EPRI | ELECTRIC POWER RESEARCH INSTITUTE

Interoperability Robustness Checklist for Metering and Customer Communications

Support For Demand Response and Energy Service Applications

1016268

Interoperability Robustness Checklist for Metering and Customer Communications

Support For Demand Response and Energy Service Applications

1016268

Technical Update, January 2008

EPRI Project Manager

J. Hughes

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

DISCLAIMER OF WARRANTIES AND LIMITATION OF LIABILITIES

THIS DOCUMENT WAS PREPARED BY THE ORGANIZATION(S) NAMED BELOW AS AN ACCOUNT OF WORK SPONSORED OR COSPONSORED BY THE ELECTRIC POWER RESEARCH INSTITUTE, INC. (EPRI). NEITHER EPRI, ANY MEMBER OF EPRI, ANY COSPONSOR, THE ORGANIZATION(S) BELOW, NOR ANY PERSON ACTING ON BEHALF OF ANY OF THEM:

(A) MAKES ANY WARRANTY OR REPRESENTATION WHATSOEVER, EXPRESS OR IMPLIED, (I) WITH RESPECT TO THE USE OF ANY INFORMATION, APPARATUS, METHOD, PROCESS, OR SIMILAR ITEM DISCLOSED IN THIS DOCUMENT, INCLUDING MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, OR (II) THAT SUCH USE DOES NOT INFRINGE ON OR INTERFERE WITH PRIVATELY OWNED RIGHTS, INCLUDING ANY PARTY'S INTELLECTUAL PROPERTY, OR (III) THAT THIS DOCUMENT IS SUITABLE TO ANY PARTICULAR USER'S CIRCUMSTANCE; OR

(B) ASSUMES RESPONSIBILITY FOR ANY DAMAGES OR OTHER LIABILITY WHATSOEVER (INCLUDING ANY CONSEQUENTIAL DAMAGES, EVEN IF EPRI OR ANY EPRI REPRESENTATIVE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES) RESULTING FROM YOUR SELECTION OR USE OF THIS DOCUMENT OR ANY INFORMATION, APPARATUS, METHOD, PROCESS, OR SIMILAR ITEM DISCLOSED IN THIS DOCUMENT.

ORGANIZATION(S) THAT PREPARED THIS DOCUMENT

EnerNex Corporation

Hypertek, Inc.

This is an EPRI Technical Update report. A Technical Update report is intended as an informal report of continuing research, a meeting, or a topical study. It is not a final EPRI technical report.

NOTE

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

Electric Power Research Institute, EPRI, and TOGETHER…SHAPING THE FUTURE OF ELECTRICITY are registered service marks of the Electric Power Research Institute, Inc.

Copyright © 2008 Electric Power Research Institute, Inc. All rights reserved.

CITATIONS

This report was prepared by

EnerNex Corporation
170C Market Place Boulevard
Knoxville, Tennessee 37922-2337

Principal Investigators
Erich W. Gunther
Grant Gilchrest

Hypertek, Inc.
14624 Country Creek Lane
North Potomac, Maryland 20878

Principal Investigators
Dr. Martin Burns
Ronald Pasquarelli

With contributions from Joseph Hughes, Electric Power Research Institute.

This document describes research sponsored by the Electric Power Research Institute (EPRI).

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

Interoperability Robustness Checklist for Metering and Customer Communications: Support For Demand Response and Energy Service Applications. EPRI, Palo Alto, CA: 2008. 1016268.

PRODUCT DESCRIPTION

This report provides a strategic framework and a simplified checklist for the development and design of future dynamic customer-to-utility and customer-to-service-provider systems such as advanced metering and demand response. This framework and checklist is intended to help utilities ensure the technology they are deploying is flexible and robust enough to avoid premature obsolescence, vendor "lock-in," and/or system-wide "forklift" upgrades.

Results & Findings

This framework for the development of customer communications systems infrastructure is presented hierarchically, starting with a set of high-level principles for achieving flexibility and robustness, followed by some key requirements for implementing each principle and a checklist for evaluating whether a given system satisfies the requirements. The report concludes with a detailed example of a system that could be designed with infrastructure that is available today.

The strategies described in the report include both the adoption of developing industry technologies and the use and application of the emerging methods and processes necessary to adequately specify, document, and manage systems over their life cycle. The checklist identifies some of the key gaps in the available technology that must be filled to achieve robust systems.

Challenges & Objectives

Utilities are about to specify and install massively scaled customer communication systems on an unprecedented level. These systems are extremely large and push the limits of what systems engineering can currently develop, design, and deploy. The checklist in this report is a simplified version of what industry-level architecture needs to accomplish. It provides guidelines for the development, procurement, and life-cycle management of interoperable communication networks and intelligent equipment. While the industry has developed significant open-systems-based infrastructures that can and should be used, there are also several remaining issues that have yet to achieve industry consensus and/or are clearly in need of further development. The main driver for this work is in recognition that systems are presently being specified even though key elements of infrastructure are missing.

Applications, Values & Use

Utilities currently specifying systems can use this checklist to augment their own decision-making processes. The checklist is not exhaustive; and utilities will need to develop their own sets of requirements; but the checklist can encourage a broader view of the development of advanced metering and customer communication systems. The report discusses the thinking that lies behind the specification process and provides general guidance on the content of the infrastructure that is illustrated by an example from important emerging open industry standards.

EPRI Perspective

There is an urgent need to put technologies into place that will make possible dynamic customer applications such as advanced metering, demand response, and the integration of metering and outage management. While several standards organizations have done good work in supporting this effort, their work is not fully mature and industry level infrastructure also requires additional development. This project can provide some of the strategies by which utilities could design and deploy systems in the near term that have some ability to meet future requirements as needs

change and the balance of the infrastructures mature. This checklist provides some direction toward a vendor neutral open standards based infrastructure and identifies where additional work is needed.

Approach

The team worked from experience with ongoing utility and standards based infrastructure development projects currently under way across the relevant industries. The team's approach included examining the key elements at each level of a design hierarchy and noting the strategies that could be adopted as part of a longer-term robust approach to customer dynamic systems.

Keywords

Customer metering
Data communications
Architecture
Object model
Standards
Harmonization
Interoperability

CONTENTS

LIST OF FIGURES

LIST OF TABLES

1
INTRODUCTION

Future systems supporting metering, demand response, and customer communications will need to be flexible and useful for years after they are initially deployed. Utilities prefer to deploy new technology with a minimum of risk related to premature obsolescence.

This project worked from existing industry use cases to develop a set of guidelines that if followed will enable a robust deployment of interoperable and upgradeable equipment. This report also notes where additional research and development is necessary to ensure future systems will be able to meet these design requirements.

The opportunity is at hand. If a large installed base of utilities begin requesting compliance with the interoperability and upgradeability guidelines outlined in this report, the deployment of advanced metering, demand response and other customer-centric systems could be accelerated. The opportunity for creating industry-level standards at key interfaces will provide a significant stimulus for a new generation of applications. If minimum levels of integration and flexibility are not effectively established, the industry runs the risk that a new set of stranded assets will be created that are not changeable and cannot be integrated with future systems or new technology.

Objectives

The following represent the objectives of this checklist

1. Define a framework for processes and an approach for specifying, developing, deploying and managing technologies for metering, customer communications and energy service functions.
2. Define a framework for applying standards and open systems to the development of advanced customer communication systems.
3. Develop a requirements checklist for both methods and content that can be used to guide decisions and evaluate critical elements of the infrastructure
4. Define elements of the checklist that are missing and need further development by key industries.
5. Build upon relevant prior work by the industry in all the key areas including requirements development, standards and technical interoperability agreements and proposed best practices by closely related industries

Scope

The applications scope of this checklist is focused on the set of advanced applications surrounding next generation customer communications including integration with customer owned equipment. The scope includes customer communications integrated with industry operations including:

- ISO/RTO operations

- T&D operations,
- Customer Service
- Billing Services
- Energy Services

The scope is limited to the applications of T&D and Generation operations that would interact with customer operations.

The scope of this checklist cuts across several industries and technical disciplines including but not limited to the following: Telecommunications, Electrical Engineering, Software Engineering, Systems Engineering and System Architecture Development.

Approach

This report is organized as a hierarchical set of tools describing how to achieve interoperability and technological flexibility starting with a philosophical approach and progressing to specific examples.

- Section 2: A description of a high-level, "no regrets" approach to systems development.
- Section 3: A description of how to achieve "no regrets" design using this document and the EPRI IntelliGrid systems design methodology.
- Section 4 is organized according to three different levels of specification:
    - Design principles agreed upon by various organizations currently addressing AMI, including UtilityAMI and OpenAMI. These are general principles such as "Security" or "Ease of use".
    - Requirements for meeting these design principles. These are specific tasks that the system must perform, e.g. "Log significant events" is a requirement that must be met under "Security".
    - The checklist items necessary for verifying that an implementation is meeting the requirements, e.g. "Does the system provide audit logs of all configuration changes, including the following…."
- Section 5 describes a specific example set of technologies that could be used to meet this checklist.

2
SYSTEM INTEGRATION WITH "NO REGRETS"

The contents of this document are intended to help utilities develop advanced metering and demand response systems in a top-down, requirements-driven manner that will permit the system to be easily upgraded and prevent costly surprises later on. One term for this kind of development is "No Regrets" design. This section presents two brief scenarios to illustrate the "No Regrets" concept.

How It's Usually Done

Most utilities tend to develop intelligent systems in isolation, with unique interfaces determined by the needs of the particular project that was funded at the time. For instance, as illustrated in Figure 2-1, a utility may decide to participate in energy markets; it may also implement automatic meter reading (AMR). However, it's often the case that neither project is developed with the other in mind. If the utility decides to try to integrate these functions, this integration is done in a "one-off" or project-oriented manner. This of course costs significant money to implement.

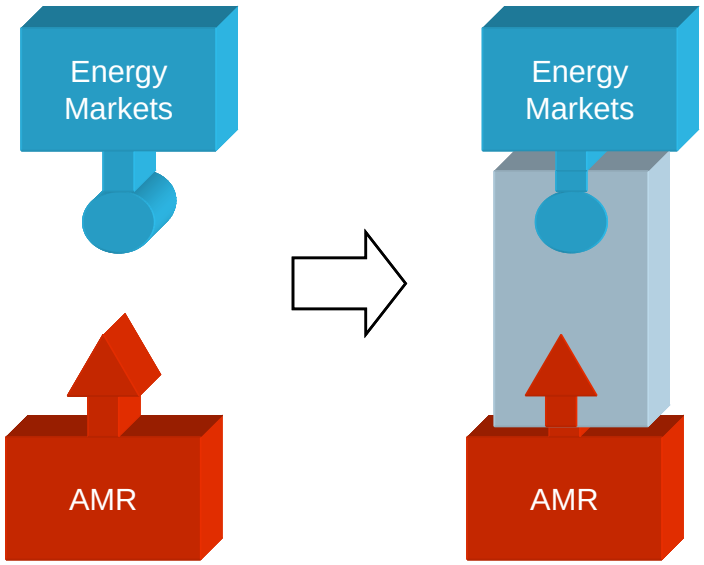

Figure 2-1
Single Project, "One-Off" Integration

The next time a similar integration project is needed, the utility must first spend money to make the original integration expandable. For instance, with AMR in place and integrated with energy markets, a utility may decide to develop demand response programs and integrate AMR with distribution automation and outage management. However, in this example, the original development did not define interfaces for such functions. The utility must therefore perform a more complicated integration phase to link the new systems into the old one. As illustrated in

Figure 2-2, the resulting interface between the new systems and the existing ones is often fragile and inflexible.

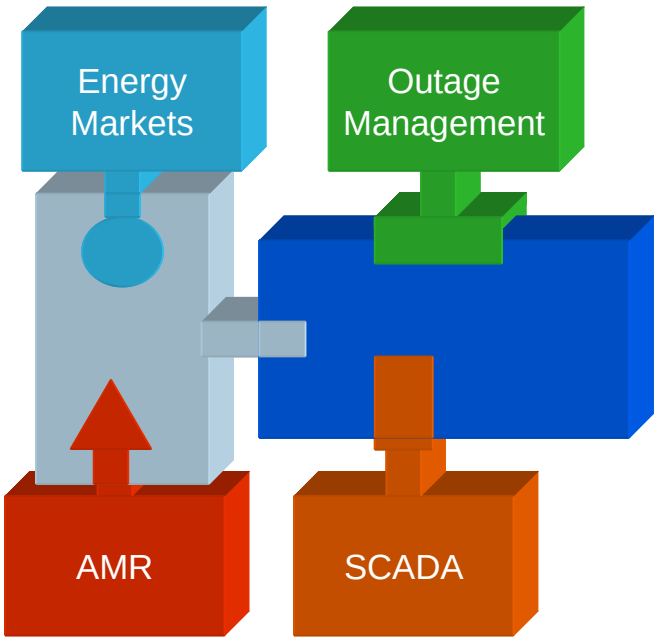

Figure 2-2
Expanding on a One-Time Integration Project

This pattern of development typically repeats, each time costing more money and becoming more awkward technologically, until finally, some flaw is found that will prevent the system from expanding. In hindsight, it becomes obvious that some major feature or service should have been designed into the system from the beginning. Such unexpected issues may cause nearly catastrophic costs, or simply prevent any further expansion. As illustrated in Figure 2-3, the sudden realization of the need for network security is often one such unexpected issue. It is often impossible, or at least extremely costly, to retrofit such system-wide concerns.

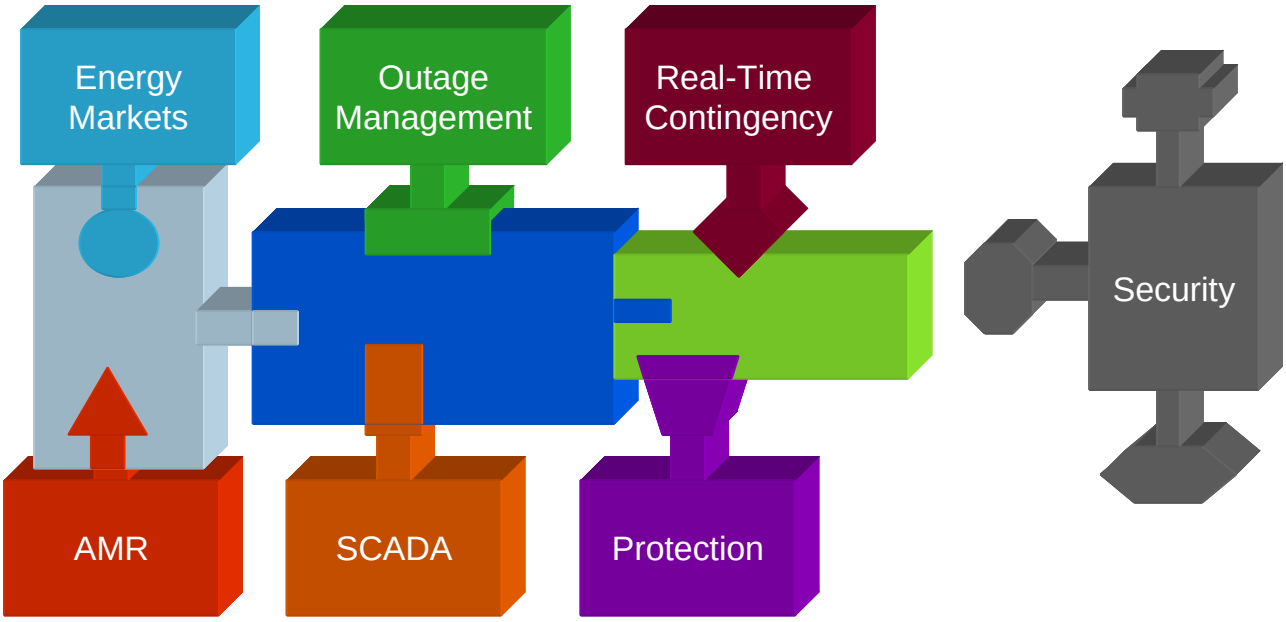

Figure 2-3
"One-off" Integration Unable to Retrofit System-Wide Concerns

Doing it the "Right Way"

The right way to develop an intelligent system is from the top down. By defining standard interfaces first, and planning for the future, high costs can be prevented later. System-wide concerns, such as security, network management, and data management can be built into the architecture from the beginning.

