used for the transport of voice, video, data, and images. ATM is an ITU-T standard for the transfer of small fixed size packets called cells. ATM is the world's most widely deployed backbone technology. ATM has been widely adopted because of its flexibility in supporting the broadest array of technologies, including DSL, IP Ethernet, Frame Relay, SONET (Synchronous Optical Networking)/SDH and wireless platforms.

ATM is a cell-switching and multiplexing technology that combines the benefits of circuit switching (guaranteed capacity and constant transmission delay) with those of packet switching (flexibility and efficiency for intermittent traffic). It provides scalable bandwidth from a few megabits per second (Mbps) to many gigabits per second (Gbps). ATM can be used both for WANs and LANs and is

capable of very high speeds (currently up to 40 Gbps using SONET/OC-768). Because of its asynchronous nature, ATM is more efficient than synchronous technologies, such as time-division multiplexing (TDM).

ATM is a network and data link layer protocol which encodes data traffic into small (53 bytes; 48 bytes of data and 5 bytes of header information) fixed-sized cells. ATM provides data link layer services that run over SONET Layer 1 links. ATM differs from other technologies based on packet-switched networks (such as the Internet Protocol or Ethernet), in which variable sized packets (sometimes known as frames) are used. ATM is a connection-oriented technology, in which a logical connection is established between the two endpoints before the actual data exchange begins.

By contrast with SONET, ATM puts data on the system as it arrives in private packets. Channels are re-constructed from packets as they come through. It is more efficient as there are no null packets sent, but has the overhead of prioritizing packets and sorting them. Each system has different system management options for coping with problems.

ATM itself consists of a series of layers. The first layer - known as the Application Adaptation Layer (AAL) - holds the bulk of the data transmission. The 48-byte payload divides the data into different types. The ATM layer contains five bytes of additional header information, referred to as overhead. Lastly, the physical layer attaches the electrical elements and network interfaces.

Application to utility systems: IntelliGrid core technology for WAN backbone communications**.**

Strengths: ATM is one of the world's most widely deployed backbone technology. ATM has been widely adopted because of its flexibility in supporting the broadest array of technologies, including DSL, IP Ethernet, Frame Relay, SONET (Synchronous Optical Networking) /SDH and wireless platforms. ATM can be used both for WANs and LANs and is capable of very high speeds (currently up to 40 Gbps using SONET/OC-768).

Concerns: The most significant concerns regarding ATM are the incompatibilities with IP that require complex adaptation making it largely unsuitable in today's predominantly IP networks. In addition Packets must be segmented, transported and re-assembled over an ATM network using an adaption layer, which adds significant complexity and overhead to the data stream. MPLS, on the other hand, simply adds a label to the head of each packet and transmits it on the network. MPLS dispenses also with the cell-switching and signaling-protocol baggage of ATM. ATM cells are no longer needed in the core of modern networks, since modern optical networks (as of 2001) are so fast (at 10 Gbit/s and well beyond) that even full-length 1500 byte packets do not incur significant real-time queuing delays (the need to reduce such delays, to support voice traffic, having been the motivation for the cell nature of ATM). Thus ATM is a protocol that is rarely chosen today for new equipment today.

Layers: Data link layer, physical

References:

- http://www.mfaforum.org/index.shtml

MPLS

Multi Protocol Label Switching (MPLS) is a data-carrying mechanism that belongs to the family of packet-switched networks. MPLS operates at an OSI Model layer that is generally considered to lie between traditional definitions of Layer 2 (data link layer) and Layer 3 (network layer), and thus is often referred to as a "Layer 2.5" protocol. It was designed to provide a unified data-carrying service for both circuit-based clients and packet-switching clients which provide a datagram service model. It can be used to carry many different kinds of traffic, including IP packets, as well as native ATM, SONET, and Ethernet frames. At the same time, it attempts to preserve the traffic engineering and out-of-band control that made frame relay and ATM attractive for deploying large-scale networks.

A number of different technologies were previously deployed with essentially identical goals, such as frame relay and ATM. MPLS is now replacing these technologies in the marketplace, mostly because it is better aligned with current and future technology needs.

In particular, MPLS dispenses with the cell-switching and signaling-protocol baggage of ATM. MPLS recognizes that small ATM cells are not needed in the core of modern networks, since modern optical networks (as of 2001) are so fast (at 10 Gbit/s and well beyond) that even full-length 1500 byte packets do not incur significant real-time queuing delays (the need to reduce such delays, to support voice traffic, having been the motivation for the cell nature of ATM). In addition MPLS is able to work with variable length packets while ATM transports fixed-length (53 byte) cells. Packets must be segmented, transported and re-assembled over an ATM network using an adaption layer, which adds significant complexity and overhead to the data stream. MPLS, on the other hand, simply adds a label to the head of each packet and transmits it on the network.

MPLS was originally proposed by a group of engineers from Ipsilon Networks, but their "IP Switching" technology, which was defined only to work over ATM, did not achieve market dominance. Cisco Systems, Inc. introduced a related proposal, not restricted to ATM transmission, called "Tag Switching" when it was a Cisco proprietary proposal, and was renamed "Label Switching" when it was handed over to the IETF for open standardization. The IETF work involved proposals from other vendors, and development of a consensus protocol that combined features from several vendors' work.

One original motivation was to allow the creation of simple high-speed switches, since for a significant length of time it was impossible to forward

IP packets entirely in hardware. However, advances in VLSI have made such devices possible. Therefore the advantages of MPLS primarily revolve around the ability to support multiple service models and perform traffic management. MPLS also offers a robust recovery framework[1] that goes beyond the simple protection rings of synchronous optical networking (SONET/SDH).

Of particular interest for applications is MPLS VPN which is a family of methods for harnessing the power of Multiprotocol Label Switching (MPLS) to create Virtual Private Networks (VPNs). MPLS is well suited to the task as it provides traffic isolation and differentiation without substantial overhead. Three methods are described below

Layer 3 MPLS VPN

A layer 3 MPLS VPN, also known as L3VPN, combines enhanced BGP signaling, MPLS traffic isolation and router support for VRFs (Virtual Routing/Forwarding) to create a virtual network.

The MPLS solution is more scalable and less costly than classic provider-based frame relay or ATM-based networks, or IPsec-based VPNs. Layer 3 MPLS VPNs also support Quality of Service.

Layer 2 MPLS VPN

A layer 2 MPLS VPN, also known as L2VPN, is a point-to-point pseudowire service. It can be used to replace existing physical links. The specification is based on the Martini drafts, which define methods to transport layer 2 packets across MPLS networks, and methods to encapsulate transport protocols such as ATM, Ethernet, and SONET. The primary advantage of this MPLS VPN type is that it can transparently replace an existing dedicated facility without reconfiguration, and that it is completely agnostic to upper-layer protocols. By contrast, in a layer 3 VPN the hosts must speak IP.

Multipoint Layer 2 MPLS VPN

A Multipoint layer 2 VPN for Ethernet, can be implemented using Virtual Private LAN Service (VPLS) and MPLS pseudo wires (ATOM). It builds on the foundation of point-to-point layer 2 MPLS VPNs to extend an Ethernet broadcast domain across multiple sites. The VPLS network appears as a private Ethernet switch to the attached MPLS end site.

Application to utility systems: IntelliGrid core technology for WAN backbone communications.

Strengths: The biggest single advantage that MPLS has over ATM is that it was designed from the start to be complementary to IP. Modern routers are able to support both MPLS and IP natively across a common interface allowing network

operators great flexibility in network design and operation. Importantly MPLS supports Quality of Service (QoS) requirements by changing the hop-by-hop paradigm with the enabling of devices to specify paths in the network based upon QoS and bandwidth needs of the applications. In other words, path selection can now take into account Layer 2 attributes. In addition MPLS is able to work with variable length packets while ATM transports fixed-length (53 byte) cells. Packets must be segmented, transported and re-assembled over an ATM network using an adaption layer, which adds significant complexity and overhead to the data stream. MPLS, on the other hand, simply adds a label to the head of each packet and transmits it on the network.

Concerns: While the traffic management benefits of migrating to MPLS are quite valuable (better reliability, increased performance), there is a significant loss of visibility and access into the MPLS cloud for IT departments.

Layers: Network, Data Link, Physical

References:

- http://www.ietf.org/html.charters/mpls-charter.html
- http://www.ietf.org/rfc/rfc2702.txt
- http://www.mplsrc.com/
- http://www.mfaforum.org/index.shtml

Frame Relay

Frame relay is a widely used, mature packet technology used mainly for wide-area network (WAN) services. Frame relay provides connection-oriented, data link layer communication with the addition of packet relaying, based on the assumption of low noise links and high-speed processors.

The designers of frame relay aimed at a telecommunication service for cost-efficient data transmission for intermittent traffic between local area networks (LANs) and between end-points in a wide area network (WAN). Frame relay puts data in variable-size units called "frames" and leaves any necessary error-correction (such as re-transmission of data) up to the end-points. Thus frame relay results in very high speed data transmission. For most services, the network provides a permanent virtual circuit (PVC), which means that the customer sees a continuous, dedicated connection without having to pay for a full-time leased line, while the service-provider figures out the route each frame travels to its destination and can charge based on usage.

An enterprise can select a level of service quality - prioritizing some frames and making others less important. Frame relay can run on fractional T-1 or full T-carrier system carriers. Frame relay complements and provides a mid-range service between ISDN, which offers bandwidth at 128 kbit/s, and Asynchronous

Transfer Mode (ATM), which operates in somewhat similar fashion to frame relay but at speeds from 155.520 Mbit/s to 622.080 Mbit/s.

Frame relay has its technical base in the older X.25 packet-switching technology, designed for transmitting analog data such as voice conversations. Unlike X.25, whose designers expected analog signals, frame relay offers a fast packet technology, which means that the protocol does not attempt to correct errors. When a frame relay network detects an error in a frame, it simply drops that frame. The end points have the responsibility for detecting and retransmitting dropped frames. (However, digital networks offer an incidence of error extraordinarily small relative to that of analog networks.)

Frame relay often serves to connect local area networks (LANs) with major backbones as well as on public wide-area networks (WANs) and also in private network environments with leased lines over T-1 lines. It requires a dedicated connection during the transmission period. Frame relay does not provide an ideal path for voice or video transmission, both of which require a steady flow of transmissions. However, under certain circumstances, voice and video transmission do use frame relay.

Frame relay relays packets at the data link layer (layer 2) of the Open Systems Interconnection (OSI) model rather than at the network layer (layer 3). A frame can incorporate packets from different protocols such as Ethernet and X.25. It varies in size up to a thousand bytes or more.

Frame Relay originated as an extension of Integrated Services Digital Network (ISDN). Its designers aimed to enable a packet-switched network to transport the circuit-switched technology. The technology has become a stand-alone and cost-effective means of creating a WAN. Frame Relay switches create virtual circuits to connect remote LANs to a WAN. The Frame Relay network exists between a LAN border device or frame relay access device (FRAD) and the carrier switch. The technology used by the carrier to transport the data between the switches is variable and changes between carrier (i.e. Frame Relay does not rely directly on the transportation mechanism to function.)

The Frame Relay Forum is an association that promotes the development and use of the technology. Frame relay was developed as a part of the Integrated Services Digital Network (ISDN) framework, and is specified in many X-series ITU-T standards. Parts are also specified in ITU I.122 and Q.922.

Application to utility systems: Core technology for WAN backbone communications. Appropriate for all data where error rates and variable data latencies are compatible with the application requirements. Limitations may render frame relay inappropriate for phasor measurement data and streaming video/voice data.

Strengths: Frame Relay has become one of the most extensively-used WAN protocols. Frame Relay Provides uses one or more PVCs (permanent virtual channels) for continuous stand alone connections at each site. The extreme

simplicity of configuring user equipment in a Frame Relay network offers another reason for Frame Relay's popularity. Fewer network delays versus X.25. Bandwidth can be highly scalable depending the on the service agreement with the telco. Usually quite economical compared to multiple leased and PSTN lines with charges based on usage.