Figure 2-4 illustrates how the previous scenario shown in Figure 2-1 would be implemented using this methodology. The interfaces are defined first, allowing for the system-wide issues mentioned above. Then new applications such as AMR and the use of energy markets can build directly on to the standard interfaces.

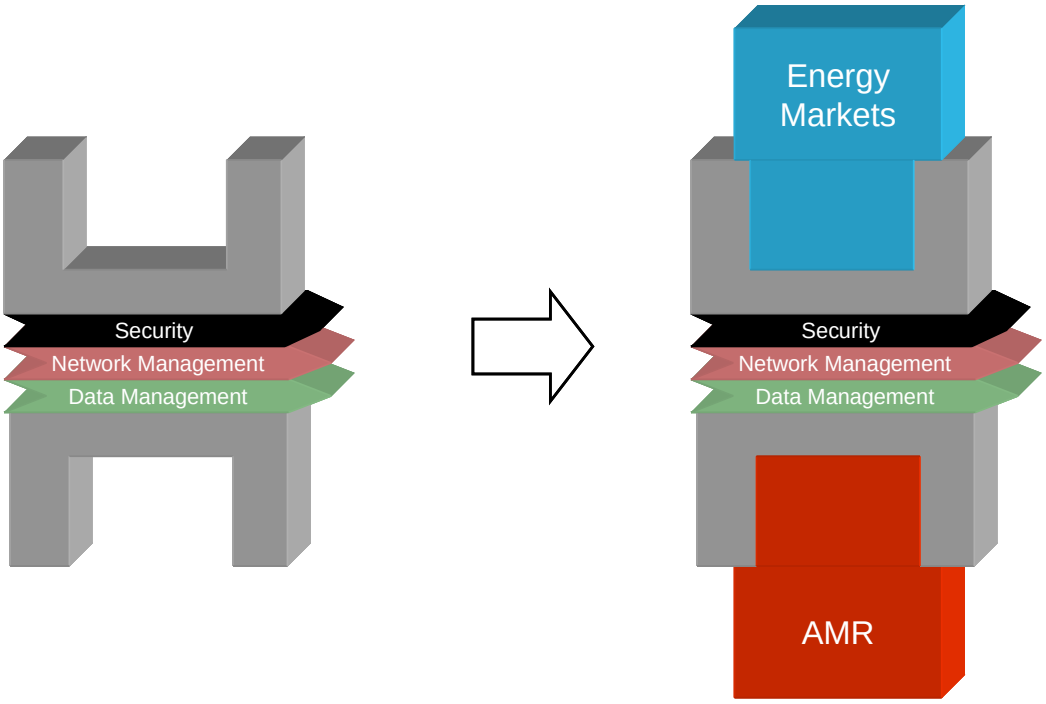

Figure 2-4
Building an Integration Architecture Framework First

Figure 2-5 illustrates what happens when further phases of integration are needed. The work done in the first phase can be re-used for subsequent expansion, eliminating waste.

Older "legacy" systems – SCADA and outage management shown here as examples – can be integrated at much lower costs than a "one-off" scenario. Often, standardized "adaptors" or "gateways" for legacy interfaces have already been developed by other organizations. Even if such adaptors are not already available, it is less costly to adapt a system once to a standardized interface, than many times to several different custom applications as the system evolves.

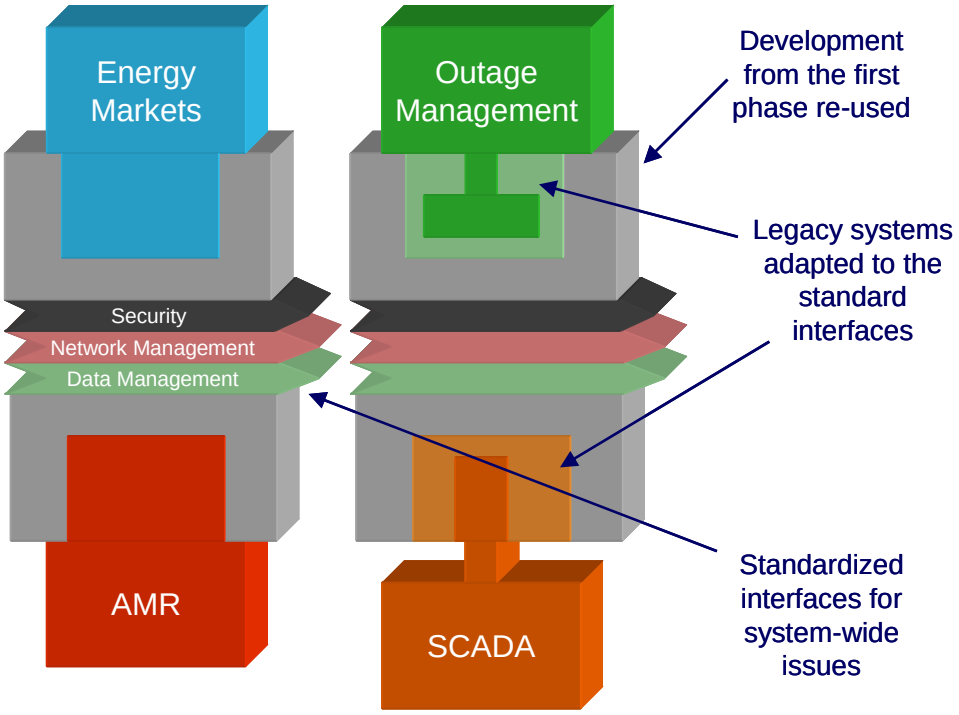

Figure 2-5
Expansion Using an Integration Architecture Framework

Figure 2-6 shows how a "no regrets" system continues to expand in a flexible manner. The costs of properly architected systems integration do not increase significantly with time, and the benefits will increase. This situation is the exact opposite of a system integrated in the "one-off" manner. In such traditional systems, costs only increase, and benefits are sometimes lost.

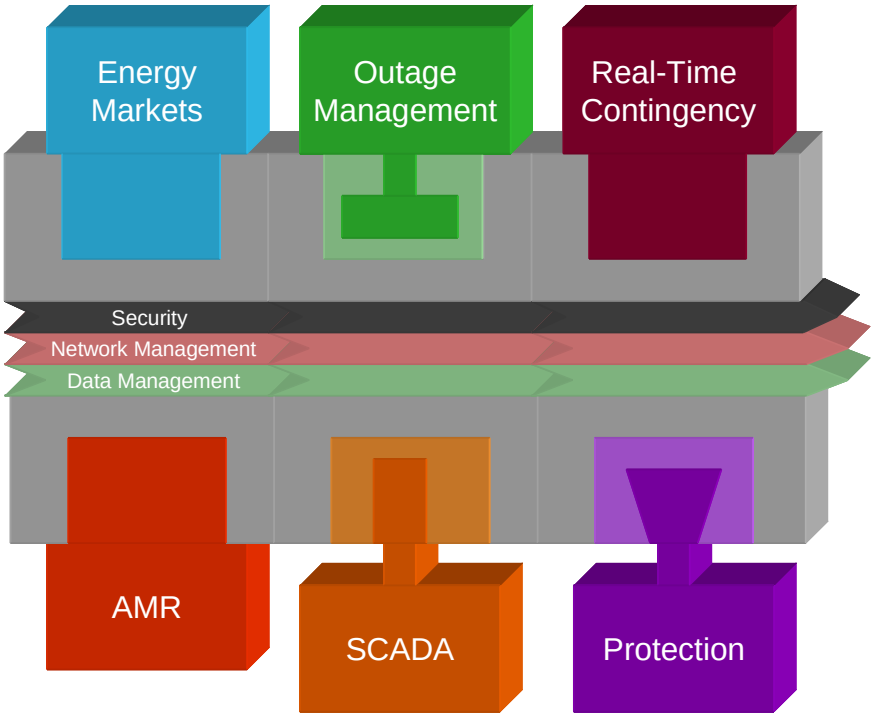

Figure 2-6
System Continues to Expand with No Regrets

In summary, a “no regrets”, top-down design permits capital investment to be re-used, eliminates redundant effort and last-minute retrofits, and prevents “forklift upgrades” of large numbers of systems. Vital system-wide capabilities, like security, come standard instead of needing to be added on afterwards at high cost.

The greatest benefit of a “no regrets” philosophy, however, is that it prepares the system for unforeseen circumstances. Technology, applications, and organizations are always changing, and defining an open, standard, flexible architecture ahead of time means being able to adapt to these changes.

3
USING THIS CHECKLIST

This section describes how to use this document and the checklist it contains as a part of the IntelliGrid development methodology.

The IntelliGrid Methodology

The EPRI IntelliGrid initiative has developed a methodology based on best practices in systems engineering to help utilities follow the "no regrets" design principle. Figure 3-1 illustrates this methodology. The checklist in this document is a tool for facilitating this process at the Requirements level.

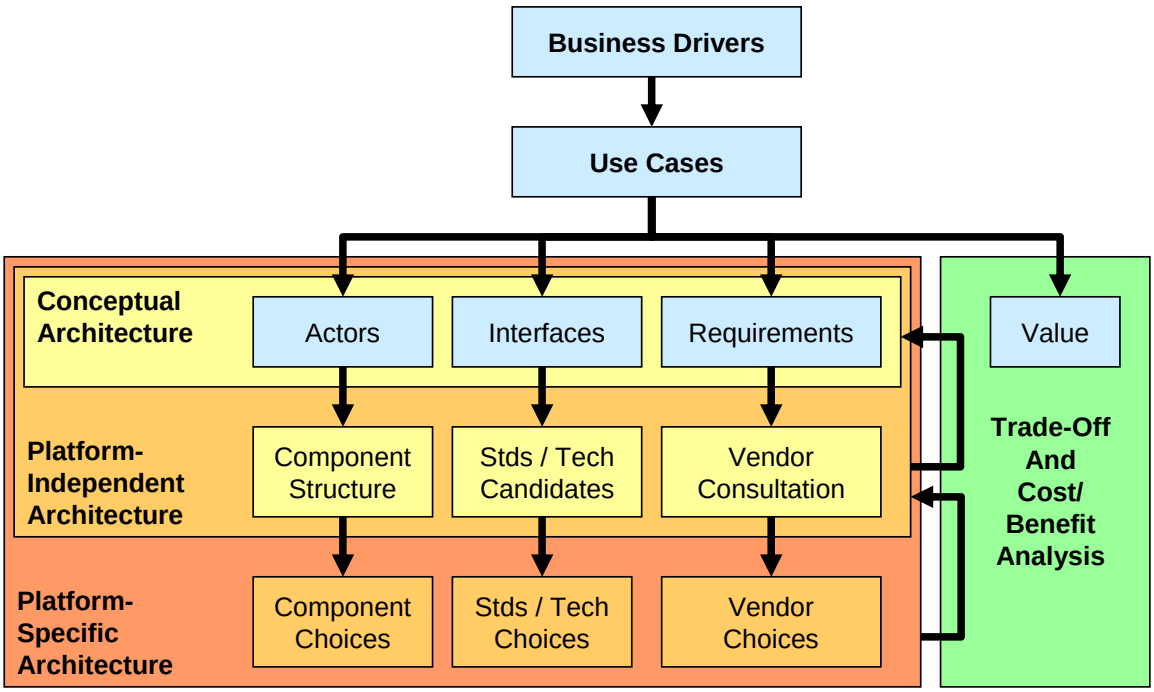

Figure 3-1
IntelliGrid Development Methodology

The IntelliGrid methodology consists of the following steps:

1. Executives determine what functions the system needs to perform based on **business drivers.**
2. The organization forms cross-functional teams to develop a set of **use cases**, which are complete "stories" describing the steps in which the system will be used from end-to-end.
3. From the use cases, an architecture team defines idealized **actors**, **interfaces**, and **requirements** for implementing the use cases. This is known as a **conceptual**

architecture. The team also defines the qualitative **business value** of each use case and requirement.

4. Design teams determine what is practically feasible by investigating which **open standards and technologies** are valid candidates for implementing the interfaces, what **vendor offerings** are available to meet the requirements, and how vendors are typically grouping the conceptual actors into physical components. This list of possibilities is the **platform-independent architecture**.
5. Business teams compare what's technologically available to the conceptual ideal and to the business value of each requirement, resulting in a **cost-benefit analysis** and a series of engineering **trade-offs**. This typically results in modification or elimination of some of the original requirements. It may also identify new technologies that must be developed.
6. Finally, the utility chooses among the available components, standards, technologies and vendors to implement and deploy this particular project. This is known as the **platform-specific architecture.** Additional trade-offs and re-evaluation of requirements may also occur at this stage.

Industry Contributions

Several prominent industry organizations have already gone down this path. These organizations have been actively collaborating to create a reasonably uniform set of use cases, as illustrated in Figure 3-2. Based on these use cases, these organizations have developed their own sets of requirements for Advanced Metering Infrastructure.

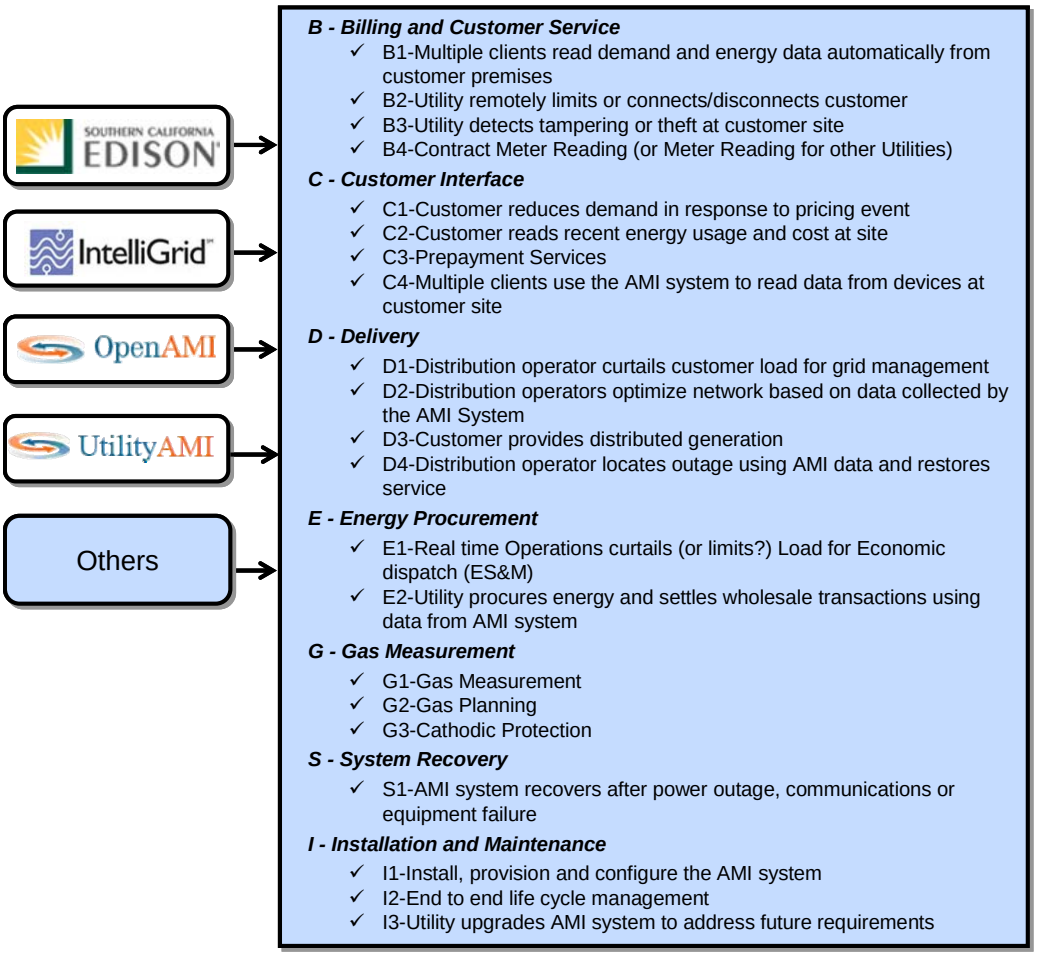

Figure 3-2
Example List of Use Cases and the Organizations Producing Them

A complete summary of the AMI related use cases being consolidated by OpenAMI from those contributed by IntelliGrid, Southern California Edison, Consumers Energy, San Diego Gas & Electric, and others. See the reference in Appendix II for *OpenAMI*.