Concerns: The sophistication of the technology requires a thorough understanding of the terms used to describe how Frame Relay works. Without a firm understanding of Frame Relay, it is difficult to troubleshoot its performance. No guaranteed data integrity (error detection). Messages (frames) are routed by the telco's network management services normally involving many "hops" making message latency highly non-deterministic. Not well suited for voice and video data transmission. As with ATM,

Layers: Data Link, Physical

References:

- http://www.mfaforum.org/index.shtml
- http://www.frforum.com/

WiMAX

IEEE 802.16 (WiMAX) is a wireless metropolitan area network (MAN) technology that provides wireless coverage for last mile (last km) broadband access. Like WiFi, WiMAX is a wireless technology defined in the IEEE 802.11 standard. WiMAX uses frequencies in the 2-11GHz and 10-66GHz ranges; the former is restricted to line-of-sight communications but the latter is not. The intended deployment of WiMAX is in networks with a wide coverage pattern similar to cellular telephony, in multiply linked "hotspots" as Wi-Fi is now used. Currently WiMax delivers up to 40Mbps per channel in typical cells of radius 3 to 10 kilometers without direct line-of-sight to a base station. WiMAX's maximum range is 50km line-of-sight, but it operates at a much lower bitrate at longer distances.

Application to utility systems: Wide area network to connect field installations. It could be used in conjunction with other "last mile" technologies such as WiFi.

Strengths: Does not require deployment of a costly wired infrastructure. Cellular providers are offering proprietary technologies with similar capabilities, and WiMAX is losing market share to competing technologies including LTE.

Concerns: Market deployment of IEEE 802.16 was increasing with deployments of G4 networks.

Layers: Data Link, Physical

References:

- http://www.wimaxforum.org/home - WiMAX Forum

- http://standards.ieee.org/getieee802/802.16.html - IEEE 802.16 page.

Digital Subscriber Line (DSL)

Asymmetric Digital Subscriber Line (ADSL) is the formal name for what is being commonly called Digital Subscriber Line (DSL). Its most common use is to connect residential telephone customers to the Internet. ADSL converts existing twisted-pair telephone lines into access paths for Plain Old Telephone System (POTS) voice telephone circuits plus simultaneous high speed data communications. ADSL transmits two separate data streams with much more bandwidth devoted to the downstream than upstream leg. ADSL has a range of downstream speeds depending on distance. For up to 9000, 12000, 16000, 18000 feet, the speed is 8.448, 6.312(DS2), 2.048(E1), and 1.544 (T1) Mbps respectively. The upstream speeds range from 16 kbps to 640 kbps. Products with downstream rates up to 8 Mbps and duplex rates up to 640 kbps are available today.

ADSL is most commonly used to carry IP-based protocols, but also supports ATM. ADSL is officially ITU-T standard G.992.1.

Application to utility systems: Wide-area access between the utility and customer site.

Strengths: Available to most urban homes through telephone lines. Available bandwidth is consistent regardless of number of subscribers and time of use.

Concerns: Available bandwidth decreases with distance.

Layers: Data Link, Physical

References:

- http://www.dslforum.org/
- http://www.itu.int/publications/index.html

Cable Modem

The CableLabs Cable Modem project, also known as Data Over Cable Service Interface Specification (DOCSIS), defines standard interface requirements for cable modems providing high-speed data distribution over cable television networks. CableLabs provides services to certify devices to this specification. The DOCSIS specification has been internationally standardized as ITU-T J.112. In Europe, both J.112 and a competing standard called EuroModem are used. The CableHome project has developed interface specifications to extend cable-based services to IP network devices within the home. The CableHome project builds on the DOCSIS connectivity specification to address issues such as device interoperability, user convenience, Quality of Service, and network management.

Application to utility systems: Access between the utility and customer site, and also network management within the customer site.

Strengths: Wide bandwidth, strong market penetration. CableLabs claims 33.5 million households in the U.S.A. had broadband service at the end of 2004, of which cable had 58.6 percent of the market. Development of the DOCSIS standards has reduced the price of cable modems considerably.

Concerns: Inconsistency of bandwidth depending on time of day and number of customers on a link.

Layers: Application, Transport, Network, Data Link, Physical

References:

- http://www.cablemodem.com

Power Line Communication

Power Line Communication (PLC), originally called Power Line Carrier, is the transfer of data by modulating the standard 50 or 60 Hz alternating current on the existing electric power lines. This section describes the characteristics of several types of PLC and their applicability to support future systems and in particular consumer portals.

Broadband over Power Line (BPL)

When power lines are used to carry a high-bandwidth data signal, power line communication is known as Broadband over Power Line, or BPL. There is some debate over the definition of "broadband", but the U.S. Federal Communications Commission (FCC) definition of 200 Mbps in each direction per customer site is generally accepted as an absolute minimum. In a notice released in October 2004, the FCC divides power line communication into three groups for the purposes of regulation. Systems that radiate frequencies from 1.7MHz to 80 MHz are considered to be BPL, while systems radiating below 1.7MHz are simply known as PLC and are covered by previous regulations.

The FCC further divides BPL into two categories:

- BPL used for access to and from customer sites, known as Access BPL (discussed below).
- BPL used within a customer site, known as In-Home (or In-Building) BPL. The primary candidate for In-Building BPL is the recently-released HomePlug BPL standard.

Access BPL

Deployment of BPL has met with resistance in North America for two reasons:

- **Transformers.** In Access BPL, the broadband signal must bypass the final step-down transformer from the utility to the customer. In North America this means high equipment costs because there are at most a few customers connected to a given transformer. Some vendors are attempting to address this limitation by combining BPL with Wi-Fi.
- **Interference.** Several lobby groups maintain that BPL causes too much electromagnetic interference, particularly in the shortwave bands used by amateur radio operators, emergency services, aircraft and maritime radios.

The FCC remains convinced that electromagnetic interference from BPL can be successfully mitigated by moving antennas, reserving certain geographic areas, or "notching" the BPL spectrum to not use particular frequencies in certain locations. In their October 2004 Report and Order, they now require BPL vendors to:

- Certify the emission levels of their equipment
- Support notching
- Provide government organizations of notice in advance of any deployments.

The FCC also relaxed some of the testing requirements and emissions on BPL. This ruling is far short of the ban on BPL that the anti-BPL lobby was hoping for, and they have announced intentions to challenge it. However, the text of the FCC order repeatedly states that the benefits of BPL (namely, a competitive broadband alternative to DSL and Cable) deployment outweigh the risks, and it is unlikely the appeal will be successful. Several North American jurisdictions, including Ontario and Texas, are in the process of passing regulations that encourage BPL.

In Europe, BPL is known as Power Line Telecommunications (PLT). PLT is much more widely accepted in Europe than in North America because a single transformer often supplies a hundred or more homes. The European Commission has issued a recommendation that regulators remove "any unjustified regulatory obstacles," to the deployment of BPL. The European Telecommunications Standards Institute (ETSI) is developing a standard able to provide up to 2.7Mbps on a carrier between 1.6 MHz and 30MHz. The IEEE has also begun work on a BPL standard.

In the meantime, there are several different groups in both Europe and North America dedicated to the promotion of BPL, to the point where it is very difficult to determine their different roles. Some of these are listed in the "references" section below.

Application to utility systems: Wide-area network access for field installations. Potential for utilities to charge for non-energy services such as Internet service provision and related offerings. The BPL terminal is a good candidate for the physical site of a consumer portal.

Strengths: There is existing wired infrastructure to nearly every home. This is a particularly strong advantage over Cable and DSL in rural areas.

Concerns:

- Cost of deployment is a major barrier in North America. It is likely that WiMAX deployment will outstrip BPL in North America for this reason, unless regulators create particularly favorable economic conditions for BPL.
- BPL is not suited for providing some portal applications because it is dependent on current existing on the power line. Automatic meter reading and demand response, for example, could work over BPL because the portal could buffer data until power was restored. However, many advanced distribution functions could not be implemented because the communications system would be lost during an outage.
- Most North American BPL implementations are proprietary, although they may provide standardized interfaces, such as IP/Ethernet and WiFi, at the edges of the network.

Layers: Data Link, Physical, some discussion of Network and Application

References:

- http://www.plcforum.com/ PLC Forum
- http://www.uplc.utc.org/ United Power Line Council
- http://www.bplia.org/ Broadband over Powerlines Industry Association
- http://www.upaplc.org/ Universal Powerline Association
- http://www.etsi.org/plt/ ETSI Power Line Telecommunications Standard
- http://grouper.ieee.org/groups/bop/ IEEE Working Group for Broadband Over Powerline

Narrowband PLC

Use of narrowband PLC for access between the utility and the customer site has been greater in Europe than in North America because of the higher number of customers connected to each low-voltage transformer. Therefore, the international standards for customer access via narrowband PLC are mostly European-based. The most popular narrowband PLC systems in North America are used within the customer site and are discussed in this chapter. The standard for narrowband PLC in the utility industry is IEC 61334-5.

1. The regulatory environment for narrowband PLC differs considerably between Europe and North America, as shown in **Error! Reference source not found.**. While the FCC permits use of any frequency below 540kHz,

CENELEC defines five different bands ranging up to 148.5kHz. Each of the individual bands have restrictions on their use. The one range permitted to energy providers (as opposed to their customers) is the "A" band from 9-95kHz.

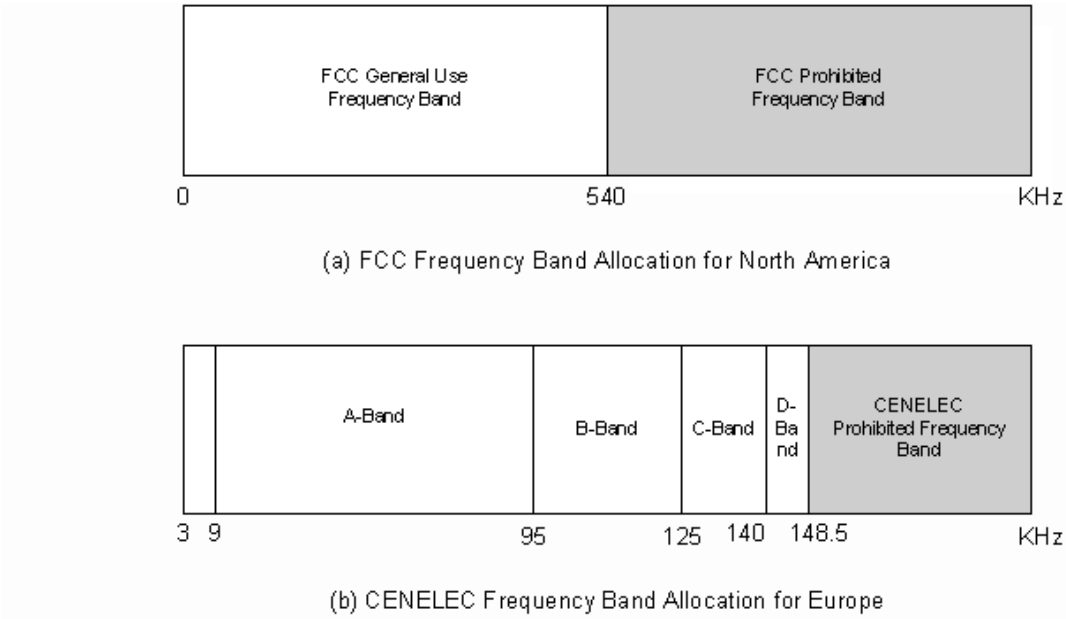


Figure B-5
Frequency Allocation for Narrowband PLC

IEC 61334-5 PLC

The IEC 61334-5 series of PLC standards define reliable mechanisms for the transmission of data on a medium voltage or low voltage transmission or distribution system. Each of the standards in the series use different modulation schemes.

- IEC 61334-5-1 transmits binary symbols using widely-spaced frequency shift keying (termed S-FSK). Two carriers are used to send the same information, one for the "mark" signal and one for the "space" signal. The receivers choose to use either or both carriers depending upon the noise characteristics of the line at the moment of reception.
- IEC 61334-5-2 transmits data using standard frequency-shift keying (FSK).
- IEC 61334-5-3 transmits using a spread-spectrum adaptive waveband (SS-AW) technique.
- IEC 61334-5-4 transmits data using Orthogonal Frequency Division Multiplexing (OFDM) similar to that used in ADSL systems.
- IEC 61334-5-5 transmits using spread-spectrum fast frequency-hopping (SS-FH). It sends M-bit symbols using 2^M sequential carrier bursts. This standard provides higher immunity to moving narrow-band noise than 61334-1.

IEC 61334-5-1 in particular has been widely deployed by utilities in France, Sweden and Norway, as part of the Power Line Automation Network (PLAN) along with some of the IEC 61334-4 standards that led to DLMS.

Application to utility systems: Access between the utility and customer site, or to equipment within the customer site. Typically used with a data concentrator at the medium-to-low-voltage substation. The data concentrator could be a potential location for the consumer portal functionality.

Strengths: Field-proven in Europe.

Concerns: Costly to implement in North American systems because of the need to bridge distribution transformers. There is currently no user's group particularly defined for this suite of protocols.

Layers: Data Link, Physical. IEC 61334-5 provides the media access control (MAC) portion of the Data Link layer and is usually used with IEC 61334-4-32 logical link control sub-layer.

References:

- http://www.iec.ch - IEC

Paging Systems

Paging networks are radio systems for delivering short messages from the telephone system or Internet to (and sometimes from) small remote, mobile terminals. Paging systems use a variety of technologies including microwave and satellite.

Like cellular systems, virtually all of the paging networks use more than one transmitter. Unlike cellular systems, they usually rely on simulcast capability to blanket an area. Several transmitters must send the same message over a wide area using the same frequency. A system controller applies sophisticated scheduling algorithms to manage the frequency spectrum used by the system.

Some paging standards exist, such as POCSAG, or ERMES in Europe, but many systems remain either proprietary or licensed. Fortunately, paging systems typically provide a variety of open standard gateways in and out of the system, including direct serial, dial-up, and email.

Paging systems are generally highly reliable, although satellite-based systems may be vulnerable to solar storms.

Application to utility systems: One-way systems can provide control messages to many different devices such as capacitor banks and customer site equipment, or notifications of emergencies. A portal could use two-way systems to report simple but important events for customer sites such as trouble calls, outage detection, or tampering.

Strengths: Ubiquity, reliability, low cost.

Concerns: One way communications poses serious limitations in certain applications where feedback on successful operation is important. Low bandwidth may not be suitable for downloading new applications or tariffs to customer equipment, or for customer interface other than simple emergency notifications. Although currently widespread, paging system use is on the decline and could soon be replaced by other technologies such as cellular.

Layers: Data Link, Network, Transport, Application, Physical

References:

- http://www.refreq.com/braddye/pager.html

Satellite Services

Satellite communication technology presents many interesting opportunities and challenges for connectivity to consumer locations. The main advantage of the technology is that a data connection can be established regardless of a lack of complete terrestrial infrastructure.

Satellite service can be best considered as a very long line-of-sight radio system. In this light, the challenges of the media become clear. These challenges are high-cost, low reliability during inclement weather, latency, security, and a lack of redundancy.

The cost of satellite service depends upon the system needs. Some services, such as broadcast video service, can be very inexpensive. However, the portal services will be required to use two-way (non-broadcast) service. This type of service uses a shared communication channel (transponder) which is very expensive. Various mechanisms are available to reduce the effective costs, but these all involve a delay in the access to the channel by fractions of a second. If there is no need for real-time data transfer, this will not present a problem.

Satellite service operates at the extreme limits of power levels. The transmitted power of the satellite is limited by the collection area of its solar cells while the received power is attenuated by the shear distance (more than 30 000 kilometers) of the receiver. The communication link has very little additional power beyond the absolute minimum. If weather conditions cause additional attenuation, the link can become unusable for a matter of minutes. Care must be taken to ensure that these random data dropout cannot cause operational problems.

The extreme path length of satellite channels causes high transmission latencies. If each data packet requires an acknowledgement, then the data packet and acknowledgment together require four traversals of the satellite-to-earth distance or about 500 milliseconds. For 1000 bytes packets, this translates into a data rate of only 2000 bytes per second. Usage of satellite technology requires mitigation through clever means.

Satellite data transmission is inherently insecure because it uses both public airwaves and insecure Network Operation Center (NOC) equipment. Only encrypted data must be allowed to pass through the satellite data system.

Satellite systems are mainly deployed in remote areas. Equipment failures can lead to long-term data loss unless some type of redundancy is employed. Users of satellite systems have very little hope for redundancy except by replication of entire data paths.

Application to utility systems: Limited applicability as a technology except for accessing very hard-to-reach customer sites. The high cost of the service will typically prove to be greater than any benefit for most sites.

Strengths: Universally available, regardless of the physical location.

Concerns:

- High cost will limit applicability to sites with unusual requirements.
- Low effective bandwidth due to high latency.
- Requires additional security to meet privacy requirements.

Layers: Network, Data Link, Physical

References:

- http://www.skycasters.com/broadband-satellite-internet-how-it-works/index.html

Cellular Services 3G, 4G and LTE

Cellular data service is ubiquitous in many parts of the world. It is tempting to use this service to obtain device and portal connectivity. Two basic types of cellular services are available:

- Circuit-switched Cellular Data (CSD) – guaranteed, slow data rate
- Packet-Switched Cellular Data – best effort, fast data rate

Circuit-switched Cellular Data service is used in exactly the same fashion as a dial-up data Modem. Upon connection establishment, there is a guaranteed channel of up to 14.4K bps which persists until the connection is closed. The per-minute cost for this service is generally the same as the cost of voice-only service. Examples of circuit-switched service are GSM (Global System for Mobile communication) and older CDMA (Code Division Multiple Access). These are the same services used for cellular voice systems. This is generally most suitable when an existing analog modem application needs to be migrated to a wireless solution.

Packet-Switched Cellular Data service converts the byte data stream into a stream of packets for delivery by the network. Each packet is individually routed by the network and then re-assembled at the receiving end. Use of Internet Protocol (IP) over such networks is very common.

Packet switching uses the network more efficiently and thus allows much higher data rates, and potentially lower costs.

Cellular communications technologies are rapidly evolving and third generation (3G) and fourth generation (4G) implementations are now common. For 3G and 4G systems, cellular providers have narrowed down to two competing systems:

- *CDMA2000* evolved out of the earlier CDMA service that was also known as IS-95. Its second-generation data service is called 1xRTT (Radio Transmission Technology) and has two third-generation technologies, 1xEV-DO (Evolution Data Optimized) and 1xEV-DV (Evolution Data and Voice). CDMA2000 is primarily deployed in North America and Japan, although it has some support elsewhere.
- *Universal Mobile Telecommunications System (UMTS)* is also known as 3GSM indicating that it has evolved from GSM technology. Many people are familiar with the second-generation packet-switched data services in GSM called General Packet Radio Service (GPRS). The third generation is based on Wideband CDMA, or W-CDMA, which is completely different from the earlier IS-95 CDMA. GSM is the most widely deployed cellular service in the world, and most GSM carriers have plans to eventually migrate to UMTS.

Long Term Evolution (LTE) is the next step in cellular technology and it provides support for GSM/UMTS with CDMA venders agreeing to switch to LTE. Thus LTE may become the first global cellular standard. In the interim, cell phones typically include multiple radios to support the different cellular bandwidths.

There are a variety of data rates available, but in general second-generation cellular packet systems provide data rates in the high tens or low hundreds of kilobits per second, while 3G systems operate around two or three megabits per second and 4G systems operate around 4 to 11 megabits per second. The LTE standard specifies download rates of 300 megabits per second and uplink data rates of 75 megabits per second.

Application to utility systems: Useful for wide-area access to sites that are too remote for utility data connection and yet still served by cellular telephony. A few smart meters now feature cellular communications and cellular companies are offering data plans for meters for $0.50 to $1.00 per meter per month.

Strengths: Huge coverage area, potential for low cost. Circuit-switched Cellular Data has previously had higher availability; Packet-Switched Cellular Data has lower cost and much higher data rates.

Concerns:

- Because of the speed at which cellular technology and markets are evolving, utilities should be careful that selection of a cellular system does not "lock them in" to using a particular provider. It is recommended that utilities verify with the cellular provider that communications equipment built for use with one provider also works with others.
- Some packet-switched networks are not very reliable and require robust transport layer protocols. A few providers are trying to address this vulnerability by building in redundancy.
- Confidentiality might be compromised by the network in circuit-switched systems unless higher-layer encryption is used.
- Packet-switched services are not available in all areas served by cellular voice service.
- Some technologies may not permit unsolicited transmission of data without first having a connection initiated by the network; might be a problem for outage detection, for instance.

Layers: Network, Data Link, Physical

References:

- http://en.wikipedia.org/wiki/Universal_Mobile_Telecommunications_System - UMTS
- http://en.wikipedia.org/wiki/Cdma2000 - Description of CDMA2000

SONET/SDH

Several types of communication protocols are used with fiber optic systems. Two of the most common are Synchronous Optical Networks (SONET/SDH) and Asynchronous Transfer Mode (ATM). SONET systems are channel oriented, where each channel has a time slot whether it is needed or not. If there is no data for a particular channel at a particular time, the system just stuffs in a null packet.

Synchronous optical networks are well established in electrical utilities throughout the world and are available under two similar standards: 1) SONET (Synchronous Optical Networks) is the American System under ANSI T1.105 and Bellcore GR Standards; 2) SDH (Synchronous Digital Hierarchy) under the International Telecommunications Union (ITU) Standards.

The transmission rates of SONET systems are defined as OCx (Optical Carrier x, x = 1…192); with OC1 = 51.84 Mbps and OC192 = 39.8 Gbps. Available in the market and specially designed to meet the electrical utility environment are SONET systems with bit rates of OC1 = 51.8 Mbps and OC3 = 155 Mbps.

SONET and SDH networks are based on a ring topology. This topology is a bi-directional ring with each node capable of sending data either direction; data can

travel either direction around the ring to connect any two nodes. If the ring is broken at any point, the nodes detect where the break is relative to the other nodes and automatically reverse transmission direction if necessary. A typical network, however, may consist of a mix of tree, ring, and mesh topologies rather than strictly rings with only the main backbone being rings.

Self healing (or survivability) capability is a distinctive feature of SONET/SDH networks made possible because it is ring topology. This means that if communication between two nodes is lost, the traffic among them switches over to the protected path of the ring. This switching to the protected path is made as fast as 4 ms, perfectly acceptable to any wide area protection and control.

The set of next generation SONET/SDH protocols to enable Ethernet transport is referred to as Ethernet over SONET/SDH (EoS).

Application to utility systems: . In the future, highly reliable wide area networks between field installations that provide high bandwidth, high determinism and low latency.

Strengths: Supports peer to peer messaging such as IEC GOOSE between substations and field installations within specific time requirements. SONET is inherently more secure than shared IP networks as it is normally installed as a closed utility network. Technology is mature and widely deployed. Supports a simple ring topology with built in path protection.

Concerns: Cost is higher for SONET vs other options. Technology is less efficient at handling IP traffic and mesh topologies. Bandwidth provisioning is fixed.

Layers: Physical

References:

- http://www.sonet.com/

Fiber to the Home (FTTH)

"Fiber to the Home (FTTH)" or "Fiber to the Premises (FTTP)", are the common terms for a number of different technologies that provide a broadband fiber-optic connection to consumer sites. FTTH has been the "holy grail" of the telecommunications industry for decades now, promising nearly unlimited bandwidth to the home user. However, until recently the costs of installing that much fiber optic cable and the associated electronics have been prohibitive.

Increases in the cost-effectiveness of electronics have helped, but the key enabler of FTTH is the Passive Optical Network (PON). PON technology permits a single fiber to be split up to 128 times without active electronic repeaters. This creates a point-to-multipoint network that does not require any electronics between the consumer premises and the central office.

A few telcos have deployed point-to-point fiber networks to supply FTTH. Others have connected PONs to neighborhood data concentrators called Optical Network Units (ONUs), creating "Fiber to the Curb (FTTC)" systems that may use either copper or fiber for the last connection to the customer. However, such systems have inherently higher costs than a point-to-multipoint PON.

There are therefore three main FTTH candidate technologies, all based on PONs, as shown in Table C-15. BPON is in use by major telcos now, while GPON and EPON are just beginning deployment. GPON has much higher bandwidth and flexibility, and is at a more advanced stage of standardization. EPON, on the other hand, requires lower-cost equipment costs and has the advantage of the worldwide deployment of Ethernet-compatible technology. BPON has a drawback in that it can only be used with Asynchronous Transport Mode (ATM) networks, and more common technologies like Ethernet must be packetized on top of ATM.