Role of this Document

As illustrated in Figure 3-3, some of the system requirements developed from these use cases are specific to particular projects and applications. However, others are universal principles that should be applied in every case.

This document provides a summary of those universal principles including a checklist with which to evaluate whether these principles have been met, and an example set of technology choices that exemplify these principles.

The purpose of this document is therefore to summarize the AMI requirements work that has been already done and make it available to utilities beginning to develop their own AMIs.

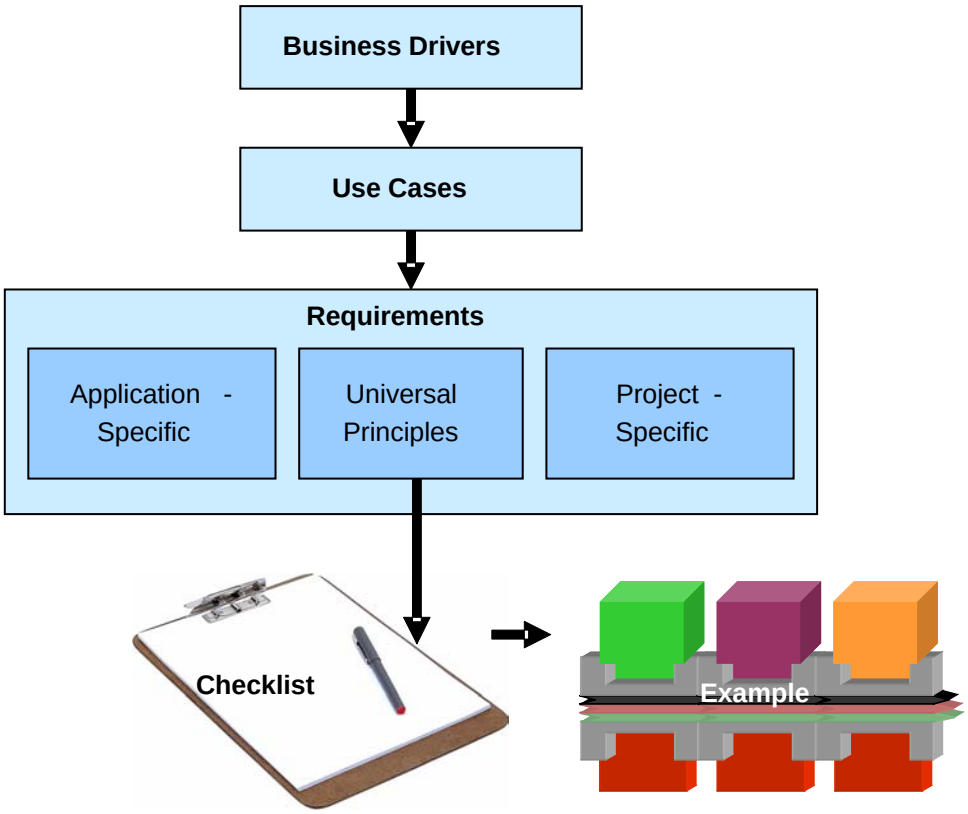

Figure 3-3
Derivation of this Checklist and Guideline Example

4
REQUIREMENTS AND CHECKLISTS

This section contains requirements and checklists suitable for evaluating a design concept or specific proposal for an advanced metering and/or demand responsive infrastructure project. It is organized based on eight key design principles identified by the industry OpenAMI task force. In addition, two new categories are added to facilitate life cycle management of deployed systems – specifically manageability and extensibility.

It is not mandatory that all systems answer "Yes" to all questions on the checklist. However, better (i.e. more extensible, interoperable systems) systems will be able to provide more "Yes" answers than lesser capable systems. It is assumed that the information necessary to answer these questions can be obtained directly from within the AMI or DR system design proposal documentation or by forwarding the questions on to an appropriate party who would respond and indicate where in the proposal each issue is addressed in more detail.

In the discussions that follow, a "consumer" is given to mean either an individual consumer or an agent representing multiple consumers.

Each subsection below summarizes the requirements recommended for the topic principle. Following these requirements summaries is a set of "checklist" questions that can be asked to assess the correspondence of product offerings and standards to these requirements.

Entities that will be the owners/operators of an AMI or DR system should use the checklists to evaluate the candidate project or technology using the following procedure:

1. Determine what stage of evolution towards open systems that this particular project is in, and identify those checklist items for which an answer of "in the future" is permitted.
2. Determine the response of the vendor / system designer to the checklist. This may be done in one of three ways:
    a. Issue the checklist to vendors along with the bid/RFI package
    b. Issue selected questions from the checklist to vendors after examining their bid/RFI responses
    c. Issue the checklist to vendors as a separate document before or after the formal bid/RFI issuance.
3. Based on the vendors' responses, determine what the vendor believes to be the boundaries of the AMI/DR system. Refer to section 0 for a discussion of system boundaries.
4. Resolve any disputes regarding the system boundary and the responsibilities of the vendor in fulfilling the items on checklist.

5. Compare the responses of multiple vendors to the checklist.
6. Select vendors / system designs who:
    a. ***Provided the most "Yes" answers.***
    b. Provided the most "In the future" answers where those were permitted.
    c. Define the boundaries of the AMI/DR system in a manner consistent with the project goals.
    d. Seem to most agree with the idea of evolution to open systems, well defined points of interoperability and multi-vendor implementations.
    e. Provide milestones for evolution consistent with this project.

Shareability

The infrastructure uses shared resources which offer economies of scale, minimize duplicative efforts, and if appropriately organized, encourage the introduction of competing innovative solutions.

Requirements

Widen the System Boundary

One of the first actions that the OpenAMI task force took was to clearly identify the boundary of what was considered to be "the AMI System".

There are functions that are vital to the success of AMI, and in particular, demand-response systems, that have not traditionally been the responsibility of AMI vendors. Some examples of such functions are those that deal with:

- Supplying energy usage and cost to consumers
- Notifying consumers of tariff changes
- Permitting more frequent billing
- Permitting access to data by metering service providers

A traditional AMR vendor would typically say that such functions are the responsibility of some domain other than the AMI, e.g. the billing department, the customer service department, perhaps even the regulator or the Independent System Operator (ISO). Some more specialized vendors might draw the boundary still smaller, to the metering systems only, or even to just the metering equipment itself.

The checklist in this document takes a wider view that while the AMI may be contained within the boundary identified in utility domain, the a utility must specify not only the AMI but how it interacts with consumers and works in concert with other domains.

Figure 4-1 illustrates a comprehensive set of components of an AMI and its users or clients. Although the boxes with rounded corners are typically those items considered to be within the

AMI boundary, it is important that the AMI be able to share data and resources with each of the other groups shown.

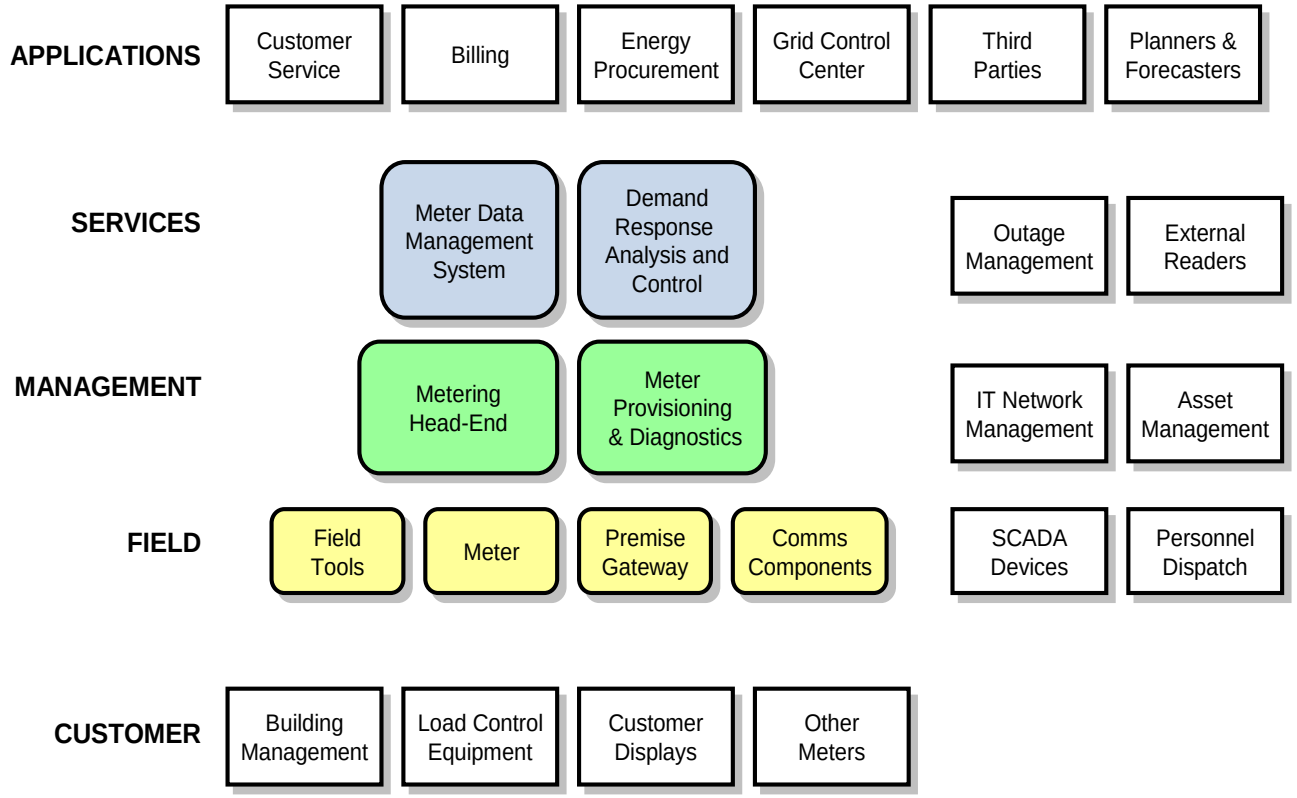

Figure 4-1
AMI Components and Clients

Share Data with Multiple Clients Simultaneously

An AMI should be able to share data with any number of client applications at the same time. In the traditional AMR model, metering data was only available through the billing system, and only to a specific set of clients, each of which would have to have a customized interface. This was an example of "one-off" integration.

A common solution to this requirement is the introduction of a Meter Data Management System (MDMS), as illustrated in Figure 4-1, which serves validated data to various client applications. In addition, the metering "head-end" might also serve non-validated or "raw" data to selected clients such as third-party energy aggregators, meter service companies, outage management, or other utilities.

Provide a Common Set of Shared Data

A well-designed AMI should be able to share any of its data with any client using a standardized interface. If the interface cannot be an actual international standard (see section 0), there should at least be a well-defined set of shared data which any client can access. A proposed bare minimum set is shown in the checklist.

Share Infrastructure with Other Utilities

Sharing communications and data management infrastructure with other utilities to reduce costs is in the best interests of both consumers (as ratepayers) and utilities. An AMI should be flexible enough to permit the following functions, even if they are not included in the first deployment of the system:

- Share electrical metering information with third parties
- Permit gas or water utilities to read their meters using the AMI
- Make use of already existing communications networks

Checklist

Is at least the following information available to all authorized users?

a) Energy usage for each consumer?	Y ☐ N ☐
b) Energy costs for each consumer over each metering interval?	Y ☐ N ☐
c) Aggregated energy usage for large numbers of consumers?	Y ☐ N ☐
d) Audit trails of changes to tariffs, configuration, software and firmware?	Y ☐ N ☐
e) Audit trails of failures in the system?	Y ☐ N ☐
f) Records of which meters responded to the most recent read?	Y ☐ N ☐

Is the information from the system available to each of the following users, simultaneously, if authorized?

a) The designated billing system?	Y ☐ N ☐
b) Auditors and regulators?	Y ☐ N ☐
c) Rate analysis and design systems?	Y ☐ N ☐
d) Energy management and control systems?	Y ☐ N ☐
e) Distribution management and control systems?	Y ☐ N ☐
f) Load management systems?	Y ☐ N ☐
g) Utility network engineers, planners and forecasters?	Y ☐ N ☐
h) Meter service companies?	Y ☐ N ☐
i) Outage management systems?	Y ☐ N ☐
j) Complaint resolution systems?	Y ☐ N ☐
k) The System Operator (e.g. NYISO, CAISO, ISO-NE)?	Y ☐ N ☐
l) Distributed generation providers?	Y ☐ N ☐

m) Customer service representatives?	Y ☐ N ☐
n) Consumer equipment such as thermostats and building management systems?	Y ☐ N ☐
o) Energy procurement personnel and energy marketers?	Y ☐ N ☐
p) Work management systems and field personnel?	Y ☐ N ☐
q) Other utilities?	Y ☐ N ☐

Does the system use a communications network that is already in place, e.g. Cable, DSL, Cellular, other utilities?	Y ☐ N ☐
Does the system permit other utilities such as gas and water to access their meters through the AMI?	Y ☐ N ☐

Ubiquity

Users can readily take advantage of the infrastructure and what it provides.

Requirements

Serve as Many Consumers as Possible

For maximum effectiveness of demand response programs, either for grid reliability, economic dispatch, or for deferring generation, it is important that as many consumers be able to participate as possible. Many of the other benefits of deploying an AMI also increase when the percentage of customers served increases. Geographic location or class of service should not be a barrier to the deployment of an AMI to any particular customer, or to their participation in any of the programs that AMI enables.

Enable Smart Customer Premises Equipment

One of the major benefits of AMI is that it permits utilities and consumers to work in a partnership to improve energy efficiency and reliability. Demand response, distributed generation, and many of the other programs enabled by AMI, work better when the AMI can exchange information with customer premise equipment such as thermostats, pool pumps, appliances and building management systems. An AMI should either communicate with such equipment, or be easily upgraded to do so. The most common way discussed to perform this communication is by way of a local area network connected to the meter, but there are a other mechanisms through which it can occur.

Use Multiple Physical Communications Technologies

In order to increase the number of customers served, an AMI should be able to use a variety of qualified physical communications technologies to reach the consumer (e.g. centralized wireless, power line carrier). Keep in mind that any technologies used should be "qualified" by meeting

the utility and industry requirements for not only supporting the applications but also management and security policy support. The AMI should be able to support any of these technologies simultaneously. In this way, consumers are not prevented from taking advantage of the system, and the utility continues to receive the benefits, even though the consumer may not be reachable using a particular technology.

Checklist

Can *all* consumers (residential, agricultural, commercial and industrial) within the service territory do the following?

a) Be connected to the system?	Y ☐ N ☐
b) Be notified of tariff changes, including critical peak pricing?	Y ☐ N ☐
c) Access their energy usage and cost information?	Y ☐ N ☐
d) Receive load control signals?	Y ☐ N ☐

If there are consumers who are not served by the system, are these exceptions due only to truly extreme physical, geographic or economic conditions?	Y ☐ N ☐
Will the system permit selected consumers to provide generation, i.e. be able to perform "net metering"?	Y ☐ N ☐
Can consumers be configured for net metering service remotely?	Y ☐ N ☐
Is the system able to detect and report when a consumer is generating more power than they are consuming?	Y ☐ N ☐
Can the system be upgraded to support distributed generation in some fashion without site visits?	Y ☐ N ☐
Does the system have the ability to communicate with customer premise equipment such as thermostats or building management systems?	Y ☐ N☐
Can the system use different technologies to reach different consumers?	Y ☐ N ☐

Integrity

The infrastructure operates at a high level of availability, performance and reliability.