Table B-15
FTTH Technologies

Acro-nym	Name	Standard	Rate down/up	Data Link	Release	Notes
BPON	Broadband PON	ITU G.983	155/622 Mbps 155 Mbps	ATM	1998; 2005	Formerly called ATM-PON or APON
GPON	Gigabit PON	ITU G.984	1244/2488 Mbps 155-2488 Mbps	ATM, Ethernet, others	2003	
EPON	Ethernet PON	IEEE 802.3ah	1000 Mbps 1000 Mbps	Ethernet	2004	Also called Ethernet over the First Mile (EFM)

Major telephone companies in the United States are committing to FTTH. Deployment in Japan is much farther along thanks to support from leading telcos. Bandwidth provided to individual users with BPON now is 15-30 Mbps.

Application to utility systems: Wide area network access to feeder devices and consumer portals. Portal software could be designed to run within the Optical Line Terminal (OLT) itself, combining telecom and power utility portals. Ethernet PON could enable portals to use Ethernet for both local-area and wide-area networking, potentially reducing costs.

Strengths: High bandwidth, scalability. Will have the backing of the large telecom providers, and may end up being used by the cable providers also. Security has been planned in ahead of time. Most analysts seem to agree that fiber optic to every home is the eventual destiny of the Internet.

Concerns: Not clear which technology will win the market battle, or whether the business case for FTTH has really been solved. Unlikely that rural areas will be served soon. Wireless technology, having no cabling costs at all, may end up leapfrogging fiber.

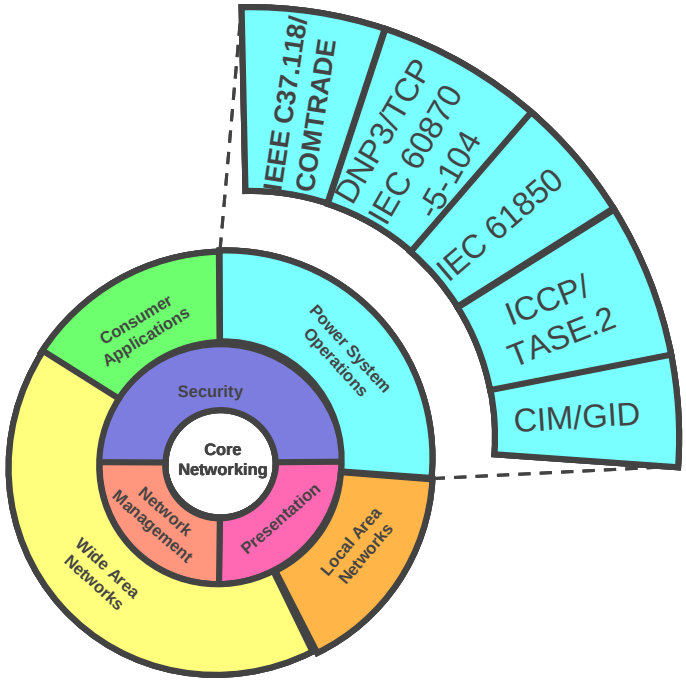
Layers: Data Link, Physical

References:

- http://www.ftthcouncil.org – FTTH Council
- http://www.efmalliance.org – Ethernet over First Mile Alliance
- http://www.fsanweb.org – Fiber Services Access Network (creators of APON)
- http://www.lightreading.com – Fiber industry news service
- http://www.ftthblog.blogs.com – FTTH Blog

Power System Operation Technologies

Power system operation technologies provide communications capabilities for power system and other utility applications. Communications protocols are most useful for applications such as EMS/DMS data delivery, power quality monitoring, outage detection and automatic recovery, distributed generation, grid management, and other advanced distribution features.



Distributed Network Protocol (DNP3) over TCP/IP (IEEE P1815)

The Distributed Network Protocol (DNP3) is a protocol that represents a distillation of IEC 60870-5 working group work and extensive experience from proprietary protocols for performing Supervisory Control And Data Acquisition (SCADA) in substation and distribution automation. It was originally developed by Westronic, Inc. (now part of GE) but released to the industry as an open protocol. It is now maintained and promoted by the DNP Users' Group, which also provides test procedures, implementation guides and specifications to companies that perform certification. DNP3 and IEC 60870-5 are cited in the IEEE Std 1379-2000 recommended practice for remote-terminal-unit to IED communications.

Like most SCADA protocols, DNP3 uses a simple object model mostly based on a few basic data types: binary inputs, binary outputs, counters, analog inputs, and analog outputs. Individual data items in each of these data types are called "points" and are numbered but do not have names identifying what the data means. DNP3 differs from earlier SCADA protocols in its "object-oriented" approach that permits the definition of new data types, the mixing of data types in a single message, and that it transmits meta-data in each message to help parse it.

Later updates to the standard have added more advanced features like file transfer, arbitrary data sets, flexible object attributes, and limited self-description. Work is now completed on an XML-based configuration scheme for DNP3 based devices. A method of application layer authentication for DNP3 has been published in February 2007 called the DNP3 Specification for Secure Authentication. The DNP User's Group and others such as EPRI are continuing to evolve the DNP specification. Also of note regarding security, the IEC Working Group 15 is in the process of developing IEC 62351 for (Substation) Data and Communication Security. IEC 62351 part 5 standard specifically addresses security requirements for IEC 60870-5 and derivatives (i.e. DNP 3.0).

DNP3 was based on some of the early IEC 60870-5 standards, and it can be argued that it still complies with those parts of the specifications. However, the two protocol families chose to implement different parts of the lower-layer standards and are therefore non-interoperable.

DNP3 has defined a standardized mechanism for carrying the original serial protocol over IP networks, with the option to use UDP for LANs or TCP for WANs.

Application to utility systems: Communication between SCADA/EMS/DMS and field installations. Also LAN based communications within field installations for connecting IEDs if necessary (utility standards) and legacy devices.

Strengths: Simplicity, very efficient use of bandwidth, very reliable. DNP3 has excellent User Group, utility and vendor support in North America, where it has become a de facto standard for substation and distribution automation. It is also popular in South America, Australia, UK, regions of Asia and parts of the Middle East.

Concerns: Supports objects, but no way to flexibly access the structured data within the objects. It needs a way to map logical names into point numbers.

Layers: Application, Data Link. Specifies use of TCP and UDP Transport.

References:

- http://www.dnp.org – DNP Users' Group

IEC 60870-5-104 Telecontrol over TCP/IP

IEC 60870-5-101 is the international standard for Telecontrol, which is the European term for SCADA or distribution automation. It is a three-layer protocol originally intended for serial links. IEC 60870-5-104 is the companion standard for carrying this protocol over TCP/IP. It is therefore the most suitable protocol in the IEC 60870-5 family for implementation in utility systems.

IEC 60870-5-104 uses the same kind of "point-based", anonymous object model, and provides mostly the same communication services as DNP3. IEC 60870-5-104 and DNP3 are both based on sub-parts 1 through 5 of the IEC 60870-5 specification, which in turn was based on a body of experience with dozens of earlier proprietary SCADA protocols. IEC 60870-5 is often called "the European DNP3" and DNP3 is similarly called "the American version of IEC 60870-5" depending on which side of the world the speaker is located.

The IEC 60870-5 protocols do not have a formal users' group which is a significant disadvantage, but members of the IEC working group that created it maintain a mailing list and web site. The IEC 60870-5-6 standard defines guidelines for conformance testing, and specifications for detailed test procedures are in development. A common method of application layer authentication for both IEC 60870-5 and DNP3 is also under development as part of the IEC 62351 work.

Application to utility systems: Communication between SCADA/EMS/DMS and field installations. Also LAN based communications within field installations for connecting IEDs if necessary (utility standards) and legacy devices.

Strengths: Simple, efficient and reliable. Widely used in Europe, Asia and parts of the Middle East and Africa.

Concerns: Not yet truly object-oriented; needs a way to map logical names into point numbers. Discussion is underway about a developing a standard to do this using XML.

Layers: Application, Data Link. Specifies use of TCP Transport.

References:

- www.iec.ch – International Electrotechnical Commission

IEC 61850 Substation Automation

IEC 61850 is the new international standard, released in 2004 and 2005, for substation automation based on Ethernet LANs. It is also being proposed as the basis for automation in several other areas of the utility communications network.

Partially based on a project by the Electrical Power Research Institute (EPRI), called the Utility Communications Architecture (UCA®), IEC 61850 has been a decade in development. IEC 61850 incorporates a number of advanced features that had not been previously been used in substation or field equipment automation.

- A structured, hierarchical object model with human-readable, descriptive names.
- Standardized objects (known as *logical nodes*) for substation functions like protection, metering, power quality monitoring, fault recording, transformer monitoring, etc. One of the reasons the standard took so long to develop was achieving consensus from vendors on these objects.
- The use of online self-description, permitting the possibility of "plug-and-play".
- An XML-based description language that promises to automate the labor-intensive and error-prone process of configuring field installations (substations).
- High-speed, multicast peer-to-peer messaging, enabling the ability to trip and close breakers using LAN messages.
- A similar high-speed protocol for multicasting samples of power waveforms over a LAN in real-time, permitting new applications and reduced costs due to decentralization of automation functions.

IEC 61850 is promoted and supported by the UCA International Users' Group, which provides certification for test labs, and a quality program that analyzes and forwards user concerns to the IEC so the specification can be updated.

The IEC 61850 object model structure is extremely flexible, permitting vendors to produce products that implement a subset or superset of the standard while maintaining interoperability. Various parts of the IEC are in the process of developing additional object models based on IEC 61850 for use in equipment found elsewhere in the utility industry. These efforts include the development of

new objects for distributed generation, hydro power, and wind power. Some of these will be published under a different standard number.

Unlike many IEC standards, there is no corresponding "North American version" of this standard. Members of UCA International and other standards bodies agreed that there would only be a single standard; the earlier UCA2 specification is obsolete now that IEC 61850 has been released.

The IEC Working Group 15 has completed the majority of the work for the component parts of IEC 62351 for (Substation) Data and Communication Security. of IEC 62351 part 6 specifically addresses security requirements for IEC 61850 profiles.

Application to utility systems: The 61850 family of standards is the IntelliGrid recommended technology for new substation LAN implementations when practical considering installed base and training needs. The next edition of the standard is due out shortly. Updates are expected to Part 9-2 on sampled measured values and phasor measured data as well as new object models such as revenue metering and Distributed Energy Resources (IEC 62350).

Strengths: Advanced features, support for new applications, flexible object modeling. All major substation vendors are producing products. IEC 61850 is one of the intial set of 5 NIST recommended Smart Grid Standards. Will support future enterprise wide integration once IEC 61850 and CIM object models are harmonized (see below).

Concerns: Complex to implement for clients, although not so much so for servers. All vendors buy their software from one of only a few sources. It has received limited deployment so far in North America.

Layers: Application. Specifies a variety of three-layer and seven-layer profiles for carrying the application layer.

References:

- http://www.iec.ch – International Electrotechnical Commission
- http://www.ucainternational.org – UCA International Users' Group

IEC 61850-7-420 Distributed Energy Resources

The IEC 61850 series of standards was originally developed to define a set of next-generation communications protocols for substation automation. Since its initial release in 2004 its scope has been expanded to include almost every aspect of utility communications.

The core of the IEC 61850 series is the "Part 7" standards, which include:

- **IEC 61850 -7-2 Abstract Communication Services Interface.** Specifies the protocol services possible with IEC 61850 such as reading data, operating

controls, spontaneously reporting data, file transfer, and the framework for defining data objects.

- **IEC 61850-7-3 Common Data Classes.** Describes the lowest-level data types used for building data objects.
- **IEC 61850-7-4 Basic and substation logical node classes and data object classes.** Describes the data objects built from the Common Data Classes and defines "logical nodes" which are functional groupings of data objects.

The IEC 61850-7-420 standard is an extension of IEC 61850-7-4 that specifically defines the data to be exchanged with DERs. It makes use of the IEC 61850-7-3/4 common data classes, data objects and logical nodes and adds those required for implementing DERs.

Application to utility systems: IEC 61850-7-420 models will applicable to the control and monitoring of renewable generation resources as well as storage systems.

Strengths: Models are easily integrated into 61850-based systems

Concerns: Limited vendor involvement has led to large, overly specific data models

Layers: Application layer.

References:

- http://www.iec.ch – International Electrotechnical Commission

IEC 61968/61970 Common Information Model

The Common Information Model (CIM) represents an attempt to develop a single information model and a common interface for software access to all data exchanged by a power utility. The CIM is very abstract and incorporates many complex technologies. Therefore the CIM is discussed in considerable detail here to help give the reader an idea of their capabilities.
The CIM was originally developed as part of the EPRI Control Center Application Programming Interface (CCAPI) project and later standardized by the IEC as part of the IEC61970 series standards for control centers. The IEC 61970 standard includes information associated with control center applications such as energy management, SCADA, and network planning. The IEC 61968 standard extends CIM to include Distribution Management Systems (DMS) functions such as asset management, outage management, auto-restoration, geographic information systems (GISs) and workforce management.

The CIM differs from the IEC 61850 standard in a number of ways:

- **Scope.** CIM is intended to represent all operations of a utility, while IEC 61850 addresses mainly substation devices and functions. Both models contain measurements, breakers, transformers, substations, and voltage levels. However, CIM's focus is on the power system level and also includes objects

like assets, work orders, crews, and schedules. Similarly, both IEC 61850 and GID define standard communications services, but GID goes farther to define the details of software interfaces for these services.

- **Methodology.** The CIM is captured in Unified Modeling Language (UML) and makes extensive use of object modeling techniques such as inheritance. The IEC 61850 models use a few standard object-oriented techniques, such as common data classes, but differ from commercial object modeling in a number of ways. For instance, two objects may contain different attributes but still share the same name.
- **Topology.** The CIM is an extremely interconnected, cross-linked model with several different approaches to viewing the data. The IEC 61850 model, on the other hand, while being quite flexible, is nevertheless organized in a very top-down and hierarchical manner.
- **Technology.** CIM/GID is most frequently implemented using common commercial computing technologies like OPC and Java, while IEC 61850 is most often mapped onto the Manufacturing Message Specification (MMS), which has a very specialized market. Both use Extensible Markup Language (XML) for configuration and setup, but GID has an XML messaging format already defined, while an XML mapping for IEC 61850 messages is still under development.

CIM data may be carried on a number of different communications technologies, which for the most part are not specified in the standard. Instead, the Generic Interface Definition (GID) focuses on defining standard application level software interfaces which may be implemented on a number of different platforms using several different "middleware" technologies, including in particular:

- Remote Procedure Call (RPC)-based application interfaces using CORBA, COM, Java, or C language specializations
- World-Wide Web Consortium Web Services using XML and HTTP

The GID standard specifies two different aspects of each interface:

- The **programmatic** details, i.e. the parameters and semantics of their exchange
- The **namespace,** i.e. how data is named, searched, and specified. A namespace can be thought of as a hierarchical "tree" for the organization of the data. It provides meaning to the data rather than just an arbitrary text name.

CIM and GID define three different types of namespaces, or trees of organization. The difference between these namespaces is illustrated by explaining where a breaker fits in each namespace:

- **Physical**. Breakers are contained in Substations, which are found in Control Areas, which are owned by utilities.

- **Class**. Breakers are a type of Switch, which are a type of Conducting Equipment, which are a type of Power System Resource.
- **Information Service**. Breakers are listed in Breaker Test Reports, which are part of the Maintenance Management System.

To access these namespaces, the GID defines four separate interfaces, which are distinguished by their type of service they provide and the type of data they carry, as described in **Error! Reference source not found.**. All of these interfaces support **self-description** of the structure of the namespace (the object schema) and the actual data available on a particular device (the object instances).

The GID interfaces were mostly developed and specialized for utility use based on the following commercial computing technologies:

- **Object Linking and Embedding (OLE) for Process Control (OPC) Interfaces.** OPC is a set of technologies developed by Microsoft, based on their earlier COM and DCOM products, and widely adopted for industrial and power industry automation applications. Microsoft no longer extends the OPC technology but continues to provide it, while the independent OPC Foundation markets and supports it.
- OPC is used to implement the GID in the COM, .NET, and web services environments.
- **Object Management Group (OMG) Interfaces**. The OMG is a consortium including Hewlett-Packard, Apple Computer, Sun Microsystems, and IBM, which develop standards for distributed multi-platform computing using object models. OMG developed the Data Access for Industrial Systems (DAIS), Data Access Facility (DAF) and Historical DAIS (HDAIS). These are cross-platform versions of OPC interfaces which are all used to implement GID.
- The OMG interfaces are used to implement GID in CORBA, Java, and C-language environments.

The IEC standards define both Microsoft and non-Microsoft versions of the GID, both or either of which are considered to be compliant.

CIM and GID are supported by the CIM Users' Group, which is considering becoming part of UCA International User's Group.

Table B-16
Summary of the Generic Interface Definition (GID)

Type of Service	Type of Data			
	Description	**Generic**	**High-Speed**	**Time-Series**
Type of Service		User-friendly access to non-time critical bulk data	Optimized for speed and volume, at the cost of requiring more configuration	Arrays of data containing the history of values over time
Request/Reply	Data at a server is queried by a client	Generic Data Access (GDA) Used for browsing, database access, or data warehousing	High-Speed Data Access (HSDA) Used for transferring real-time SCADA data within the enterprise	Time-Series Data Access (TSDA) Used for exchanging data for trending and analysis
Publish/Subscribe	A client registers to be notified of data later by the server	Generic Eventing and Subscription (GES) Used for application integration using XML-based message buses		

Application to utility systems: An information model representing utility wide data in power utility software applications located anywhere in the power systems communications network. Focus is on enterprise level operational applications.

Strengths: One of the initial set of 5 NIST recommended Smart Grid standards. CIM/GID is versatile and is independent of underlying communications technologies. It may eventually permit true plug-and-play of utility software applications.

Concerns: Extremely complex, with many layers, and runs well only on larger computing platforms. Likely to provide access to substation, feeder and consumer portal data only through "wrappers" – specialized gateways – translating data from other communications technologies discussed in this document. Because CIM models are abstract data models there is no clear path to define concrete data representations for either data storage or data in transit. Because of its abstract nature, virtually any product can be considered CIM compliant.

Layers: Application layer and above.

References:

- http://www.ucainternational.org – UCA Users' Group
- http://www.cimuser.org – CIM Users' Group
- http://opcfoundation.org – OPC Foundation
- http://www.omg.org – Object Management Group
- http://www.omg.org/technology/documents/formal/dais.htm - DAIS specification

IEC 60870-6 Telecontrol Application Service Element (ICCP/TASE.2)

The IEC 60870-6 standard was an early success of standardization in the power industry. It was originally developed as the Inter-Control Center Protocol (ICCP), a project of the Electrical Power Research Institute (EPRI). It was proven through a series of multi-vendor interoperability tests and quickly gained industry acceptance, to the point where almost it is supported by almost every Energy Management System (EMS) or Distribution Management System (DMS) currently produced.

It was standardized as IEC 60870-6, the Telecontrol Application Service Element 2. (TASE.1 was the ELKOM 90 protocol, which was not successful as a standard.)

TASE.2 is an interesting mix of technologies. It uses the same underlying protocol layers as the IEC 61850 client/server stack, and supports self-description although it is not an "official" part of the specification. Its object model uses human-readable names, but there is no standard naming convention. Therefore the object model more closely resembles DNP3 or IEC 60870-5 "points lists" than IEC 61850 logical nodes.

For this reason and because of its widespread acceptance, some utilities mistakenly try to apply TASE.2 to communications between control centers and field installations. However, it is missing some of the key features of these SCADA protocols and is much more suited for master-to-master communications.

TASE.2 is considered a UCA protocol and is supported by the UCA International Users' Group along with IEC 61850.

Application to utility systems: Communications between EMS, DMS and select other system such as metering systems.

Strengths: Widespread acceptance in its market area. One of the initial set of 5 NIST recommended Smart Grid standards.

Concerns: Technically weak for use in the substation, distribution and consumer domain. May not be appropriate for direct connection to a substation or portal, but may carry information elsewhere in the network.

Layers: Application. Specifies multiple seven-layer profiles; most commonly used with TCP/IP.

References:

- http://www.iec.ch – International Electrotechnical Commission
- http://www.ucainternational.org – UCA International Users' Group

Phasor Measurement Data and Disturbance Recording

The growing importance and utilization of these measurement technologies is driving need for effective data exchange. Phasor data and disturbance records present unique data requirements, including high speed streaming phasor data that must accurately time synchronized. In the case of disturbance records the data tends to be large time synchronized data records of events that may be 10MB records or larger. It is also necessary to define the data base formats for these data types.

The latest Phasor Measurement Unit (PMU) / Phasor Data Concentrator (PDC) protocol is the IEEE C37.118 that was developed in the last few years and approved in 2005. It replaces the IEEE 1344 synchrophasor protocol which has been in use as the PMU standard since its development in 1998. Before these standards were developed, the defacto standard for PMU to PDC communication has been the Macrodyne type 1 and type 2 protocols developed by Macrodyne Corporation. Some of the PDC to PDC protocols include the PDC data exchange format, the PDC stream, second level PDC using NTP time and the PDC stream, second level PDC using native time. These standards address issues like synchronization of data sampling, data to phasor conversions, and formats for timing input and phasor data output. There is an ongoing effort to adapt IEC 61850 to carry C37.118 data.

IEEE 1344-1995 (reissued 2001) IEEE Standard for Synchrophasors for Power Systems

The original IEEE standard for synchrophasors for power systems. The standard defines the communication data formats including a configuration frame, header frame and phasor information frame. Also defines a consistent and accurate time tagging method. Supports the use of synchronized and non-synchronized sampling. Specifies that the system lock on the frequency of the signal and not the nominal frequency and requires the correction of internal phase angle delays.

Application to utility systems: Used for PMU to PDC and PDC to PDC communications.

Strengths: The first standard dedicated phasor measurement protocol.

Concerns:

- Limited implementations by vendors.
- Defined angle convention at zero-crossing only.
- Limited to steady state conditions and accepts different device responses to non-steady state conditions.
- Data format not compatible with IP network communications. Approach similar to COMTRADE for serial communications.

Layers: Application. (Serial protocol only)

References:

- http://www.naspi.org/

IEEE C37.118-2005 IEEE Standard for Synchrophasors for Power Systems

Replaces the IEEE Std 1344, the standard has been completely revised and defines the communication data formats including a configuration frame, header frame and phasor information frame. The new standard provided a number of improvements over the previous including:

- Improved time tagging method
- Defined an "Absolute Phasor" referenced to the GPS-based and nominal frequency phasors.
- Introduced the concept of a Total Vector Error (TVE).
- Recommended PMU steady-state performance compliance testing with two levels of testing.
- Data format compatible with IP network.

Application to utility systems: Used for PMU to PDC and PDC to PDC communications.

Strengths: Significant improvement over IEEE 1344 that includes performance testing levels of accuracy etc. Vendor support is quite strong. Compatible with network protocols – UDP & TCP.

Concerns:

- Dynamic performance compliance is recommended but not required.
- Lack of frequency measurement accuracy requirement – results in TVE varying over a time window.
- Does not provide needed detailed test set-up and procedures for compliance testing.

- Does not include field installation and commissioning guidance
- Lack of guidance for connections to PDC.

Layers: Application layer

References:

- http://www.naspi.org/

IEEE Std C37.111-1999 - IEEE Standard Common Format for Transient Data Exchange (COMTRADE) for Power Systems

A common format for data files and exchange medium used for the interchange of various types of fault, test, or simulation data for electrical power systems. Sources of transient data are described. Issues of sampling rates, filters, and sample rate conversions for transient data being exchanged are discussed. Files for data exchange are specified, as is the organization of the data.

Application to utility systems: Data format and file conventions for event recording by Digital Fault Recorders, Power Quality meters and other IEDs. Useful for post-fault analysis of system disturbances, e.g. inter-area oscillation problems.

Strengths: Primary standard for power system event data. Strongly supported by vendors. The other similar standard (IEEE Std 1159.3 - 2003) is focused to power quality data and event recording.

Concerns:

- Data format not compatible with IP network communications. Intended for serial communications.
- Needs improved specificity for channel definitions and phase codes
- Need method to represent spectral and statistical data
- Need method to handle min/max/average and other channel and variants
- Need method to handle Multi-Need and Multi-Time Base data in a single file.

References:

- IEEE Std C37.111-1999, http://standards.ieee.org/

IEEE Std Series 1547 – Standard for Interconnecting Distributed Resources with Electric Power System

This series of standards describes connections between the bulk power system and Distributed Energy Resources. IEEE Standard 1547 was issued in 2003 as a set of guidelines for installing electric generation equipment with a gross output

value of 10 MW or less to the utility distribution system. The intent of the standard is to have a consensus standard that collects the technical requirements for interconnection between distributed generation resources and the utilities.