Requirements

Provide Measurable High Availability

High availability is an inherent requirement of any utility communications system, and an AMI is no exception. Although billing systems are accustomed to dealing with data that is not

available and therefore perform estimates of energy usage, demand response programs are much more sensitive to lack of availability. Grid reliability demand response events, in particular, are much more effective if communications is available to all the requested sites.

Experience has shown that a critical part of the business case for AMI is that the system be highly available and reliable. A matter of less than a percentage point can make the difference between particular AMI functions providing a benefit or not.

The availability capabilities of various systems may vary widely, but an important factor when deploying AMI is to ensure that availability and other performance targets are published and contractually agreed upon, and then measured in order to determine if the contract is being met. A few of the key factors in achieving availability are discussed in this section; others are discussed in the context of manageability in section 4.10.

Provide Measurable High Reliability

It is important to note that availability and reliability are not the same quantity and should be specified and measured separately.

Provide Alternate Communications Paths

One of the most basic methods to ensure availability is to provide alternate communications paths. Redundancy of communications paths may be required for AMI systems that participate in mission critical applications. An AMI should at a minimum provide mechanisms for identifying failed paths and manually selecting alternate paths.

Automatically Re-Route Communications

Ideally, an AMI should automatically select alternate communications paths based on periodic monitoring of the communications links. Some technologies support this capability inherently.

Operate During Power Outages

Communications portions of the AMI system used for outage management should operate during power outages, to better distinguish between true outages and losses of communication due to device failure. This is even more critical if the AMI is used to improve the effectiveness of an Outage Management System (OMS). Because of the hierarchical nature of many AMI communications systems, it is possible that the failure of a data collector could incorrectly be identified as a large power outage because of loss of communication with a large number of meters.

The issue of whether meters should be supplied with alternate power sources or support “last gasp” messaging when they are participating in outage management or communications networks is controversial. This issue must be resolved at design time. However, it is clear that the communications network, at least, needs to continue operation during outages.

Take Advantage of the Potential for Interval Metering

As with availability and reliability, basic performance of an AMI in automatic meter reading can vary widely depending on the data being read from the meters and the other functions being performed by the system. However, it is clear that the expense of deploying AMI does not provide a benefit if it is used only to automate monthly reads, or even daily reads. AMIs are

therefore almost always deployed along with interval metering in order to enable Time of Use (TOU), Critical Peak Pricing (CPP) and other advanced tariffs.

With interval metering, it is important to note the difference between how often the data is *recorded* versus how often it is *reported* or read. As shown in the checklist, a minimum AMI system should be able to record data at least once per hour and retrieve the complete set of data at least once per day. Many systems are capable of better performance, and requiring 15-minute recording intervals from selected customers is considered quite common for establishing load profiles.

Notify Consumers Promptly of Upcoming Events

When deploying demand response systems, a critical element is the ability to inform consumers when they will have choices available. Often this notification can be performed through the AMI itself, perhaps communicating to customer premise equipment like thermostats. Whether notification is performed through the AMI itself or not, the notification mechanism must be part of the demand response deployment, and must be considered as part of the system's performance targets.

Checklist

Does the system have published targets for availability, performance and reliability?	Y ☐ N ☐
Does the system meet its published targets for availability, performance and reliability?	Y ☐ N ☐
Can all equipment in the system continue operation during a power failure?	Y ☐ N ☐
Is there more than one communications path to every consumer site?	Y ☐ N ☐
Can the system select alternate communications paths automatically?	Y ☐ N ☐
Can all meters in the system be read within a specified time?	Y ☐ N ☐
Can data from every consumer meter be recorded at specified intervals?	Y ☐ N ☐
Can data from selected groups of consumers be recorded at specified intervals?	Y ☐ N ☐
Is there provision for selected meters to be recorded at a specified minimum framework of time intervals?	Y ☐ N ☐
Are Energy Service Providers and consumers automatically notified when a regulator makes a tariff change?	Y ☐ N ☐
Is a consumer automatically notified when a rate change is offered?	Y ☐ N ☐
Can all consumers be notified of a critical peak within a day prior to the peak?	Y ☐ N ☐
Can selected consumers be notified of a critical peak within a specified time of the peak?	Y ☐ N ☐

Can the Energy Service Provider be certain that all consumers have received notice of an upcoming tariff change or critical peak, sufficiently prior to the event?	Y ☐ N ☐

Ease of use

There are logical and consistent (preferably intuitive) rules and procedures for the infrastructure's use and management.

Requirements

Maximize the Information Consumers Know About their Energy Usage

It has been shown in studies that the more information a consumer knows about their energy usage and rate information, the more successful a demand response program will be. For the consumer to become a partner in energy efficiency and for utility operations to be effectively linked with markets, is essential that consumers become familiar with the effect their behavior has on the cost of electricity.

Consumers should be able to view their energy usage and its estimated cost as soon after measurement as possible; ideally in the following recording interval, but at a minimum by the next day.

The other critical piece of information a consumer must know is when a demand response event (such as a critical peak price day) is underway. Without the consumer knowing this information, the event cannot be effective.

Maximize the Number of Ways a Consumer Can See their Data

There are a variety of methods that can be integrated with an AMI to provide consumers with the information discussed in the previous section. These may include:

- Meter display
- Customer equipment (e.g. thermostat) display
- Web site
- Automatic phone messages
- Email
- Newspaper or other news media
- Monthly bill

If more methods can be used, demand response programs will be more effective, since different people prefer to get their news from different sources.

Minimize the Actions a Consumer Must Take to Participate

Although consumers need to understand the effects of their behavior on their electricity bill, many consumers are not present on their own premises during peak demand periods, and the highest-usage activities (heating, cooling, pool pumps) are typically automatically controlled. Therefore demand response programs are more successful if participation can take place automatically. The most common methods for doing so are, for instance:

- Using thermostats programmed to reduce load based on real-time rate information.
- Controlling consumer equipment directly through direct wiring or a local area network.
- Disconnecting consumers' service in emergencies through integrated switches in the meter.

Encourage the Consumer to Feel in Control of Their Energy Usage

Other factors affecting consumer participation in demand response have to do with the design of the program; for instance:

- Whether consumers must enroll in the program or are considered enrolled by default
- Whether consumers can "opt in" or "opt out" of a particular demand response event

It has been shown that consumers are more likely to participate if they feel in control of their energy usage. Many programs can be designed to provide consumers with a choice without affecting the technology of the AMI. However, some demand response options require support from the meter and communications system to implement. These options include:

- Load limiting programs, in which the meter automatically disconnects the consumer's service if it exceeds a preset threshold during a demand response event.
- Override buttons on the meter or consumer equipment, that prevent service from being disconnected during certain classes of events.
- Prepayment programs, in which consumers can see on their meter or consumer equipment their remaining account balance.

If the utility intends to deploy any of these types of programs as part of initial deployment or in the future, system engineers must ensure that the AMI is capable of being cost-effectively upgraded to support such features.

Checklist

Can a consumer view their energy use for the previous day?	Y ☐ N ☐
Can a consumer view their energy cost for the previous day?	Y ☐ N ☐
Can selected customers be upgraded to see their energy usage and cost data on a more frequent basis, e.g. hourly?	Y ☐ N ☐
Is it clear from the information available to the consumer what impact their energy usage has on their energy costs (for instance, can they see a daily load curve or similar tool)?	Y ☐ N ☐

Can a consumer tell when a critical peak price or other demand response event is in effect?	Y ☐ N ☐
Can consumer equipment be notified automatically when a demand response event is in progress?	Y ☐ N ☐
Can a consumer participate in a demand response program without having to actively respond to each rate change or other event?	Y ☐ N ☐
Can a consumer tell what rate is in effect at any time?	Y ☐ N ☐
Can a consumer use multiple methods to learn about rate choices, energy usage and cost (e.g. phone, internet, newspaper, local display)?	Y ☐ N ☐
Do consumers have a choice to participate or not participate in demand response programs?	Y ☐ N ☐
Can consumers actively indicate participation in demand response through the AMI, or can it be cost-effectively upgraded to do so?	Y ☐ N ☐
Does the system permit prepayment or can it be cost-effectively upgraded to permit prepayment?	Y ☐ N ☐

Cost effectiveness

The value provided is consistent with capital and operational cost.

Requirements

Use and Re-Use Two-Way Networks

One of the chief arguments against a truly open AMI system has been that many of the features of an open system require an expensive two-way communications network. A properly designed AMI system can be independent of whether it is implemented on a one-way or two-way network. However, if a two-way network really is required, there are ways to mitigate the cost. Utilities should:

- Require that vendors use industry standards based technologies that make it possible to re-use existing two-way networks, such as cable, Digital Subscriber Line, cellular telephony, and two-way paging.
- Investigate the use of emerging commercial standards such as wireless wide-area networks that will come down in cost as they are deployed for non-utility use.
- Start by specifying and using separate one-way networks, but ensure vendors base them on a common design so they can be linked together when two-way networks become more common.

Minimize Site Visits

As noted in Appendix I, one of the key benefits of an AMI arises from reduction in labor when site visits are no longer necessary for meter reading, maintenance, or account changes. One key feature that has been shown to greatly improve the business case for AMI is the ability to connect or disconnect service remotely.

Permit Remote Upgrades

The business cases developed for AMI by several different utilities clearly show that automatic meter reading by itself is unlikely to pay for the cost of deploying an AMI. The ability to upgrade a system remotely to support new features that may reduce cost or improve revenue is therefore critical to an AMI from its initial deployment onward. The checklist shows a few of the features that should be remotely upgradeable. Of particular interest is the ability to change technologies or communications networks.

Checklist

Can the system be deployed to millions of consumer sites economically?	Y ☐ N ☐
Can the following information be changed without any visits to consumer sites?	
The selection of a rate?	*Y* ☐ *N* ☐
The definition of rate structures (including selection of flat rate vs. CPP event vs. periodic, number of periods, start and stop time for each period, and rate for each period)?	*Y* ☐ *N* ☐
The software or firmware for all equipment in the system?	*Y* ☐ *N* ☐
Security parameters, credentials, and algorithms for all equipment?	*Y* ☐ *N* ☐
The frequency of formal billing for each consumer?	*Y* ☐ *N* ☐
The frequency of access to energy usage and cost information for each consumer?	*Y* ☐ *N* ☐
The selection of a data recording interval?	*Y* ☐ *N* ☐
Can customer service be connected or disconnected remotely?	*Y* ☐ *N* ☐

Can any selected portion of the system be upgraded to use a different communications network?	
Without changing consumer equipment?	*Y* ☐ *N* ☐
Without visiting consumer sites?	*Y* ☐ *N* ☐
Without requiring software or firmware changes?	*Y* ☐ *N* ☐

Can older equipment be upgraded with equipment from different vendors without changing the rest of the system?	Y ☐ N ☐
Can different collection rates and technologies be applied in different parts of the system to make collection of data more cost-effective?	Y ☐ N ☐
Can the system be easily scaled up or down based on consumer participation levels?	Y ☐ N ☐
Can new functionality such as detection of energy theft and diversion or outage management, be added?	
Without changing consumer equipment?	*Y* ☐ *N* ☐
Without visiting consumer sites?	*Y* ☐ *N* ☐
Without requiring software or firmware changes?	*Y* ☐ *N* ☐

Standards

The elements of the infrastructure and the ways in which they interrelate are clearly defined, published, useful, open and stable over time.

Requirements

Use Open, Published Standards

An AMI should utilize methods and technologies published by recognized standards organizations such as the IEEE, IEC, ANSI, ASHRAE, ISO, IETF, W3C, and others. The benefits of using standards have been widely discussed elsewhere, including many EPRI documents. A few of these benefits are:

- Elimination of "vendor lock-in"
- Increase of the available market for vendors
- Competition based on value added rather than brand name
- Less vendor-specific training needed
- Increase in available replacement equipment
- Reduction of obsolescence
- Reduction of costs for the reasons listed above

There are many standards specifications, so much so that the joke goes, "The nice thing about standards is that there are so many to choose from." There are ways to evaluate standards, however. Some of the important criteria for doing so are included in the checklist, including, whether the standard is complete, published, in use, recognized, maintained and supported.

Re-Use Industry Knowledge and Experience

Even if an AMI system uses proprietary technology, it may provide some of the benefits of a standard if other utilities have made use of it, have been able to influence its design, and have been able to share experiences using it.

Checklist

Are the specifications for connecting to the system complete (i.e. they are not still in development)?	Y ☐ N ☐
Have the specifications for connecting to the system been published?	Y ☐ N ☐
Are the specifications for connecting to the system available online?	Y ☐ N ☐
Have the specifications for connecting to the system been available for more than two years?	Y ☐ N ☐
Are the specifications for connecting to the system used elsewhere in the world?	Y ☐ N ☐

Are the specifications for connecting to the system recognized by any of the following categories of organizations?	
An international standards development organization (SDO), e.g. the ISO, IEEE, or IEC?	*Y* ☐ *N* ☐
A national standards organization?, e.g. ANSI, CSA, CEN?	*Y* ☐ *N* ☐
An industry consortium, e.g. ASHRAE BACnet™ Users Group, UCA® International OpenAMI Group, DNP User's Group	*Y* ☐ *N* ☐

Is there an independent (non-vendor) organization that is responsible for:	
Updating the specifications for the system?	Y ☐ N ☐
Certifying that devices or systems comply with the specification?	Y ☐ N ☐
Answering questions and/or resolving disputes regarding the specification?	Y ☐ N ☐
Permitting users to share experiences with the technology?	Y ☐ N ☐
Do the system performance targets make reference to an open, published standard?	Y ☐ N ☐
Do the security measures applied to the system follow open, published standards?	Y ☐ N ☐

Has another regulatory body, system operator, or utility approved for use in its jurisdiction:	
This AMI system?	Y ☐ N ☐
Another AMI system from the same vendor(s)?	Y ☐ N ☐
The technology underlying this AMI system?	Y ☐ N ☐

Openness

The infrastructure is based on open standards that are available to all qualified entities on a nondiscriminatory basis.

Requirements

Plan for Evolution

The term openness indicates a measure of how. Open standards are publicly maintained and available through standards development organizations or industry consortia. 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 AMI because it will reduce barriers for new vendors to enter the market, and therefore help to create economies of scale.

The majority of AMIs currently offered are not open. To encourage evolution to open systems, utilities should:

- Clearly identify their commitment to open systems and which portions of AMI s they expect to be standardized in the future.
- Ensure vendors are committed to evolution to open systems and have a published, detailed plan for getting there.
- Identify clear milestones for the evolution of particular AMI projects and realistic schedules for achieving these milestones.
- Make it clear that open systems functionality is a requirement for *all* vendors wishing to serve the utility, and that initial costs will therefore have the same impact on all competitors.

Permit Co-existence

To provide a minimum indication of commitment to openness, an AMI system should be able to co-exist with, and overlap geographically with, proprietary AMI systems from other vendors in the market. This is not always the case, when competing wireless systems may interfere with each other.

Reduce Economic Barriers to Interoperability

Acquiring the specifications for accessing an AMI system should not be so costly that doing so might on its own prevent devices from connecting to the AMI system. For instance, if a utility defines it's AMI using technology from vendor X, but wishes to connect devices from vendor Y to the system. In an open system, vendor X should not charge vendor Y a license fee for use of the technology, and should not charge more than a nominal administrative fee for providing the specifications for the interface.

This is not to say that a utility should not charge fees for third parties to access its AMI; but the fees should be associated with access to that system, not for the use of the technology. Furthermore, they should be paid to the owner of the system, not to a vendor who supplied equipment to the system.

It is recognized that the majority of AMI technologies are still proprietary and that it may be a long time before AMI systems are open. However, vendors willing to make concessions toward openness should be encouraged by utilities to do so.

Well Defined, Published Interfaces and Points of Interoperability

Even if an AMI is implemented using a, standards-based approach, interoperability is not achieved unless there are well defined points within the overall system where interoperability is expected to be achieved. These points should be well documented, and the specific standards used to implement the interfaces at these points of interoperability must be defined.

An example of this concept can be found in work produced by the OpenAMI group (http://www.openami.org/) – a task force within the UCA International Users Group (http://www.ucausersgroup.org/ that is addressing the requirements of AMI. As illustrated in Figure 4-2, OpenAMI listed a number of different interfaces that could be standardized and made interoperable between different vendors.

An AMI specification should clearly define which interfaces are to be open and interoperable among multiple vendors.

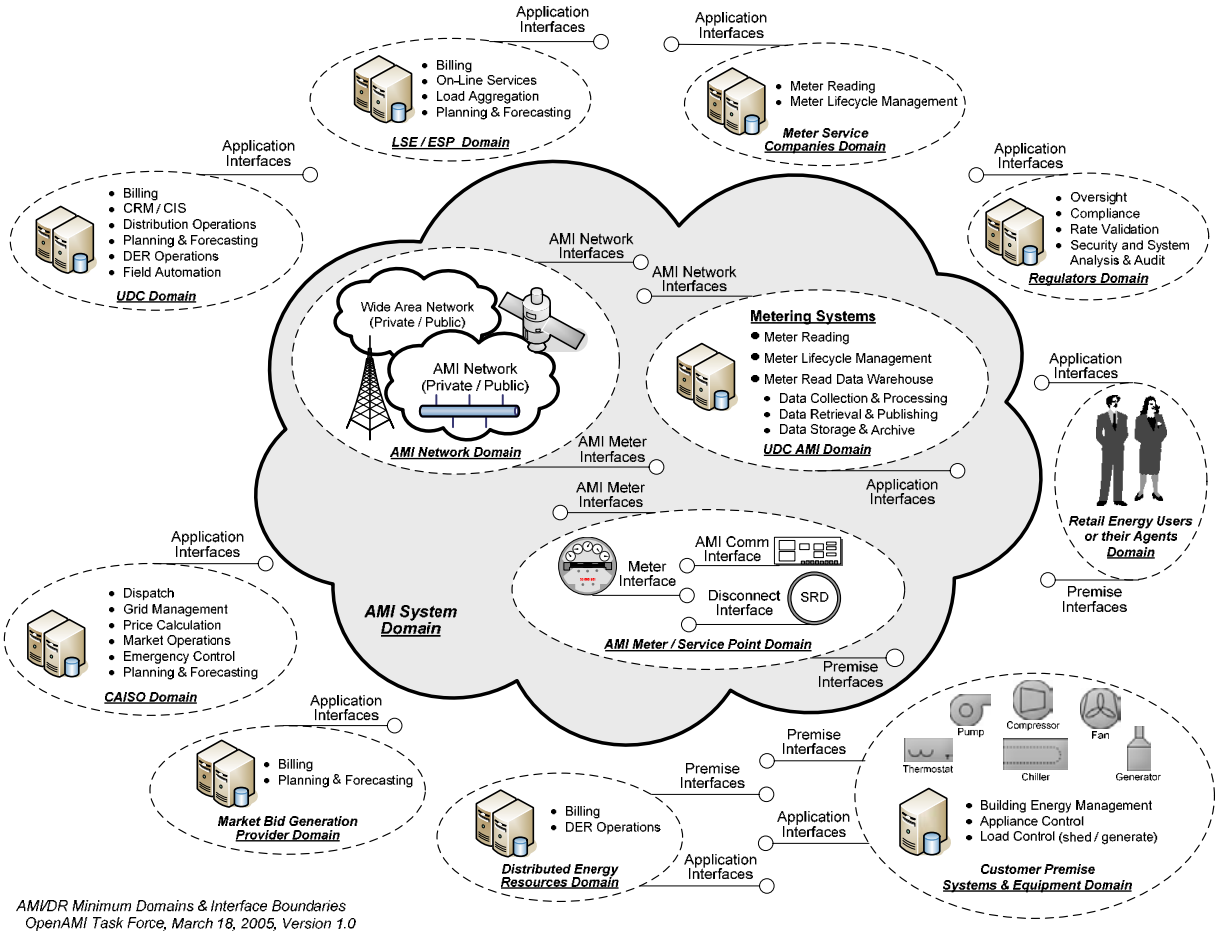

Figure 4-2
OpenAMI Domains and Interface Boundaries

Checklist

Is the equipment for the system available from more than one vendor?	Y ☐ N ☐
Are the specifications for connecting to the system available to anyone?	Y ☐ N ☐
Are the specifications for connecting to the system available at low cost (i.e. no more than necessary to administer their distribution and promotion)?	Y ☐ N ☐
Can any vendor connect equipment to the system without providing profit to a competitor?	Y ☐ N ☐
Is the body responsible for updating the specifications a non-profit organization?	Y ☐ N ☐
Does the vendor of the system have a documented plan for how the system will eventually evolve to become an open system?	Y ☐ N ☐

Is there a published, standardized specification describing exactly how to do each of the following items?	
Connect a meter to the system?	Y ☐ N ☐
Connect customer premise equipment to the system, such as load control devices and automated building management systems?	Y ☐ N ☐
Connect distributed generation equipment to the system, monitor it and control it?	Y ☐ N ☐
Change a tariff or rate structure?	Y ☐ N ☐
Incorporate a different communications network into the system?	Y ☐ N ☐
Read any meter in the system?	Y ☐ N ☐
Induce demand response in any consumer or group of consumers?	Y ☐ N ☐
Access individual and aggregate load profiles?	Y ☐ N ☐

Can the communications networks used by the system co-exist (not interfere) with the networks used by nearby systems belonging to other vendors or other utilities?	Y ☐ N ☐
Is there a single, standard specification for the data exchanged in the system such that it can be carried over a variety of different communications technologies?	Y ☐ N ☐

Security

The infrastructure is protected against unauthorized access, interference with normal operation; it consistently implements information privacy and other security policies.

Requirements

Ensuring Co-existence and Security

A key factor in developing an evolution plan toward open systems is that the system will not evolve if certain key OpenAMI principles are not applied from the very beginning. Two of these are co-existence (geographical overlap), and security. It should be the goal of utilities to evolve AMI from largely proprietary systems with few standard interfaces, to open systems with many standardized interfaces.

To do this, utilities must:

- Ensure that neighboring AMI networks can co-exist without interfering with each other. Ensure that even proprietary systems protect the personal information and data of consumers

from eavesdropping, tampering, and impersonation, especially from nearby networks that use similar technologies.

Deploy Minimum Levels of Cryptographic Capabilities

Security of metering can be a huge topic, and standards for secure AMI are still only in development. Therefore it is difficult to predict what will be needed in the future. Yet, it is essential that devices going into the field today support at least a minimum, significant security capability. The following basic security requirements should be satisfied by all field devices:

- Ability to support and manage emerging industry management and security policies
- Ability to perform cryptographic hash functions
- Ability to encrypt and decrypt messages, ideally with a hardware accelerator
- Secure storage of cryptographic credentials (ideally with tamper detection)
- Software-updateable encryption algorithms
- Flexible credential sizes
- Role-based authentication on local maintenance ports

As an example of the processing power that may be required for secure AMI, vendors and users should consider the following statement from the recently approved Technical Specification for Programmable Communicating Thermostats (PCTs) in the state of California.

> *"Confidentiality of PCT message contents is not a requirement. For this reason, message packets are not encrypted but are instead signed using a method consistent with the FIPS 186-2 Digital Signature Standard. The Elliptic Curve Digital Signature Algorithm (ECDSA) as defined in FIPS 186-2 and ANSI X9.62 shall be utilized. The PCT shall be capable of supporting a public key length of 256 bit or larger."*

Although PCTs are only one of many different devices within an AMI, and the final details of the PCT security protocols have not yet been defined, the statement above nevertheless reflects a commitment by members of the industry to significant minimum processing power dedicated to security within AMI devices.

Plan for Remote Upgrading

Because security is a volatile field in which attackers and defenders are both constantly trying to improve their technology to obtain an advantage, it is vital for security purposes that the security measures in an AMI be upgradeable. The items that are likely to be upgraded include:

- the size and number of credentials necessary
- the types of algorithms used
- the protocols used to exchange the credentials

Therefore it is important that very few of the security measures in an AMI device be prescribed or "hard-coded" in the device.

Because it is not cost-effective to visit consumer sites for upgrading, the security measures of the AMI must include a secure means of upgrading the security measures themselves remotely.

Permit the Implementation and Support of Emerging Security Policies

An AMI system should support the security features necessary to implement and support emerging industry and corporate security policies. These should be applied as appropriate for the environment in which the device of system is to be implemented. Industry security policies are developing under regulatory and government agencies that can influence the security capabilities of AMI and advanced automation systems. This includes the mechanisms necessary to implement authentication, authorization, auditing, confidentiality, integrity, and availability.

Protect Consumer Information

An AMI system should at all costs protect the personal information of consumers, in particular their name, address, email or phone number, and their account information. Specifiers are encouraged to identify all applicable government and industry regulations for this requirement.

Protect Business Information

An AMI system should protect information critical to the business of the utility. Specifiers are encouraged to identify all applicable government and industry regulations for this requirement.

Prevent Unauthorized Access

An AMI system should prevent unauthorized access to the services of the system, particularly the capability to disconnect consumers' electrical service or shut down consumer premise equipment, but also more traditional services like the ability to read energy usage.

Add or Remove Credentials Promptly

An AMI system should be able to quickly and easily add or remove the access permissions permitting individuals or organizations to access the AMI's data and services. Typically this means that the cryptographic credentials used to provide access be managed in a centralized manner. Providing this capability greatly reduces one of the primary risks to security – authorized employees leaving the organization.

Authorize Access Using Roles

An AMI system should provide access to interface by assigning users well-defined roles, so that certain roles are not permitted to access specified functions. For instance, some roles may be "read only" and are not permitted to change the operation of the system. Others may only be permitted to access specific types of data. Role-based access permits security policies to be implemented much more easily, cost-effectively, and consistently.

Authenticate using Multiple Factors

An AMI system will be more secure if users of the system must supply more than one of the following factors in order to authenticate who they are:

- Something you know – such as a password or PIN.
- Something you have – such as a token or access card
- Something you are – such as a fingerprint or retina scan

AMI systems should authenticate users by testing more than one of these factors.

Ensure System Availability

An AMI system should have the capability to resist "denial-of-service" attacks, in which an attacker attempts to transmit large numbers of messages at the system in hopes of preventing any other traffic from being processed or overwhelming the processing power of the system. Although such attacks are among the most difficult to protect against, a few basic measures help to reduce the risk:

- Provide multiple message paths so if one path is overwhelmed, another can be used
- Provide "stopping points" where messages can be filtered based on their source or destination address or other criteria
- Measure network statistics and raise alarms when unusual numbers of messages are transmitted
- Provide "defense in depth" in which additional credentials are needed to access the most vital information in the system, and fewer users are permitted access.

For the portions of the AMI that reside in a normal office environment, these measures are typically available as part of standard networking hardware such as firewall routers. They may be much more difficult to deploy in the field portion of the AMI, but some measures, like gathering and alarming statistics, may still be possible.

Apply Security at All Exposed Interfaces

There is a tendency in evaluating technologies to assume that because a technology is not well-known, it is more secure. This theory, known as "security through obscurity", is incorrect because it ignores the facts:

- The specifications of many supposedly obscure technologies are actually easily available, especially with the advent of the Internet.
- Although the details of a technology may not be well known, the basics (e.g. frequencies, encoding mechanism) may be easy to discover and use in an attack.
- The most common threats come from previously authorized individuals (i.e. ex-employees) who are likely to be familiar with the technology and operation of the system already.

The power industry, because its operations are less well-known than commercial computing, is particularly vulnerable to this type of thinking.

For this reason, it is important that all exposed interfaces be secured, particularly wireless technologies, rather than relying on the proprietary nature of some technologies to ensure security.

Log Significant Events

One of the most important requirements of secure systems is the ability to record and audit the source of significant events in the operation of the system. This permits system operators to reconstruct the events surrounding attacks and improve the possibility of locating the attacker. In particular, the capability to prevent "repudiation", in which an authorized user performs an illegal or damaging operation and then later denies doing so, is important. A number of events significant to the operation of AMI systems should be logged and are identified in the checklist. Ideally these items should be logged by the device performing the action rather than at the device requesting the action, to reduce the possibility of falsification of logs.

Checklist

Can the system co-exist and not interfere with neighboring AMI networks?	Y ☐ N ☐
Does the system prevent unauthorized users from doing any or all of the following?	
Accessing personal information about consumers?	Y ☐ N ☐
Reading energy usage or cost information for a given consumer?	Y ☐ N ☐
Downloading incorrect tariff schedules, load control requests, software, firmware, or other data to equipment at a consumer site?	Y ☐ N ☐
Controlling load at the customer site?	Y ☐ N ☐

Does the system prevent any user (authorized or not) from tampering with the energy usage data supplied from the consumer site?	Y ☐ N ☐
Does the system restrict access to different parts of the system based on the role of the user making the request?	Y ☐ N ☐
Does the system make appropriate use of standard network security equipment and practices such as firewalls and intrusion detection systems?	Y ☐ N ☐
Does the system keep statistics of message exchanges and raise alarms if messages exchanges exceed preset thresholds?	Y ☐ N ☐
Does the system permit centralized control of security credentials like passwords, keys, and certificates?	Y ☐ N ☐
Does the system have a published default security policy that utilities can use as the basis for developing their own policies?	Y ☐ N ☐
Does the system authenticate users by means of more than one authentication factor?	Y ☐ N ☐

Are all devices in the system capable of performing basic security functions such as hashing, encryption, secure credential storage, and secure login?	Y ☐ N ☐
Are all devices in the system capable of upgrading security algorithms, credentials, and protocols remotely and securely?	Y ☐ N ☐
Are all exposed interfaces of the AMI secured, including….	
Back-office networks?	*Y* ☐ *N* ☐
Wide-area networks?	*Y* ☐ *N* ☐
Neighborhood or "last mile" networks?	*Y* ☐ *N* ☐
Customer premise networks?	*Y* ☐ *N* ☐

Does the system provide audit logs of all configuration changes, including:	
Tariff or rate changes?	*Y* ☐ *N* ☐
Software or firmware changes?	*Y* ☐ *N* ☐
Load control requests (i.e. initiating demand response)?	*Y* ☐ *N* ☐
Addition or deletion of consumers?	*Y* ☐ *N* ☐
Changes to personal information?	*Y* ☐ *N* ☐
Changes to operating parameters, e.g. recording or polling intervals?	*Y* ☐ *N* ☐
Enrolment in or resignation from programs e.g. prepayment, DR?	*Y* ☐ *N* ☐

Does the system perform these security functions while permitting authorized users to access any of the data discussed under "Shareability"?	Y ☐ N ☐
Does the system perform these security functions while adhering to open standards as discussed under "Standards" and "Openness"?	Y ☐ N ☐

Extensibility

The infrastructure is not designed with built-in constraints to extension as new applications are discovered and developed.

Requirements

Self-Announcement

The devices in an AMI should be able to announce to the rest of the system that they are connected and available for communication. This feature reduces the probability of configuration mismatches during installation and extension of the system. It reduces time and

effort in installation because installers do not have to "search for" the device on the network. It helps improve security by calling attention to devices that have not announced themselves or have announced themselves incorrectly or with invalid credentials. Note that devices should not automatically connect to the system without human intervention, however, because that would create a security risk.

Self-Description

The technologies used to implement the AMI should permit devices to interrogate each other and determine what data they can access, including the names, descriptions, types, and the structure of the data. This "information about information" is also referred to as "meta-data". Self-description is important because it permits the system to be extended by personnel who have less training but nevertheless perform the extensions with fewer errors. It is much easier to correctly select data chosen from a list generated by the device providing that data, than to manually enter the name or address of data from memory.

Information Modeling / Object Modeling

The data stored and provided by an AMI should be defined and structured according to a shared information model, also known as an "object model". The information model describes the behavior of a device or the entire system in an abstract manner using a consistent language and organization method.