The intent was to create a standard that could be universally adopted, by utilities, manufacturers, energy service companies, regulators and others in the energy business. The technical requirements are related to the performance, operation, testing, safety, and maintenance of the interconnection. The standard does not consider the type of the energy technology used to interconnect to the utility. The standard is technology neutral and provides guidelines for the minimum technical requirements for a technically sound interconnection.

The 1547 standard is a family of standards that grows with time and technology.

- The base standard, 1547, covers the connection of a generating system of 10MVA or less to the typical utility distribution system, either the primary or the secondary voltage.
- Standard 1547.1 covers the conformance testing of the inverters and equipment covered in the standard.
- Standard 1547.2 is an application guide for the installation of distributed resources.
- Standard 1547.3 is a guide for the communications, including monitoring, information exchanges and control of DER.
- Standard 1547.4 is the guide for the design, operation, and integration of DER islands into the utility operations. The guide covers intentional electrical islands, not inadvertent islands.
- Standard 1547.5 is a guide for the interconnection of DER greater than 10 MW into the electric system. This extends the coverage of the 1547 series to devices greater than 10 MW, which was the limit of the original standard 1547.
- Standard 1547.6 extends the standard to operation with utility networks, which were not covered in the original 1547.

As of this writing, there are two new sections being written and discussed.

- Standard 1547.7 will be the guide to conducting impact studies for distributed energy resources. The standard directs the study of the impacts that the DER will have on the electric utility and the other customers. That includes the impact on system protection, power quality, and technology dependent impacts, such as intermittency and dispatchability. The studies that this standard suggests are in-depth assessments of the effect of the DERs on the electric system.
- The newest section will be 1547.8, a recommended practice for establishing methods and procedures that provide supplemental support for implementation strategies for expanded use of IEEE Standard 1547. The purpose of this standard is to provide flexibility in the application of Standard 1547. For instance the utility may ask the DER to raise or lower the voltage

within the ANSI value range, but to a different level than the utility is operating without the DER connected. This operation is not to be considered a violation of the "shall not regulate the utility voltage" clause of Standard 1547. The DER may be requested to act as a supplemental voltage regulator.

Application to utility systems: IEEE 1547 defines the electrical interfaces used for small-scale dispatchable generation.

Strengths: Declares requirements such as fault ride-through which enables utilities to treat outside generation as if it was an extension of the utility generators.

Concerns: Newer sections are currently under development.

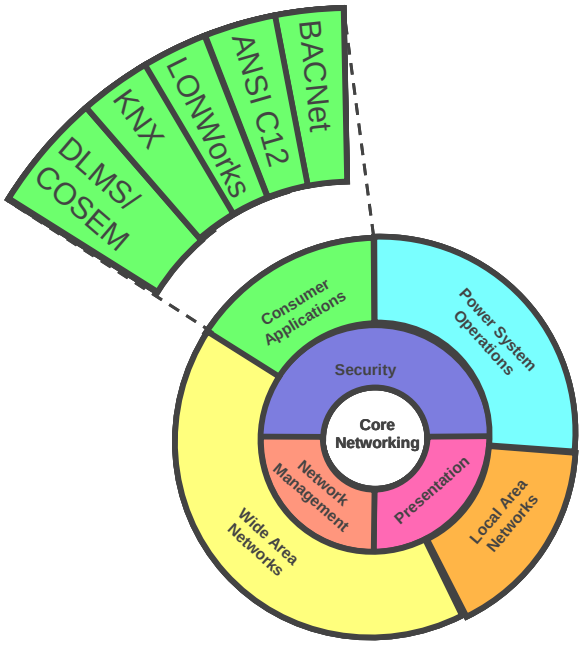
References:

- http://grouper.ieee.org/groups/scc21/dr_shared/

Consumer Applications Technologies

This chapter describes technologies that are designed specifically for the consumer environment, in other words, metering, demand response, and building automation.

Note: X10 could also be considered to fit in this service group, but is included with the LAN protocols instead because it has only a rudimentary application layer and has more in common with sensor access technologies like ZigBee.



ANSI Metering (ANSI/IEEE C12.19 and C12.22)

In 1997, the American National Standards Institute (ANSI), the IEEE Standards Coordinating Committee (SCC) 31, the American Meter Reading Association (AMRA), the National Electrical Manufacturers' Association (NEMA), and Measurement Canada worked together to release one of the first standardized object models for the utility industry.

IEEE1377 / ANSI C12.19, "Utility Industry End Device Data Tables" specifies a standard set of data "tables" for representing the data produced by revenue meters. These tables are designed to apply to water and gas as well as electrical metering. They specify such items as the name plate of the device, its physical connections, the actual measurements it makes, security parameters, load profiles, event logs, and the capability to add vendor-specific tables (manufacturer defined tables).

The tables are extremely flexible, permitting almost any existing meter to represent the information it reports. However, as a result, they are consequently fairly complex. A C12.19 client must go through a lengthy "discovery" process, using the self-description capabilities of the table definitions, to locate a particular piece of data in a meter and determine how the meter represents that data (e.g. scaled integer, fixed-point, floating-point, BCD, etc.). Because only the "root" table is mandatory, this process must be performed for every meter. However, once the process is complete, the table definitions specify how to achieve very efficient access to the data itself. Additionally, the table structures provide an information grouping mechanism that allows all critical information to be available from a single place (user defined tables)

The C12.19 standard specifies the format of the data, but does not specify a protocol to carry it. The design is that the tables can be carried by any protocol that supports read and write equivalent operations. Even operations such as resetting counters, running diagnostics, and restarting the meter can be done by writing to a table. There are several other standards in the C12 series that deal with the transport of the tables in specific environments:

- C12.18 specifies how to transmit the tables over a *local optical port*.
- C12.21 specifies how to transmit the tables over *telephone modems* (IEEE 1390).
- C12.22 specifies how to transmit the tables over a generic *wide-area network* and/or a local interface between a meter and a WAN communications interface.

The generic application layer services defined in the C12.18 and C12.21 standards are known as the Protocol Specification for Electric Metering (PSEM). The C12.22 WAN interface standard specifies an "Extended" version of PSEM (literally, EPSEM) wrapped in the Association Control Service Element (ACSE) standard, ISO 8650-1. ACSE identifies meters using ISO application layer addresses, known as AP-Titles. In conjunction with EPSEM it specifies the following functionality:

- Transmitting multiple C12.19 table requests in a single message
- Authenticating and encrypting the C12.19 data stream
- Registering and looking up AP-Titles (what is it) in a distributed directory that maps them to "native addresses" such as IP addresses. This directory provides features similar to the ISO X.400 service.
- Segmenting large messages into sizes suitable for transmitting on a variety of transport layers, such as TCP.
- The transport, data link, and physical layers for connecting a meter to a local communications interface.
- Routing messages across "non-heterogeneous" networks, i.e. those that do not share a network layer.

A new version of C12.19 and the initial version of C12.22 were released in 2008. AMRA International acts as a user's group for these standards. Also, the Association of Edison Illuminating Companies (AEIC) maintains a specification to facilitate purchasing of C12 containing metering devices with a defined subsets of capabilities for common metering configurations.

Application to utility systems: A candidate for standard representation of metering data from a portal. The new version of C12.19 will specify an XML representation of the tables that could be used with business systems. Not all functionality in this standard is applicable to portals: The C12.22 local profile is too specialized to use as a general customer site LAN. The name registry and routing functions of C12.22 would be better performed by ISO or IETF standards in a portal environment. Similarly, the application layer authentication in C12.22 could be worthwhile, but encryption at the application layer would be redundant.

Strengths: The standards are mature, extremely well-defined, thoroughly reviewed, and accepted by all major metering vendors, in multiple industries.

Concerns: Requires considerable complexity implemented in the client to achieve interoperability, as discussed above (sometimes even requires minor modifications for pair-wise interoperability). While accepted by all North American standards organizations, C12.19 and C12.22 are not recognized by the IEC or ISO.

References:

- www.amra-intl.org – AMRA International, formerly the American Meter Reading Association
- http://strategis.ic.gc.ca/epic/internet/inmc-mc.nsf/en/lm03758e.html - Tutorial presented at a Measurement Canada seminar.
- http://www.nertec.com/standards/ansic1222/index.htm - Working Draft Documents

- http://shop.ieee.org – Online IEEE standard 1377, soon to be re-released.
- http://global.ihs.com – Official supplier of hard-copy ANSI standards
- http://www.aeic.org/ - Association of Edison Illuminating Companies

DLMS/COSEM (IEC 62056)

DLMS/COSEM is the international standard used in Europe and elsewhere in the world for exchanging metering data.

DLMS was originally created as the Distribution Line Message Specification, an application layer protocol for communicating with distribution automation devices. It was standardized as IEC 61334-4-41. It gradually evolved and was renamed the Device Language Message Specification, a generic protocol for accessing structured data models, and particularly, metering data.

The Companion Specification for Energy Metering (COSEM) expands on DLMS, defining:

- A generic set of extended communications *services* called xDLMS that is independent of lower layers (as well as the original existing services of 61334-4-41).
- A detailed *object model* for metering, based on a naming convention called the Object Identification System (OBIS).
- A *transport* specification based on HDLC for use over serial links, including optical port, local current loop, power line carrier, telephone lines, or GSM cellular, and (soon) TCP/IP

COSEM is recognized by several standard bodies. It was originally defined by the DLMS User Association in three specifications known as the "coloured books" (green, blue and yellow). These documents were split into several parts for standardization by the IEC in 2002 as IEC 62056.

COSEM is available as European national standard EN 13757-1 for gas, water or other types of metering. Work is underway on a second edition of the application layer, and a mapping to IPv4 is due to be released in 2005 or early 2006.

The COSEM object model is based on a hierarchy defined within the specification:

- Each physical device contains one or more *logical devices*. Types of logical devices are registered as being unique world-wide, registered by the DLMS User Association. If a client does not know a device's logical device type, it must discover it upon start-up of communications.
- A logical device contains two types of objects: *interface objects* and *association objects*. Before a client can communicate with a logical device, it must authenticate itself with the association objects using either clear text

password or cryptographic means via ACSE. The association objects negotiate access to the rest of the data based on the client's identity.

- Interface objects contain the actual metering data. Each interface object is an instance of a pre-defined standard *interface class*. Interface classes include such things as registers, demand registers, load profiles, clocks, schedules, and communication channels.
- Any particular object has a *logical name,* which is a string of up to six integers called *value groups* that identify exactly what the object represents. The OBIS portion of the standard defines what each of these integers means. The six value groups are labeled A through F and define the type of metering, channel, physical quantity, processing method, metering rate, and type of historical information. Vendor-specific extensions are permitted. There is a parallel *short naming* system defined that provides more efficient access to the data, albeit with less flexibility.

The DLMS User Association provides conformance testing of COSEM devices using a standard test tool and the "yellow book". Among other things, the test tool verifies that the hierarchy defined in the device complies with the OBIS naming specification.

The COSEM standards are:

- IEC 62056-42: Serial physical layer
- IEC 62056-46: Serial data link layer
- IEC 62056-53: Application layer
- IEC 62056-61: Object Identification System
- IEC 62056-62: Interface Object Classes

Not all parts of IEC 62056 are part of COSEM. IEC 62056-31 is Euridis, another metering protocol popular in Europe. IEC 62056-21 is FLAG, an earlier metering protocol whose specification is used in COSEM to register manufacturer identifiers.

Application to utility systems: A candidate for standard representation of metering data from a portal.

Strengths: A mature, internationally recognized standard evolved over a considerable length of time. It has extremely strong user support outside of North America. The pre-defined OBIS hierarchy makes it easy to access metering information without a lengthy discovery process.

Concerns: Mapping onto WAN or LAN profiles is not complete yet. It requires an update to the standard every time a new manufacturer or type of information is added.

References:

- www.dlms.com – DLMS User Association
- www.iec.ch – Standards available from the IEC

BACNet (ANSI/ASHRAE SSPC 135)

The Building Automation and Control Network (BACnet) standard was published in 1995 by ANSI and the American Society of Heating, Refrigerating and Air-Conditioning Engineers (ASHRAE). It was intended to be a solution to the multitude of proprietary protocols that had been developed in the building automation industry.

BACnet is now ISO standard 16484-5 as of 2003. The ASHRAE Standing Standard Project Committee 135, which controls the standard, has published several addenda starting in 2001, including definitions of Interoperability Building Blocks and a conformance test specification (ANSI/ASHRAE SSPC 135.1). There are several BACnet Interest Groups (BIGs) and a BACnet Manufacturer's Association in operation to support and test the technology. The National Institute for Standards and Technology (NIST) has been closely involved with the effort to develop standardized conformance testing of BACnet.