The AMI information model should be standardized across the organization, and ideally, standardized across the industry. Standardization of any kind results in benefits for all involved, as discussed in section 0. Standardization of information models is especially useful because the same data can then be carried over a variety of technologies and translated from one technology to another with a minimum of cost and human effort. Figure 4-3 illustrates this concept.

When extending an AMI, a standard information model provides a common language for describing extensions and makes extensions immediately recognizable and usable. Standard information models work best when they describe not just the format of the data (what the data *is*) but also its semantics (what it *means*).

Technology Independence and Protocol Layering

The communications protocols used to implement an AMI should separate the meaning of the message from the mechanism by which that message is transmitted. This separation of specifications will ensure that as communications technology evolves, the AMI can be extended, to perform the same functions using newer technologies.

Most electronic communications protocols have two aspects:

- The part of the message that deals with the intent of the message such as the request to "read the meter". This part is variously known as the application layer, process layer, or user data. Data in this part would be named and structured according to the standardized information model discussed in the previous section.

- The part of the message that deals with message handling such as delivery methods, routing, reliability, addressing, etc. This part is often referred to as the transport profile, network interface, or simply the "lower layers".

As illustrated in Figure 4-3, this concept is often summarized in terms of an analogy to a postal letter. The application layer is represented by the content of the letter, the lower layers by the envelope, stamp, and addressing. The envelope part does not necessarily determine whether the letter will be delivered by air or train or truck. The mail system infrastructure (which may vary substantially from locale to locale) will work that part out according to the "higher level" directions on the envelope.

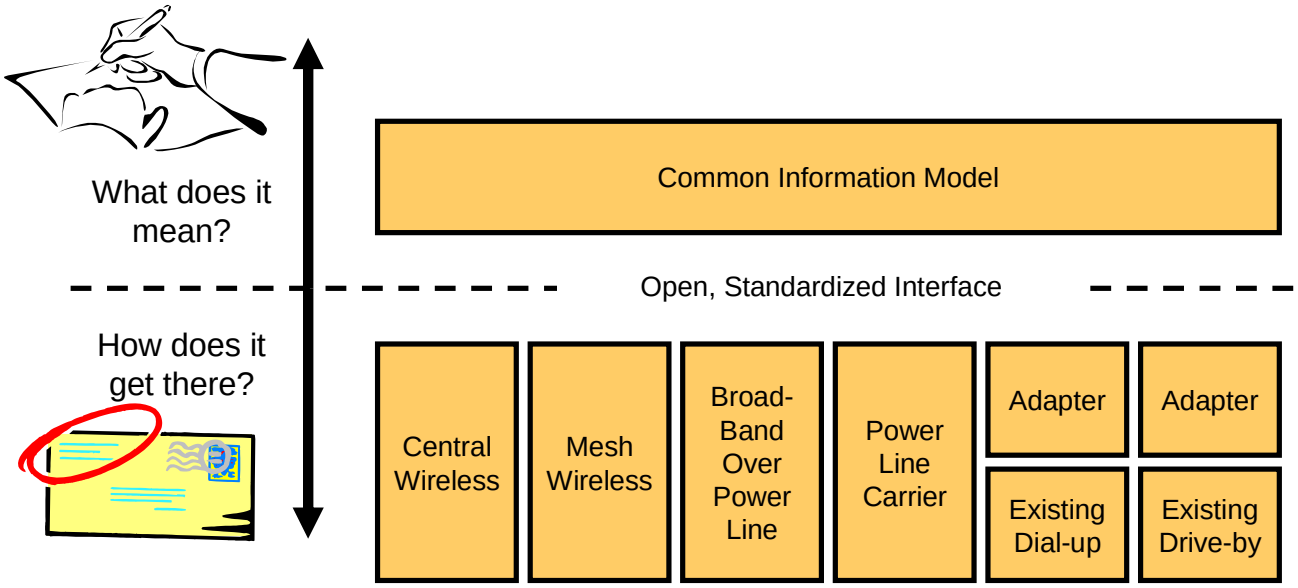

Figure 4-3
Extensibility through Technology Independence - and the Postal System Analogy

The common agreement by the entire postal system about what a letter is, what a stamp is, how addresses should be structured, and that there are different classes of service (e.g. certified, air mail, packages, courier) is represented in electronic protocols by a variety of names:

- Common services
- Generic interface definition
- Abstract service interface
- Standardized message semantics
- Common application layer interface

Whichever name is used, the important issue for AMI is that this common application layer interface is not only defined in documentation and standardized, but actually *exposed*, usually in software. Multiple vendors can then use this standardized interface to:

- Add technologies to the AMI to reach more consumers more cost-effectively

- Connect the AMI to legacy technologies, as discussed in section
- Serve as a translation point between proprietary systems from multiple vendors

Modular Design and Scalability

The requirement for a common application layer interface is an example of a more general requirement that an AMI should be modularly designed and it should have no inherent limitations on expansion.

The most common extension to an AMI will be the addition of new participating consumers, so utilities should be very aware of which components of the architecture must be changed in order to make this happen. For cost effectiveness, increases in scale or features of the AMI should not require that existing components be replaced, only that new components be added.

Often there will be a single component that provides the true upper bound of scalability; for instance, the bandwidth of a local area network, the bus speed of a backplane, or the number of expansion cards that can be added. It is important to identify such critical components early in the design phase.

Checklist

Does the system avoid imposing a numeric limit on the number of devices which can be deployed?	Y ☐ N ☐
Can the system be expanded without replacing existing equipment?	Y ☐ N ☐
Does the system avoid making a single component the bottleneck for expansion?	Y ☐ N ☐
Does the system use a well-defined information model?	Y ☐ N ☐
Is the information model common to all devices in the system?	Y ☐ N ☐
Is the information model described in an open, published standard?	Y ☐ N ☐
Does the information model define not only the name and structure of the data, but also its use and meaning (semantics)?	Y ☐ N ☐
Do the communications specifications for the system define a common application layer interface?	Y ☐ N ☐
Is the common application layer interface exposed in software?	Y ☐ N ☐
Is the common application layer interface described in an open, published standard?	Y ☐ N ☐
Does the system already support more than one transport technology through the common application layer interface?	Y ☐ N ☐

Can devices announce themselves when they are initially connected to the system?	Y ☐ N ☐
Can devices electronically describe what data they provide?	Y ☐ N ☐
Does the system provide tools that enhance extensibility using self-announcement and self-description?	Y ☐ N ☐

Manageability

The elements of application deployment can have their configuration assessed and managed, faults can be identified and isolated, and are otherwise manageable.

Requirements

Develop Systems and Network Management Requirements Up Front

Managing an AMI presents even greater challenges than specifying and executing the applications than an AMI enables. For resource-constrained equipment, management functions, (including security) must be developed at the same time as the applications. Critical management capabilities necessary to support massive scaling of the AMI should not be left as an afterthought.

Manage Devices

An AMI should permit operators to remotely manage each piece of equipment deployed in the system, including the meters. Too often in utility networks, only selected components are managed, and the most common components, such as the meters, are not visible to system management. The minimum set of equipment management functions is shown in the checklist. These functions should ideally be performed using an open standard protocol. The information gathered and reported from each device for management purposes should be well-defined and common across the organization.

Synchronize Time

Time synchronization has been identified as a key attribute for proper operation of utility field devices and systems and is especially important for auditing so system failures and attacks can be reconstructed after the events. An AMI should be synchronized to Universal Coordinated Time (UTC) using one of several available standardized methods (e.g. NTP, SNTP, GPS, IRIG-B, etc.) with a resolution and uncertainty appropriate for its use and compliant with relevant security policy. It will be necessary to expose via the self description mechanism (described in 0) what this resolution and uncertainty is.

Manage Networks

An AMI should include a method for performing from a central location the following categories of system and network management defined in the ISO Open Systems Interconnect model:

- Configuration – how is the system structured, organized, and extended? Refer to 0.
- Fault – where are failures occurring in the system and how can they be corrected?
- Performance – how can the network be optimized and critical components shared?
- Security – how can the system be protected? Is it under attack? Refer to section 0.
- Accounting – how are resources being used, by whom, and how much is it costing?

Important details of these functions are included in the checklist.

Manage Configuration

In order to operate equipment, it is essential to have control over the configuration of the device and to unmistakably recognize its state over the network. Therefore the following are necessary capabilities:

Universal Identifier	This represents an identifier that can be used to uniquely recognize a specific device over the network. An instance of universal ID is necessary to identify the make and model of a device, and, one to identify the instance of the device.
Configuration Identifier	This represents, within a single device, the ability to recognize the specific configuration, or settings, applied to the device at the present time.

Manage Change

The surest way to create a stranded asset is to install something that can only be changed via rolling a truck. Thus, it should be required that all installed devices support remote image change. Image structure can be left to the manufacturer. But standardizing on the change management mechanism and protocol will facilitate integration into client tools.

Checklist

Can any piece of equipment (e.g. meter, data concentrator, networking device) in the system be managed as follows from a central location?	
Enable/disable the device?	Y ☐ N ☐
Run local hardware and software diagnostics on the device?	Y ☐ N ☐
Change its logical address?	Y ☐ N ☐
Download software or firmware?	Y ☐ N ☐
Download new configuration?	Y ☐ N ☐
Download new security parameters or credentials?	Y ☐ N ☐

Gather operational statistics?	Y ☐ N ☐
Receive spontaneous alarm reports for serious failure conditions?	Y ☐ N ☐
Can thousands of devices within the system be managed (i.e. enabled/ disabled/ downloaded) with a single command from a central location?	Y ☐ N ☐
Is there a minimum set of management data and services specified that every device must provide?	Y ☐ N ☐
Is there a common, integrated method for synchronizing time across the system?	Y ☐ N ☐
Is there a testable specification for how well time must be synchronized across the system?	Y ☐ N ☐
Does the system periodically verify that time is correctly synchronized?	Y ☐ N ☐
Can devices within the system notify other systems what level of time synchronization they require?	Y ☐ N ☐
Does the system provide a mechanism to centrally perform the following operations on the AMI communications networks?	
Verify that the current topology and configuration of the network is as expected?	Y ☐ N ☐
Change message paths or force automatic algorithms to avoid certain paths?	Y ☐ N ☐
Add or remove devices from the network?	Y ☐ N ☐
Identify where network failures are occurring?	Y ☐ N ☐
Identify overloaded resources?	Y ☐ N ☐
Move load from overloaded resources?	Y ☐ N ☐
Identify potential security attacks?	Y ☐ N ☐
Detect device failures?	Y ☐ N ☐
Distinguish between device failures, power outages, and network failures?	Y ☐ N ☐
Filter messages passed to any part of the network by source, destination, or communications protocol?	Y ☐ N ☐
Identify which systems have access to the network and performed a given operation?	Y ☐ N ☐
Identify which human beings have access to the network and performed a given operation?	Y ☐ N ☐
Approximate the cost of operating the system?	Y ☐ N ☐
Does the system store the following information with version control?	
Device configurations and settings?	Y ☐ N ☐
Device firmware?	Y ☐ N ☐

Network topology?	Y ☐ N ☐
Database structure?	Y ☐ N ☐
Can the system verify online that device configurations, settings and firmware are correct?	Y ☐ N ☐
Can the system automatically correct devices configurations, settings and firmware if it determines that they are incorrect?	Y ☐ N ☐

5
SAMPLE GUIDELINE FOR ROBUST DYNAMIC ENERGY MANAGEMENT SYSTEMS IN NORTH AMERICA

A basic tenet of the IntelliGrid Architecture is to select implementation technologies based on careful analysis of requirements.

This section of the checklist document identifies implementation technologies based on open standards that satisfy the requirements in section 4 Requirements and Checklists.

The final selection of technologies is a local decision that must be made by the utilities after their own internal analysis. The following standards-based technologies have been identified by the IntelliGrid Architecture as cornerstone technologies that meet many of its underlying goals and objectives and are suitable for selection after requirements analysis. This is not an exhaustive list. Readers should refer to the IntelliGrid Architecture documentation for additional information. Note that in parenthesis are abbreviations for these standards used liberally through this section. See section 7 References for citations for these and other standards referenced herein.

- IEC 61850 (61850) – field device communications and general device object modeling
- IEC 61968 and, IEC 61970 – Common Information Model (CIM) and Generic Interface Definition (GID) – enterprise information management and integration
- IEC 62351 (62351) – IED communications security
- ANSI C12.22 C12.19 (C12) – revenue metering communications and object modeling (note: this document refers to the committee drafts for the 2007 version of these standards in review at this time).
- ASHRAE 135 (BACnet) – building communications and object modeling

Below, we illustrate the IntelliGrid Environments topology which indicates the key groupings of communications and application requirements. This figure shows topographically where the key standards apply.

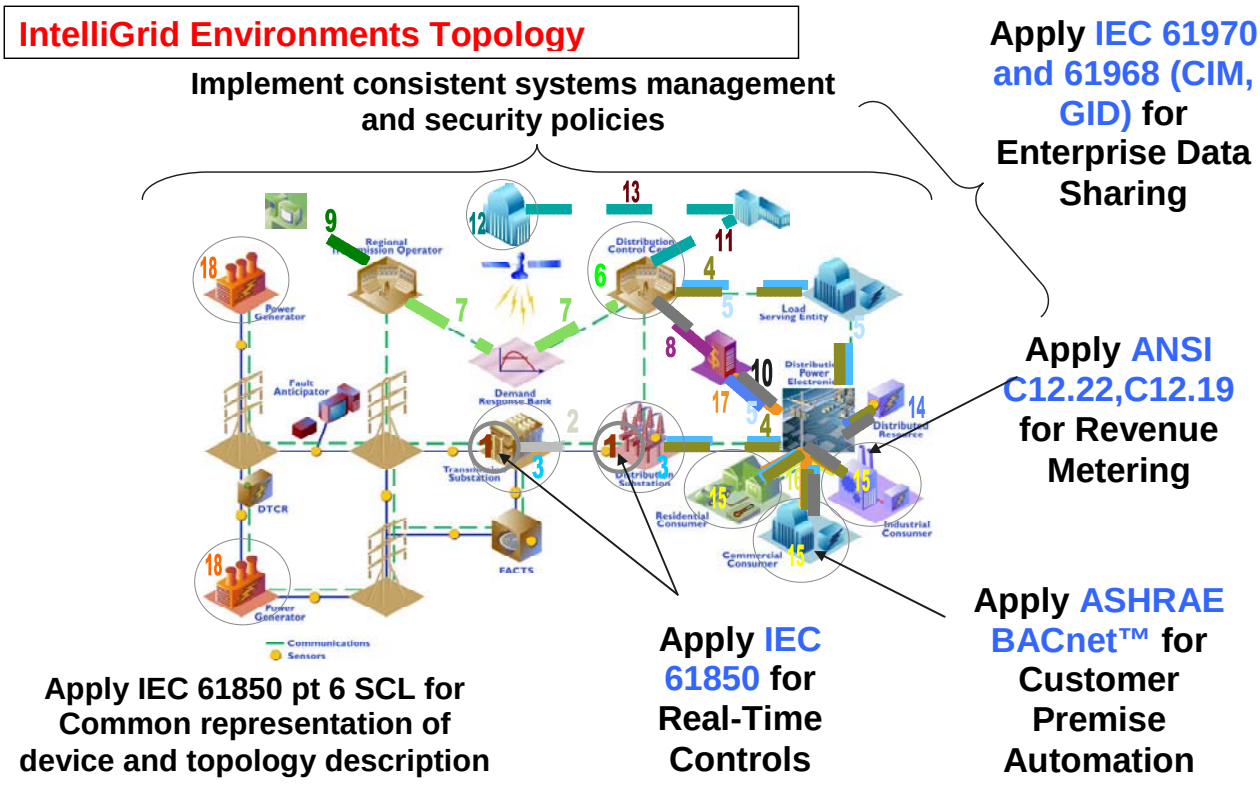

Figure 5-1
Sample Guideline Reference Topology

The figure below, Figure 5-2 Key Points of Interoperability, summarizes those key points in a deployment of these technologies. Specifically, we derive from section 0 Doing it the "Right Way" a model of how these key points can be assembled into a seamless whole.