BACnet consists of an object model, a services definition, a network layer, and a number of possible data link layers. Data link layers may include:

- The BACnet Token-Passing data link layer for use over EIA-485
- The BACnet Point-to-Point data link layer for use over EIA-232 and dial-up modems
- ARCNET
- LonTalk (a competing building automation protocol owned by Echelon)
- Ethernet directly
- Internet Protocol, by way of a "BACnet Virtual Link Layer (BVLL)" and UDP

The BACnet object model and services are similar in many ways to SCADA protocols, including binary inputs and outputs, analog inputs and outputs, accumulators, events, alarms, and files as well as a number of objects specific to building automation, such as safety zones, schedules, process control loops, programs, and calendars. However, a recent addendum being currently balloted supports a new object type that supports the hierarchical organization of these primitives into well-known aggregations that perform common functions.

Application to utility systems: Because BACnet has its own network layer separate from that of IP, it is possible to "overlay" a BACnet on top of an IP network, to coexist with it, and/or to build gateways to and from the IP network. Thus a BACnet could either:

- Act as a local area network technology connecting a consumer portal to building automation equipment, e.g. for load control.
- Be extended *through* the consumer portal, permitting a utility to manage the building automation system remotely through the same IP-based WAN used by other portal protocols.

Strengths: A mature standard with a supportive vendor and user community. Has conformance and testing specifications already in place.

Concerns:

- Its object model, like that of the SCADA protocols, is limited to low-level types. The new "Structured View" object may address this specific limitation.
- BACnet is specified with such a variety of underlying layers that it may be necessary to specify a specific profile for use with consumer portals.

References:

- http://www.bacnet.org – ASHRAE BACnet site
- http://www.bacnetassociation.org/ - BACnet Manufacturer's Association

LONWorks (ANSI/EIA/CEA 709)

The Electronic Industries Alliance (EIA) and the Consumer Electronics Association (CEA) have endorsed an extremely popular protocol for building and industrial automation that was originally developed by Echelon Corporation. This protocol was originally known as LONTalk and is now known as LONWorks, where LON stands for Local Operating Network. It is accredited as an ANSI standard through the EIA.

There are four parts to this standard:

- EIA 709.1-B – The Control Network Protocol. The original was released in 1999, while the "B" revision superseded it in 2002.
- IEC 709.2 – Power Line Carrier Physical Layer
- EIA 709.3 – Twisted Pair Physical Layer
- EIA 709.4 – Fiber Optic Physical Layer

Echelon defines other physical layers, including an RF wireless option, but only those listed above have been standardized. A method for "tunneling" the protocol over IP networks has been standardized as EIA 852. The protocol is operated at a variety of different rates depending on the media used, ranging from 4.88 Kbps to 1.2 Mbps. Range also varies, from 130 meters on high-speed twisted pair to 6000 meters on power line carrier.

The object model for EIA 709.1 is based around Standard Network Variable Types (SNVTs, pronounced "snivets"). Echelon maintains a list of SNVTs for a variety of physical measurements such as switch state, energy, power, voltage, volume, flow, sound level and pressure. Configuration tools map variables, either SNVTs or manufacturer-specific types, between devices to set up the network.

Echelon specifies network management interfaces, but these are not part of the released standard. Authentication is available, but not encryption.

LONWorks has been specified as one of the data link and physical layer options for BACnet.

Application to utility systems: Communication with home and building automation equipment. The IP tunneling option may be appropriate for portals, which could act as a transparent gateway from an IP WAN into a local EIA 709 network.

Strengths: A huge number of vendors in a variety of industries have implemented devices, especially in HVAC, lighting and other building automation areas.

Concerns:

- Despite standardization by the EIA, CEA and ANSI, this technology remains a "de facto" standard rather than a truly open standard, because almost all known implementations use the "Neuron" integrated circuit chip developed by Echelon. There are multiple vendors of this chip, but all pay license fees to Echelon and all implementers must sign a patent license agreement with Echelon.
- The LONWorks object model appears to be very simple and non-structured, similar to SCADA protocols. SNVTs are addressed by index and not by function. Structure may be added only through external, offline configuration tools. The functional meanings of objects are not available online via self-description.
- Limited support in the power industry so far.

Layers: All seven layers.

References:

- http://www.echelon.com – Echelon Corporation
- http://www.lonmark.org – LONmark International users' group
- http://global.ihs.com/ - Official standards distributor for ANSI/EIA
- http://www.eia.org – Electronic Industries Alliance

KNX (Konnex, EN 50090)

The KNX Bus, promoted by the Konnex Association, is a European standard for home and building automation that evolved out of the work of three earlier organizations:

- BatiBUS Club International (BCI)
- European Installation Bus Association (EIBA)
- European Home Systems Association (EHSA)

KNX is an attempt to harmonize these three earlier protocols. The main protocol stack comes from EIB. Physical media supported by the other two standards are permitted and can coexist, but may not interoperate with the standard.

KNX operates over a variety of media. The version standardized as EN 50090 in 2003 includes specifications for operation over twisted pair or power line carrier. Transmission is very slow, providing a maximum bit rate of 9600bps on twisted pair or 2400bps on PLC. The PLC uses a carrier of 110 or 132 kHz. The KNX specification also includes a wireless RF physical layer and a specification for carrying KNX over IP that have not been standardized yet.

KNX supports a structured object model, in which data is grouped into domains (e.g. HVAC), applications (heating), functional blocks (water heater) and data point types (temperature in Celsius)

To manage this object model, KNX supports three different configuration mechanisms, with varying levels of complexity.

- A-mode (automatic) – essentially plug-and-play with self-description, for appliances
- E-mode (easy) – using simplified tools
- S-mode (specialized?) – permitting advanced features

The different modes are apparently a major part of the legacy inherited from the three predecessor protocols.

The Konnex Association serves as an umbrella organization for its predecessors, a marketer and promoter of the protocol, and a certification and testing body. KNX can apparently be implemented on a variety of simple platforms, although chipsets are available. It is "royalty-free to Konnex Association members".

Application to utility systems: Access to home and building automation equipment. It is possible that the KNX-over-IP specification would permit KNX data to be passed transparently through a portal.

Strengths: It is a European standard and an attempt to achieve consensus among differing organizations. For this reason it is sometimes referred to as the

European equivalent of BACnet. Including the supporters of its predecessor associations, it appears to have worldwide distribution. It has considerable configuration and network management support, including a separate organization dedicated to software tools.

Concerns: Not yet accepted as an international standard. It has low data rates and no apparent security. Largely unknown in North America.

Layers: All seven layers.

References:

- http://www.konnex.org – Konnex Association
- http://www.cenelec.org – CENELEC standards

ZigBee Smart Energy Profile version 1.0

ZigBee Smart Energy Profile defines a set of application rules for using ZigBee (wireless IEEE 802.15.4) devices for 8 different device applications:

- Energy Service Portal
- Metering Device
- In-Premise Device
- Programmable Communicating Thermostat
- Load Control Device
- Range Extender Device
- Smart Appliance Device
- Prepayment Terminal Device

ZigBee SEP 1.0 mandates security, which is an optional requirement for other ZigBee devices. Zigbee SEP 1.0 fulfills two use cases: in-home devices and sub-metering applications. ZigBee 1.0 has recently fallen out of favor due to both interoperability issues and the lack of a common wired communication standard. The standard has been updated to revision 1.5 but this has not gained enough market momentum to entice the switchover to the updated specification. Generally, users are awaiting the update to SEP 2.0.

ZigBee SEP 1.0 specifies a message/acknowledge protocol where the utility-side of the protocol becomes the data server (this is the reverse of how utilities view most communication systems). The SEP 1.0 defines the specific message exchange syntax and semantics for data groups known a "clusters". For example, pricing signals are defined as a single cluster.

Application to utility systems: SEP 1.0 could be used to control loads directly (via on-off or temperature up/down commands) or indirectly via price reports.

Strengths: Support for SEP 1.0 is strong.

Concerns: Interoperability problem plague SEP 1.0. Vendors and users both await an update to SEP 2.0.

Layers: All seven layers.

References:

- http://www.zigbee.org/Markets/ZigBeeSmartEnergy/Overview.aspx – ZigBee Alliance

ZigBee/HomePlug Powerline Smart Energy Profile version 2.0

SEP 2.0 is a re-cast of ZigBee SEP 1.0 to support a common model for both wired and wireless home connectivity solutions. It is supported both by the ZigBee Alliance and the HomePlug Powerline Alliance and is well aligned with utility interests. At the time of this writing, the specification remains at the draft stage.

SEP 2.0 is designed to be link technology agnostic and can run over the Internet Protocol (particularly IPv6) as well as other protocols. SEP uses well-known HTTP-like actions such as GET / PUT / POST to allow simple integration into systems based upon the Internet-Protocol. SEP 2.0 also adds the publish/subscribe model to reduce reaction time and decrease polling bandwidth requirements (which fundamentally improves scalability). SEP 2.0 expands the set of applications from SEP 1.0:

- Energy Service Portal
- Metering Device
- In-Premise Device
- Programmable Communicating Thermostat
- Load Control Device
- Range Extender Device
- Smart Appliance Device
- Prepayment Terminal Device

with the following additional applications:

- Premise Energy Management Systems
- Inverters
- Electric Vehicle Service Equipment
- End Use Measurement Device

SEP 2.0 uses the common SOAP (Simple Object Access Protocol) paradigm to leverage existing enterprise applications. SEP 2.0 also defines temporal randomization to reduce the problem of instantaneous responses to grid signals.

Application to utility systems: SEP 2.0 could be used for application listed under SEP 1.0 as well as new applications impacting the bulk power system.

Strengths: SEP 2.0 uses a common SOAP-like interface applicable across many transport layers beyond ZigBee.

Concerns: SEP 2.0 is not yet complete. Only prototype products can be built to the specification. Specifically, device management functions are not yet defined.

Layers: Application layer.

References:

- http://www.zigbee.org/Markets/ZigBeeSmartEnergy/Overview.aspx – ZigBee Alliance
- http://www.homeplug.org/tech/smart_energy – HomePlug Powerline Alliance

Open Automated Demand Response (OpenADR)

Open Automated Demand Response (OpenADR) is an open standards based communications data model designed to promote common information exchange between the utility and electric customers. OpenADR provides demand response price and reliability signals to business and residential customers. OpenADR was developed at the Demand Response Research Center managed by Lawrence Berkeley National Laboratory with funding from the California Energy Commission (CEC) Public Interest Energy Research (PIER) program, in collaboration with California Investor Owned Utilities.

In order to leverage both existing and future vendor investments in DR system development, the intent of the OpenADR is to be compatible with existing technology, and to be compliant with IEC electrical standards and specifically to be compliant with IEC 61968. Originally designed to support industrial and business customers, the scope of OpenADR has been expanded to include support for residential consumers including support for Smart Appliances.

OpenADR is an application layer protocol that uses the Internet to transmit signals from the Utility to customers. OpenADR has been specifically designed to support the full range of Demand Response (DR) application requirements including program enrollment, asset specification for devices including Smart Appliances, DR event management, and measurement of consumers' response to DR signals.

The OpenADR application layer is intended to be build on top of the Internet link, network and transport layers. Unlike ZigBee and ISO/IEC 15067-3 protocol, OpenADR does not specify other layers below the application layer; however, OpenADR should not be construed as any less complete than the other protocols. Rather OpenADR incorporates the common OSI network model of separate and loosely coupled protocol layers.

Application to utility systems: Implementation of Demand Response in ISO/RTO and customer environments.

Strengths: Strong interoperability due to adherence to OSI network model, Implementations in place in ISO/RTOs, open protocol, designed to be both forward and backwardly compatible, strong security incorporates

Concerns: Relatively few installations at this time, does not support device-specific queries.

Layers: Application.

References:

- http://www.openadrcollaborative.org/

Infrastructure to Support Customer Integration

Any smart grid roadmap must include due consideration toward how to integrate the customer. The need to involve the customer in the overall energy production, transportation, and delivery infrastructure has been present for some time but was fully pushed into the forefront due to the policy put forward in the Energy Policy act of 2005 and the actions that have followed in state regulatory agencies.

Integrating the customer requires a collection of technologies and infrastructure – all working harmoniously with well-defined points of interoperability to achieve the business and regulatory objectives associated with enabling customer interaction and control over their energy usage.