Note that these selections don't constrain function or application. However, they provide for a degree of sameness of deployments that will allow them to be integrable and maintainable.

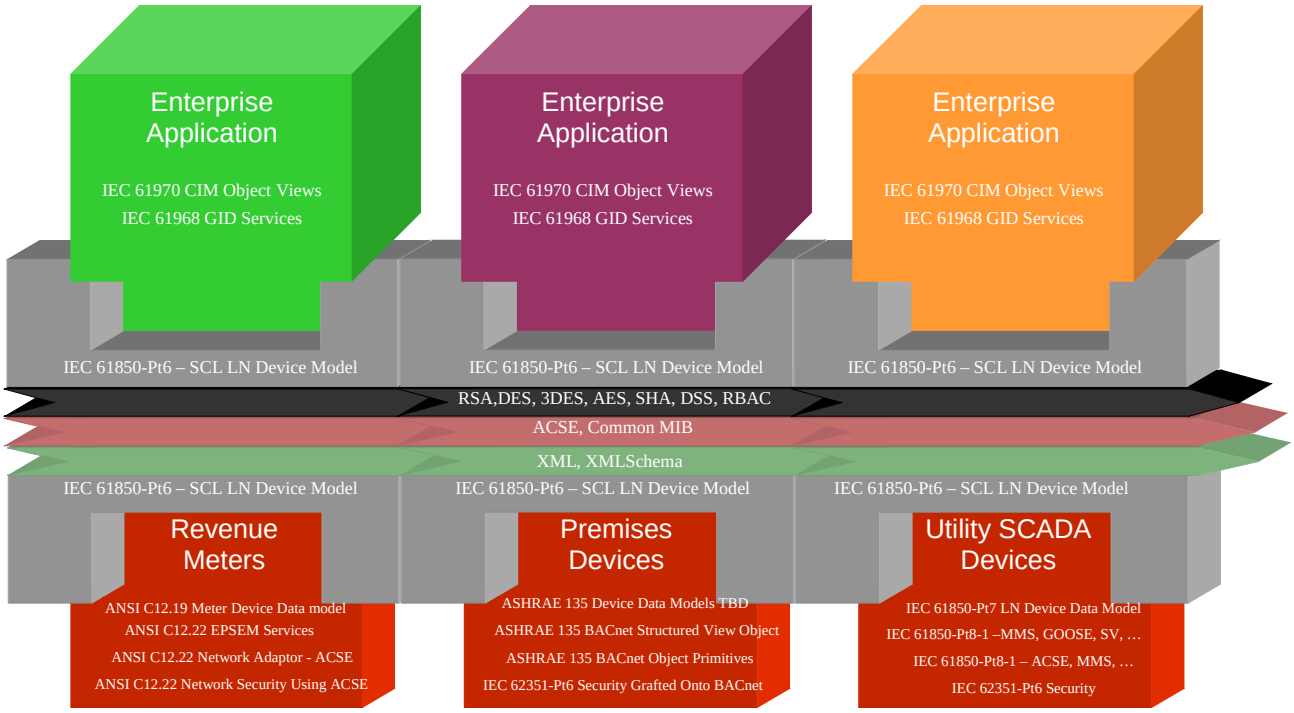

Figure 5-2
Key Points of Interoperability

Table 5-1
Key Points of Interoperability

Enterprise Applications	
IEC 61970 CIM Object Views	CIM provides a device agnostic view of a functional power system. However, the elements of the model should be derived from components of 61850 device models.
IEC 61968 GID Services	GID provides the common services required at the enterprise application level. These services may rely on computational power not available in field devices yet useful to highly scaled applications.
System Wide Interfaces	
IEC 61850-Pt6 – SCL LN Device Model	The core level of detail for modeling intelligent devices is the 61850 device model. Each domain specific device model (BACnet, C12, 61850) is translated into this common representation.
RSA,DES, 3DES, AES, SHA, DSS, RBAC	These are the key set of computational algorithms that are used by security protocols. Once embedded, they can be readily used and integrated into a secure communications environment. Role Based Access Control (RBAC) allows security policy to be managed with relatively few and stable roles as opposed to a large set of individual privileges.

ACSE, Common MIB	The Association Control Service Element (ACSE) provides a common interface to the application layer allowing security and manageability information to be utilized or provided by applications over heterogeneous communications networks. A common MIB permits a minimum availability of information from IEDs to allow for network and device communications management.
XML, and XML Schema	These technologies provide an open representation and description of information that can be understood electronically, presented, and archived.
Revenue Meters	
ANSI C12.19 Meter Device Data model	The North American standard model of a revenue meter.
ANSI C12.22 EPSEM Services	A reduced set of services for interacting with meters.
ANSI C12.22 Network Adaptor – ACSE	Describes the use of ACSE as the network interface to ANSI standard meter devices.
ANSI C12.22 Network Security Using ACSE	Definitions of ACSE's Authentication Value parameter for C12 communications
Premises Devices	
ASHRAE 135 Device Data Models *(TBD)*	Device models such as thermostats, chillers, etc… have not been explicitly modeled in BACnet to date.
ASHRAE 135 BACnet Structured View Object	The BACnet primitive permits the mapping of BACnet instance object definitions to a hierarchical model such as 61850 Logical Nodes. It is the key to representation of common functions within BACnet.
ASHRAE 135 BACnet Object Primitives	The services and object model from which BACnet devices are monitored and controlled.
IEC 62351-Pt6 Security Grafted Onto BACnet	BACnet leaves protocol, beyond a simple mechanism, to the non-standardized community of implementations. So this piece has to be assembled to achieve compatibility with the other models.
Utility SCADA Devices	
IEC 61850-Pt7 LN Device Data Model	Common library of standardized device component models.
IEC 61850-Pt8-1 –MMS, GOOSE, SV, …	Explicit mapping of these models to binary transport protocols.
IEC 61850-Pt8-1 – ACSE, MMS, …	Application of ACSE to 61850 communications using the MMS protocol.
IEC 62351-Pt6 Security	Corresponding use of authentication and encryption values within ACSE for 61850.

This balance of this section describes in some detail a how a set of possible open standards-based solutions that can address the requirements of section 4 above. Therefore, for each group in section 4 Requirements and Checklists, above, find identified specific standards and best

practices that can satisfy the requirements. Note, this guideline is optimized for North American deployment. Other choices might be selected for applications in other geographic settings.

Naturally, in the brief span of these pages, only a thumbnail presentation of these recommendations is possible.

Emphasis on Interfaces

In this example guideline, emphasis is on standardizing the interfaces to functionality, as opposed to, the instantiation of these interfaces into specific devices. The assumption is that if the key points of interoperability revolve around interfaces, many different permutations of services and device designs encapsulating the interfaces are possible which can interoperate together.

For example, if one focuses on the exposition of interfaces, it is transparent to an application, for example, if a there is a concentrator of meter data providing the meter model on behalf of many meters on the one hand or, a set of individual meters each exposing the meter model interface.

A key consequence of this approach is that interfaces can be exposed anywhere needed in a network. They can ultimately propagate down to individual devices over time, without upsetting the architecture of deployed applications relying on the content and existence of the interface.

ACSE and Conveyance to the Application Layer

IEC/ISO 8650 Association Control Service Element (ACSE) is a common standard for the representation and encoding of the transfer of application layer semantics to the application layer. There are two key advantages to recommended widespread use of this at the present time – first, it is part of 61850, DLMS, ANSI C12.22. Second, it provides a standard way of conveying a minimum set of semantics to the application layer that might otherwise be lost to the communications stack filtering. Among the key elements of this information are –

Called AP Title
Called AE Qualifier
Calling AP Title
Calling AE Qualifier
Authentication-mechanism Name
Authentication-value

ACSE's "AP Title" and "Authentication-mechanism Name" elements can take on the form of "Object Identifier" or OID. An OID is a globally unique identifier. OID's are registered with the OID Repository ensuring uniqueness. These identifiers are based on the internationally agreed universal identifier tree. This numbering scheme guarantees global uniqueness (no number used twice) as well as absolute traceability to a naming authority. OIDs are used to refer to any entity be it a data element, a device, a service and encryption or authentication mechanism etc. An example of an OID follows:

2.2.1 (Dot notation)
urn:oid:2.2.1 (urn notation)
{joint-iso-itu-t(2) association-control(2) abstract-syntax(1)} (asn.1 notation)

Here we introduce the concepts of “access role”, “encryption mechanism” and “identifiable entity.”

Access Role

Access to device services and information should be provided to various business entities however it will be desirable to limit access based on “need to know”. Role based access allows for assigning access to differing information or service based on role.

The authentication mechanisms employed must allow differing authentication identifiers (i.e. ACSE Authentication-value). Each identifier may be assigned to a role. The device data model implementation must then allow access to branches within the data model hierarchy on a per role basis.

- ACSE’s Authentication-value may be used to identify an “access role”.

Encryption mechanism

- Together Authentication-mechanism Name and Authentication-value are used to specify an authentication or encryption mechanism.

Identifiable Entity

- Together Called AP Title and Called AE Qualifier may be used to specify an entity or service of interest (i.e. a meter, a meter reading).

- Together Calling AP Title and Calling AE Qualifier may be used to identify a requesting application or device (i.e. a billing system or head-end).

The ACSE protocol is defined in:

ISO 8650: Association Control Service Element
ISO 8649: Service definition for the Association Control Service Element
ITU X.217: Information technology - Open Systems Interconnection - Service definition for the Association Control Service Element
ITU X.227: Information technology - Open Systems Interconnection - Connection-oriented protocol for the Association Control Service Element: Protocol specification
ITU X.237: Information technology - Open Systems Interconnection - Connectionless protocol for the Association Control Service Element: Protocol specification

Device and Network Management

Device and network management has traditionally been an afterthought when specifying or acquiring complex IT systems. Business units typically focus on application specific requirements. For example a system may support retrieval of meter data used for billing purposes. This is an application level functional requirement. Device and Network Management refers to a set of “non-functional” requirements that are necessary to maintain the security, reliability and robustness of the underlying infrastructure that supports and provides the application level functionality. In many cases network management and application functionality have been treated in isolation.

The 61850, CIM, BACnet® and C12 standards all provide mechanisms by which device data attributes can be modeled and in some cases provide specific network related data attributes. It is recommended that these standards are followed for modeling not only the application level attributes provided by devices but also network management related attributes when not directly provided by the standard. It is also advisable to realize that at times the two should be interchangeable or intimately related. For example, some networks may exhibit degradation in quality of service or throughput at certain times of day. This may be detected not through network management counters but in turn-around times in application level requests. This factor should be modeled in such manner that network management or application level interaction is supported. In this example the network management models may enunciate the degradation in throughput but the application models are used to make adjustments.

As the 61850, CIM, BACnet and C12 standards are applied and network management related attributes are modeled, access to these models and attributes provides a means by which functional and non-functional requirements can be met. Aside from the means by which the data are modeled and communicated the need for functional roles becomes necessary. For example in one case a "network manager" may wish to query a device for statistics that may be network management related information or possible application related. Similarly an application may wish to query network related information.

Since this guideline recommends that network management information be visible within the data model of the device as a whole, rather then a separate protocol, role based segregation of access rights to information must be achieved in the application layer itself. See the section on "Access Role

" describes role based security in more detail.

As networking related data models are created, refined or evaluated, certain external standards may be used as guidelines or references specifically:

RMON1: RFC 2819 Remote Network Monitoring Management Information Base
RMON2: RFC 2021Remote Network Monitoring Management Information Base Version 2 using SMIv2
SNMPv3: RFC 3411 An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks
SNMPv3: RFC 3418 Management Information Base (MIB) for the Simple Network Management Protocol (SNMP)
CMIP: X.700 Management framework for Open Systems Interconnection (OSI) for CCITT applications
CMIS: RFC 1095: The Common Management Information Services and Protocol over TCP/IP
CMIS: RFC 1189: The Common Management Information Services and Protocols for the Internet

These mature standards should help in assessing and defining relevant data attributes and models. A common application model for network management should be exposed. 62351 Part 7 conveys 61850 MIB mappings and common object models for network and device management.

Device, Data, Service and Identifiable Entities

Another complex topic arises when managing large networks of devices. Specifically, this is the management and assignment of identifiers used when referencing or accessing a device or data. In many cases this translates into physical network addressing information utilized by the underlying communications infrastructure. The challenge is in achieving independence from the underlying network.

ANSI C12.22 introduces the use of globally unique object identifiers into AMR. The ACSE used in C12.22 and 61850 use the application titles (AP-Title) as the means of associating logical clients and servers over heterogeneous networks.

Such identifiers are required for identifying logical communications endpoints in C12.22 but could also be used for manufacturer identifiers, product versions, customer IDs, serial numbers and authentication mechanisms and roles (as discussed previously). ANSI C12.22 has already established naming tree branches for communications and manufacturer use for use with ANSI C12 communications standards.

An area open for improvement in the standards cited in this guideline is that of network address translation. A means of standardizing translation from OIDs or AP-Titles to communications addresses at the various networking layers would be beneficial.

Security

It is assumed that messaging for AMI will often cross one or more security domains. In addition, it is essential that the applications running on devices be knowledgeable about the credentials asserted along with messaging so as to be able to filter access to information based on this knowledge.

Often, the subject of security is focused on the rights to transport and interpret messages as a whole. However, this is a severely restrictive view of the rights to interact with distributed information.

IEC 61850 and ANSI C12.22 rely on Association Control Service Element (ACSE) as a "wrapper" to convey security semantics accompanying a message to the application layer. Note that specific implementations may indeed process such information within lower communications layers. However, the population of information in ACSE makes information visible to the application which may then use it to constrain the processing of a delivered message.

This guideline, therefore, seeks to standardize on this conveyance for the purposes of facilitating role based access control to information within an intelligent electronic device (IED).

Since C12.22 and IEC 61850 already support this to a greater or lesser degree, and, since BACnet supports a more modest set of security and authentication services, there will be a gap to be addressed allowing ACSE to be used in conjunction with BACnet messaging in some customization layer. This will need to be the subject of future work.

In addition, there are components of the data models of devices which play a substantial role in the configuration and maintenance of security and authentication.

Security Support for Devices

Each of the standards employed in this sample guideline provides security through the following approaches:

Table 5-2
Summary of security support for devices

Standard	References	Notes
61850/62351	62351-6 DATA COMMUNICATIONS SECURITY – Part 6: Security for IEC 61850 Sections 4, 5 and 6 62351-4 DATA COMMUNICATIONS SECURITY – Part 4: Security for ISO-9506 based applications 62351-3 DATA COMMUNICATIONS SECURITY – Part 3: Usage of Transport Layer Security	The 61850/62351 implementation of ACSE allows for the transport of authentication information.
BACnet	BACnet currently employs a minimal set of security mechanisms. BACnet should be augmented with or enhanced through the use of 62351-6 DATA COMMUNICATIONS SECURITY – Part 6: Security for IEC 61850	This capability might be the subject of future work on this standard.
C12	ANSI C12.22-2007 (C12-22DocumentforBallot7-07.doc) Sections 5.3.4.8 Authentication Value Element (ACH), 5.3.4.13 C12.22 Security Mechanism ANSI-C1219-2007-WG2-0702.doc Section “9.5 Decade 4: Security Tables”.	C12’s ACSE implementation allows for the transport of authentication information. Application context defines default definition of the authentication information structure. However, C12’s ACSE authentication value may not correlate directly with 61850-pt8 implementation.

Cipher And Related Algorithms Supported By Devices

Table 5-3
Summary of cipher and related algorithms supported by devices

Key Capabilities	61850/62351	BACnet	C12
Ability to perform cryptographic hash functions	SHA	MD5 or SHA-256	MD5
Ability to encrypt and decrypt messages	TLS: RC4, 3DES, AES Signing: RSA, DSA Key Exc: RSA, Diffe-Hellman	DES	DES
Flexible credential sizes	TLS: RC4, 3DES, AES	No-56 bit key only	DES, 3DES

Support for Role Based Access Control

The authentication mechanisms employed must allow differing authentication identifiers. Each of these identifiers may be assigned to a role. The device data model implementation must then allow or deny access to branches within the data model hierarchy on a per role basis.