This infrastructure includes home network systems, new smart meters, communication networks from the meters to local concentrators, new concentrators and their associated back-haul communications networks to the corporate data centers, new and very large meter data management systems (MDMS) and finally data integration into existing software application platforms.

The technology choices for implementing integrated communications with end users and their devices can be broken into eight basic components. These include: home area networks (HAN), smart-meters with an attached communications modulo, wide area communications to the meters (WAN), concentrators, communications to the data centers, a head-end device for communications control, meter data management systems (MDMS), and application interfaces to existing corporate systems. We will address each of these components below, but it is important to note that each component should, whenever possible, adhere to open standards like IEC, ANSI, IETF, or IEEE, to maximize vendor choice and minimize the risk of obsolescence. Also, while a single technology choice for each category will help to minimize operational and maintenance cost, the broad coverage area for some utilities may dictate the need for multiple solutions for some the elements.

The HAN

Home area networks link smart meters or other devices performing the utility/customer interface function to devices within the home. These could include display panels that indicate energy usage or notify customers of higher energy costs; air conditioning cycling that temporarily reduces load during peak demand periods; thermostats that can be remotely adjusted by the Utility companies (with the customer's permission); connections to other meters (water, gas, electric) to allow for automated meter reads; or energy efficient home appliances that can be remotely controlled to save energy or reduce costs. Home networks can be wired or wireless. Open communications are especially necessary here, to assure that multiple appliances and other devices can work interchangeably within the AMI infrastructure. The current leader in the wireless arena appears to be the ZigBee protocol but other important technologies include IEEE 802.11, IPv6 LOWPAN and HomePlug PLC. These form the short list for in premise technology selection.

Smart Meters

Smart meters are a combination of a meter and an attached/integrated communications module that can enable communications with both the home area network and back to the Utility Company. This module (or modules) effectively implements the utility/consumer portal function which could also be implemented in a separate, purpose built device for this purpose. The communications module can be purchased separately from the meter and is often purchased from a different manufacturer – but usually under a specific agreement between the two vendors. It is becoming increasingly common however for the communications capability to be fully integrated with the meter to minimize cost.

Selection of the communications vendor determines many of the capabilities of the meter including not only the communication protocols (wired or wireless), but the data storage capacity and features available to the home network. For example, the communications module determines the ability to collect information from other meters in the home or the ability to control devices that reside in the home. Similar to a computer, this module is often a multi-purpose device that provides the intelligence to the meter. Also, similar to a computer, it is expected that this module may need to be updated with new software or replaced more often than an old mechanical meter. It is therefore important to choose a smart meter that can have its software components reliably and securely upgraded automatically through the communications network.

As of this writing, most utilities investigating the application of smart meters have found that the vendor community has not taken the issue of communications security seriously enough. To address this issue, the AMI-SEC task force was instantiated within the UtilityAMI working group in order to clearly define requirements and make technology recommendations.

Communications to / from the Meter:

Data flowing from or to the meters can be over numerous types of communication links including both wired and wireless connections. Wireless radio frequency (RF) connections can be either fixed or meshed networks. A meshed network allows for multiple communication paths in the event that one path is blocked or has failed. The data from the meter normally flows into a concentrator or aggregator, which may be just another meter. The concentrator gathers data from multiple meters via a communications link and then transports it back to the data center through a more robust communications network.

Meters can be connected through wired approaches like Power Line Carrier (PLC), Broadband over Power Lines (BPL), or telephone lines; or wireless approaches like cell phone, satellite, or WiMAX communications. The number of meters connected to a single concentrator varies widely, but the normal range is from one hundred to eight hundred devices per concentrator. Due to the large geographical coverage area of some utilities, it is expected that multiple types of communication networks will need to be deployed in various areas. Important issues to consider when selecting the meter communications network are:

The network must be able to handle large data flows for wide area outages and firmware upgrades in a secure manner.

- Meshed networks while offering redundant data paths may make local problem isolation more difficult.
- Communications network costs can be high and the network is an additional point of possible failure for the company.
- Open communication standards are necessary to avoid vendor lock-in.
- Requirements for use in applications other than supporting the customer interface (e.g. distribution automation, asset management, remote sensing, etc.) must be considered

North American communication vendors can be separated into three distinct types: Power line carriers (PLC), Broadband over Power Lines (BPL) and wireless or radio frequency (RF). Vendors included in these types are:

- PLC vendors
  - Cannon
  - Comverge
  - DCSI
  - Hunt

- BPL vendors
  - Ambient Corp.
  - Amperion, Inc.
  - Corinex Communications Group
  - Current Technologies Group
  - MainNet
- RF vendors
  - Cellnet
  - EKA Systems
  - Elster
  - Datamatic
  - Itron
  - Sensus
  - Silver Spring Networks
  - Grid-Net
  - SmartSynch
  - Tantilus
  - Trilliant

Concentrators / Data Collectors / Aggregators

The concentrator collects data from several to hundreds meters and transmits it back to the data center. It may be just another meter, with additional storage capacity, or a separate device. The concentrator, along with collecting data, provides a logical interface between the communications backbone to the data center and the communication network to the local meters.

Important features for the concentrator include:

- Scalability for data storage from multiple meters.
- Adherence to open communication standards for multiple types of connections to the local meters and to the data center.
- Ability to isolate problems during outage and restoration process and determine when full restoration is complete.

At the time of this writing, few vendors offer data concentrators that are truly standards based. There are some notable exceptions but this is an area where improvement is needed in the industry. At present, the concentrator is often considered a vendor specific component within the communication network vendors "black box" that links the meter to the head end or MDMS. As long as the interfaces to the "black box" are open and standard, the basic principles of IntelliGrid are met.

Back-Haul Communication Networks

Data stored in the concentrators must be delivered back to the data center. The back-haul communications network must be able to handle the consolidated loads from the multiple concentrators.

Options for back-haul include utility owned networks such as SONET, Telco provided communication lines like T-1 or OC3; self-provisioned wireless connections; public wireless (e.g. metropolitan WiFi or WiMAX); or BPL links.

Important features for communication backbones to the data center include:

- Scalability to handle the combined data loads from the concentrators.
- Reliability since a single communication failure here could impact very large numbers of concentrators.
- Possible need for redundant connections to help assure reliability.
- Adherence to open communication standards for both the connections to the MDMS and to the concentrators.
- Be secure and remotely manageable

The network should be capable of supporting and evolving with the most advanced of Internet Protocol management and support technologies. These include VLAN's, MPLS, VPN technologies and others.

Head-End Device / Communications Control Server

The communications control server oversees the transmission of data from the meter to the MDMS and monitors the end-to-end connections. This device must be able to accept data from the various communication network and present it to the MDMS. It monitors the communication network to determine whether or not the smart meters are communicating properly and if communication errors arise this head-end device attempts to resolve the problem.

Communication Control Servers are normally provided by the same vendors that provide the communications modulo attached to the smart meters since they need to verify the data coming from those meters. It is important that the Communication Control Server adheres to common interoperable standards where is interconnects with the MDMS platform. This adherence to open data standards will allow for plug & play interconnects for the various MDMS providers.

EPRI recommends that the vendor support the IEC 61968 / 61970 standards for the Common Information Model (CIM) and Generic Interface Definition (GID). This is an area that is still largely proprietary and needs more development within the industry. The new AMI-Enterprise task force within the UtilityAMI working group is beginning to address this and the MDMS interface.

Meter Data Management Systems

Meter data management systems for large Utilities are relatively new to the market. The current vendors in this arena have deployed systems that can handle smaller companies with fewer meters, or companies that do not currently read meters on hourly or less intervals. Therefore, scalability of these systems is an important issue. Also, it is important to consider the role of the MDMS in the organization. Since most Utility Corporations already have Customer Care, Outage Management, Billing, SCADA, and other software packages deployed, it is important not to duplicate these functions within the MDMS. However, several of the vendors of MDMS systems are attempting to do just that. Duplication of functions not only is expensive from a data storage perspective, but more importantly it can lead to differing views of customer data from the duplicated software packages. Duplication of data and applications also tends to complicate business processes since multiple systems must be accessed to retrieve information. Finally, capital, maintenance, and operating expenses tend to be higher when multiple systems are involved. It is therefore important to have a MDMS that not only stores and analyzes meter data, but that also interfaces well into the various installed software platforms. The comments made above for the head end also apply to the MDMS with regard to CIM/GID support and the need for groups such as AMI-Enterprise to develop common requirements and best practices within the utility industry.

Data Integration

Integration of data from the MDMS into the various applications residing within the company is important. A MDMS that collects, stores, analyzes and then selectively provides data to the core software packages can help to avoid massive data flows into existing applications while providing the data necessary for the functionality of those systems. Proper integration will minimize duplication of data storage and allow for a single user interface to run complex systems.

Smart Meter/AMI Summary

Several Utility companies are currently considering AMI / Demand Response / Smart Grid projects that provide a strong link to end user devices, due in part to the Federal Energy Policy Act of 2005. A few of the large Utilities have completed their initial deployments, but these early designs have been quite limited in scope. Some Utilities have started their implementation process for more robust smart grid systems and have completed pilot projects to help prove their design concepts. None of the large Utilities in North America have deployed an AMI / Smart Grid structure that has a complete set of system functionality, but several are in the process of doing so.

There are inherent risks involved in the implementation of the utility to customer interface and associated applications (e.g. smart metering) for due to the immaturity of some the technologies involved and the lack of vendor support for open standards. Vendors are currently working on better solutions that will offer the scalability necessary for larger companies in the future. Utilities will want to

avoid both untested solutions and the possibility of building infrastructure that may quickly become obsolete. The challenge will be to manage the risks by carefully balancing the use of new technologies against the possibilities for obsolescence by applying the key principles of the IntelliGrid Architecture including standards based information exchanges at well-defined points of interoperability.

Appendix C: Evaluating Roadmap Adoption

As noted earlier in this report, periodic review and update of a roadmap is critical to extracting the most value from the effort. The following is a list of questions that we have used to help utilities assess the value obtained from their roadmap efforts and can form the basis for a periodic review. These self assessment questions can also help identify any significant changes that may have occurred in assumptions, regulatory environment, infrastructure and organization that may indicate a more complete refresh of the roadmap is required.

1. The original motivation and objectives for the Roadmap
2. Summary of internal perceptions of the Roadmap project
   - Initial
   - Current
3. Have your original drivers changed
4. Who was the sponsor of the Roadmap project (Dept.)
5. Were the objectives of the Roadmap met?
6. What happened after the Roadmap was complete?
   - Architecture?
   - Business cases?
7. What organizational changes resulted from the Roadmap:
   - Executive oversight
   - Leadership teams?
   - New project teams?
   - Changes in process?
   - Changes in policy?
8. How is the Roadmap used on a recurring basis?
9. Who owns the Roadmap and is responsible for updating it?
10. Are there plans to or have you updated the Roadmap?
11. Are the requirements developed for the Roadmap used periodically?
12. Are any of the methodologies used such as use cases?

13. How well do the different departments work together to identify requirements for new projects?
14. What mechanisms are in place to guide technology investments:
    - Monthly leadership meeting
    - Project meetings and reviews
    - Engagement with industry standards development
    - Governance and policy
15. What technology activities have occurred since the Roadmap (that can be attributed to the Roadmap)?
    - Projects,
    - New plans
    - Implementations
    - Policy changes
    - Standards adoption

The Electric Power Research Institute Inc., (EPRI, www.epri.com) conducts research and development relating to the generation, delivery and use of electricity for the benefit of the public. An independent, nonprofit organization, EPRI brings together its scientists and engineers as well as experts from academia and industry to help address challenges in electricity, including reliability, efficiency, health, safety and the environment. EPRI also provides technology, policy and economic analyses to drive long-range research and development planning, and supports research in emerging technologies. EPRI's members represent more than 90 percent of the electricity generated and delivered in the United States, and international participation extends to 40 countries. EPRI's principal offices and laboratories are located in Palo Alto, Calif.; Charlotte, N.C.; Knoxville, Tenn.; and Lenox, Mass.

Together...Shaping the Future of Electricity

Program:

IntelliGrid Technology

1025470

Electric Power Research Institute
3420 Hillview Avenue, Palo Alto, California 94304-1338 • PO Box 10412, Palo Alto, California 94303-0813 USA
800.313.3774 • 650.855.2121 • askepri@epri.com • www.epri.com