Table 5-4
Summary of support for Role Based Access Control

Standard	Notes
61850/ 62351	Provides authentication and authentication IDs. 61850 - AN07002WW-RolesInScl.doc describes role based access in SCL. This work in progress will help standardized how role based access to information and services provided by devices. Roles in SCL may be used to enhance all of the standards cited in this sample guideline. Additionally, SCL may be enhanced to include modeling techniques allowing for "role" based access definitions and data access rights within the data modeling language or data models themselves. The 61850/62351 implementation of ACSE allows for the transport of authentication information.
BACnet	BACnet should be augmented with ASCE allowing for role based security and access rights.
C12	The C12 implementation of ACSE allows for the transport of authentication information.

Support for Logging

Device modeling should allow for change tracking according to role and date for data elements determined to be "significant". Centralized network management may be used to collect this information from end devices. Frequency of collection or reporting of such information on an unsolicited basis may be guided by device storage limitations or the importance of raising alerts.

Table 5-5
Logging and Event Reporting in Devices

Standard	References
61850	Logging: IEC 61850-7 Section 14 Report-control-block and Log-control-block class models Reporting: IEC 61850-8-1 Sections 16.1Report Model and 16.2 Log Model
BACnet	135_2004new.pdf ANSI/ASHRAE Standard 135-2004 Section "13 ALARM AND EVENT SERVICES" Note: Supports change tracking through "Alarm and Event Services" and "change of value reporting"

C12	DRAFT ANSI C12.19-2007 Section 9.8 Decade 7 History and Event Logs ANSI C12.22-2007 TABLE 123 Exception Report Table

Satisfying Checklist Requirements

For each requirement identified in section 4 Requirements and Checklists, the tables below identify the principle references for the standards in this guideline section that can satisfy them. Note that satisfying the high level requirements in this checklist, necessitates high level criteria.

A substantial additional level of detail is required to flesh out the detailed implementation agreements which would be required to achieve interoperable systems based on these standards.

That being said, however, the level of detail that follows is able to illustrate the goodness of fit of the selected standards to the high-level requirements.

The No Regrets Robust Technology Design Checklist and Sample Guidelines focus primarily on integrating, interfacing, securing and managing networks consisting of various devices and systems. CIM & GID provide key standards covering data modeling and enterprise application integration. Where CIM and 61850 differ for example is that whereas 61850 describes how to model a device and the data attributes and services it exposes, CIM describes how to model the functional or business domain elements. These differences are somewhat orthogonal although they complement one another and address different requirements.

The bulk of requirements in this section are satisfied principally through the instantiation of capabilities in IEDs deployed. Thus CIM & GID are often not detailed in the following tables when the requirements deal specifically with those appropriate for IED.

Table 5-6
Satisfying Requirements for "Shareability"

	Requirement	Satisfied by
Shareability	Widen the System Boundary	Utilization of the standards specified in this sample guideline will open the AMI system to interoperability between applications previously treated independently. Sharing of common standards, infrastructure and security mechanisms all expand the usefulness of the deployed technologies. The following sections describe how these standards meet these goals.
	Share Data with Multiple Clients Simultaneously	Security and role based access facilitates sharing data and infrastructure as described in "Ensuring Coexistence and Security" and "Support for Role Based Access Control".
	Provide a Common Set of Shared Data	Please refer to section "Information and Object Modeling".
	Share Infrastructure with Other Utilities	All of the standards used in this guideline provide a means for integrating systems amongst utilities through a significantly less costly manner than possible without open standards.
	Provide a Common Set of Shared Data	Security and role based access facilitates sharing data and infrastructure as described in sections "Ensuring Coexistence and Security" and "Support for Role Based Access Control". Also refer to section "Information and Object Modeling".

Table 5-7
Satisfying Requirements for "Ubiquity"

	Requirement	Satisfied by
Ubiquity	Serve as Many Consumers as Possible	The standards specified in this sample guideline help serve as many customers as possible through scalability described in section "***Modular Design and Scalability***".
	Enable Smart Customer Premises Equipment	The standards of ANSI C12, for revenue metering, and ASHRAE 135, for customer premises devices, enable the deployment of integrate-able customer premises equipment.
	Use Multiple Physical Technologies	61850, CIM, BACnet and C12.22 were designed to allow transport of application data independent of the physical medium and over a broad variety of technologies. Also, these standards make no reference to device hardware technologies such as microprocessor selection. BACnet provides key example implementations for ISO 8802-3, ARCNET LAN, EIA-485 and EIA-232 however BACnet does not need to rely on these physical transport layers.

Table 5-8
Satisfying Requirements for "Integrity"

	Requirement	Satisfied by
Integrity	Provide Measurable High Availability	Network Management requires tracking of availability. The MIB and device models must expose network and device availability information. 62351 Part 7 conveys relevant data model elements
	Provide Measurable High Reliability	Network Management requires tracking of availability. The MIB and device models must expose network and device availability information. 62351 Part 7 conveys relevant data model elements
	Provide Alternate Communications Paths	ACSE AP-Title and OID discussed in "***Emphasis on Interfaces***" provide independence from the underlying communications infrastructure. Devices are addressed independent of physical communications path.
	Automatically Re-Route Communications	ACSE AP-Title and OID discussed in "***Emphasis on Interfaces***" provide independence from the underlying communications infrastructure. Devices are addressed independent of physical communications path.
	Operate During Power Outages	The standards used in this guideline do not explicitly provide this capability. This capability is the responsibility of the applications and hardware design that make up AMI. However, the standards herein do not preclude this capability and do provide the technical means for implementation of this capability from a communications perspective.
	Take Advantage of the Potential for Interval Metering	ANSI C12.19 provides for interval metering by supporting the tables in Decade 6, These Tables provide structures for Load Profile data. ANSI C12.19 Annex J: XML File Format of TDL and EDL Files provides the ability to transport and store interval data using XML.
	Notify Consumers Promptly of Upcoming Events	The standards used in this guideline do not explicitly provide this capability. This capability is the responsibility of the applications that make up AMI. However, the standards herein do not preclude this capability and do provide the technical means for implementation of this capability.

Table 5-9
Satisfying Requirements for "Ease of Use"

	Requirement	Satisfied by
Ease of Use	Maximize the Information Consumers Know About their Energy Usage	The standards used in this guideline do not explicitly provide this capability. This capability is the responsibility of the applications that make up AMI. However, the standards herein do not preclude this capability and do provide the technical means for implementation of this capability.
	Maximize the Number of Ways a Consumer Can See their Data	
	Minimize the Actions a Consumer Must Take to Participate	
	Encourage the Consumer to Feel in Control of Their Energy Usage	

Table 5-10
Satisfying Requirements for "Cost Effectiveness"

	Requirement	Satisfied by
Cost Effectiveness	Use and Reuse Two Way Networks	All of the standards used in this guideline provide a means for integrating systems amongst utilities and various business units or applications in a significantly less costly manner than possible without open standards. Security and role based access helps in sharing data and infrastructure as described in sections "Ensuring Coexistence and Security" and "Support for Role Based Access Control". Utilizing security and role based access allows multiple applications to reuse deployed infrastructure for multiple purposes.
	Minimize Site Visits	All of the communications standards specified in this guideline provide remote command, control and data retrieval capabilities. Additionally, section "Manage Change" describes a means to remotely upgrade device software.
	Permit Remote Upgrades	Refer to section "Manage Change".

Table 5-11
Satisfying Requirements for "Standards"

	Requirement	Satisfied by
Standards	Use Open Published Standards	All of the standards cited in this guideline are published and publicly available.
	Reuse Industry Knowledge and Experience	All of the standards cited in this guideline have taken years to develop and have incorporated the knowledge and experience of significant numbers of contributing authors and companies representing the utility, equipment manufacturers, and general information technology industries.

Table 5-12
Satisfying Requirements for "Openness"

	Requirement	Satisfied by
Openness	Plan for Evolution	The tenets of this document and the nature of the standards referenced in this section have the primary goal of facilitating evolution of systems and applications.
	Permit Coexistence	Security and role based access helps in sharing data and infrastructure as described in sections "Ensuring Coexistence and Security" and "Support for Role Based Access Control".
	Reduce Economic Barriers to Interoperability	The selection of key points of interoperability and standardizing on them directly impacts and seeks to minimize the economic barriers to integration.
	Well Defined Published Interfaces and Points of Interoperability	All of the standards cited in this guideline are published and publicly available and describe interfacing methodologies and key points of interoperability.

Table 5-13
Satisfying Requirements for "Security"

<table>
<tr><th></th><th>Requirement</th><th>Satisfied by</th></tr>
<tr><td rowspan="3">Security</td><td>Ensuring Coexistence and Security</td><td>Communications authentication and cipher technologies are designed to prevent unauthorized access to data and/or services provided by the devices and network elements. These standards provide various cipher and authentication techniques.

Role based access helps in providing coexistence as described in section "Support for Role Based Access Control".

Also see "Security Support for Devices"</td></tr>
<tr><td>Deploy Minimum Levels of Cryptographic Capabilities</td><td>Each standard provides minimum levels of cryptographic capabilities as summarized in "Cipher And Related Algorithms Supported By Devices".

In addition:
<table>
<tr><td>Secure storage of cryptographic credentials</td><td>N/A</td><td>N/A</td><td>N/A</td></tr>
<tr><td>Software-updateable encryption algorithms</td><td>See "Manage Change"</td><td>See "Manage Change"</td><td>See "Manage Change"</td></tr>
<tr><td>Role-based authentication on local maintenance ports</td><td>ACSE Authentication</td><td>BACnet should be augmented with ACSE services</td><td>ACSE Authentication</td></tr>
</table></td></tr>
<tr><td>Plan for Remote Upgrading</td><td>Refer to section "Manage Change" for device upgrade mechanisms.</td></tr>
</table>

	Permit the Implementation of Adequate Security Policy	Authentication and authorization, see: ***0 ACSE and Conveyance to the Application Layer, 0 Security*** Auditing, see: ***Log Significant Events*** Confidentiality, see: ***Prevent Unauthorized Access, Protect Business Information, Protect Consumer Information, Ensuring Coexistence and Security*** Integrity, see: ***Prevent Unauthorized Access, Protect Business Information, Protect Consumer Information, Ensuring Coexistence and Security, Log Significant Events*** Availability, see: ***Provide Measurable High Availability***
	Protect Consumer Information	Communications authentication and cipher technologies are designed to prevent unauthorized access to data and/or services provided by the devices and network elements. Refer to sections "***Ensuring Coexistence and Security***" and "Support for Role Based Access Control".
	Protect Business Information	Communications authentication and cipher technologies are designed to prevent unauthorized access to data and/or services provided by the devices and network elements. Refer to sections "***Ensuring Coexistence and Security***" and "***Support for Role Based Access Control***".
	Prevent Unauthorized Access	Communications authentication and cipher technologies are designed to prevent unauthorized access to data and/or services provided by the devices and network elements. Refer to sections "***Ensuring Coexistence and Security***" and "***Support for Role Based Access Control***".
	Add or Remove Credentials Promptly	Centralized management of security information may be accomplished through the same device and network management capabilities outlined in section "***Manage Networks***".
	Authorize Access Using Roles	See summary in "***Support for Role Based Access Control***".
	Authenticate using Multiple Factors	This requirement applies to end users and the human interface to a system. From the standpoint of messaging and interfaces the authentication and encryption mechanisms described in this section are used to provide security over a given interface.

	Ensure System Availability	Provide multiple message paths so if one path is overwhelmed, another can be used: ACSE AP-Title and OIDs allow interfacing independent of communications infrastructure. This leaves message routing and forwarding to the "network layers" as described in section "***Device, Data, Service and Identifiable Entities*** ". Provide "stopping points" where messages can be filtered based on their source or destination address or other criteria: Both 61850 and C12 ASCE's Authentication-value used for role based access facilitates filtering. Measure network statistics and raise alarms when unusual numbers of messages are transmitted: Appropriate network statistics should be added according to section "***Manage Networks*** ". Provide "defense in depth" in which additional credentials are needed to access the most vital information in the system, and fewer users are permitted access: ACSE role based access control provides the mechanism by which access to differ data or services requires differing levels of authentication and/or encryption.
	Apply Security at All Exposed Interfaces	Communications authentication and cipher technologies are designed to prevent unauthorized access to data and/or services provided by the devices and network elements. Refer to sections "***Ensuring Coexistence and Security***" and "***Support for Role Based Access Control***".
	Log Significant Events	See section "0 Support for Logging" for capabilities supporting logging and event reporting.

Table 5-14
Satisfying Requirements for "Extensibility"

<table>
<tr><th></th><th>Requirement</th><th>Satisfied by</th></tr>
<tr><td rowspan="2">Extensibility</td><td>Self Announcement</td><td>Each of the standards specified provide mechanisms for reporting information in an unsolicited manner. These capabilities may be utilized to announce the availability, installation, configuration or commissioning of the device.

<table>
<tr><th>Standard</th><th>References</th></tr>
<tr><td>61850</td><td>61850-8-1_R0-9_CD_2001-08-29.doc IEC 61850-1 Section 16.1.3 Reporting Services</td></tr>
<tr><td>BACnet</td><td>135_2004new.pdf ANSI/ASHRAE Standard 135-2004 Section "13 ALARM AND EVENT SERVICES"</td></tr>
<tr><td>C12</td><td>ANSI C12.22-2007 Annex E - One-way Devices

Second paragraph describes "ACSE unsolicited messages to the C12.22 Network"</td></tr>
</table></td></tr>
<tr><td>Self Description</td><td>The 61850, CIM, BACnet and C12 standards all provide mechanisms by which device data attributes can be modeled. It is recommended that these standards are followed for modeling the appropriate end devices. These standards also provide mechanisms by which data models and attributes themselves may be queried from end devices or central data model repositories. Used in conjunction these capabilities provide the ability to discover device capabilities either at "run-time" or "design-time". The level of each is somewhat dependant on software services or gateway/protocol translations available at different levels. Depending upon specific application requirements direct support or translation methods are equally viable, however, minimization of translation is advisable.

<table>
<tr><th>Standard</th><th>References</th><th>Notes</th></tr>
<tr><td>61850</td><td>IEC 61850-6

61850-7-2_Ed2_Complete_R0-02_2007-05-05.pdf section 6.2.1 Overview of directory and GetDefinition services</td><td>Describes the use of an XML based Substation Configuration description Language (SCL). SCL is used to describe device configuration, parameters, communications system configurations and the relations between them.

Example in 61850 part 6.</td></tr>
</table></td></tr>
</table>

		BACnet	ANSI/ASHRAE Addendum d to ANSI/ASHRAE Standard 135-2004 Section 135-2004d-1	Control devices are modeled as a collection of objects. BACnet provides object access services. BACnet should be supplemented with 61850 SCL concepts. The BACnet structured view object allows acquisition of device model information.
		C12	Table 0 GEN_CONFIG_RCD. DEVICE_CLASS And corresponding EDL file provided by the manufacturer. Table 5, 6 or 3 has url (web url) or ref to the data (which tables)	Utilizes Protocol Specification For Electric Metering (PSEM) EDL file- describes meter data Table Description Language and read/write services 0 table describes major properties (i.e.) can define number of tables Big/little endian
	Information and Object Modeling	**Standard**	**References**	
		61850	SCL,DER	
		BACnet	ANSI/ASHRAE Addendum d to ANSI/ASHRAE Standard 135-2004 Section 135-2004d-1	
		C12	ANSI C12.19 200X (meter data model) and ANSI C12.22 200X (meter communications)	
	Technology Independence and Protocol Layering	**Common Set of Application Level Semantics** Base metering on ANSI C12.19 200X (meter data model) and ANSI C12.22 200X (meter communications). These two standards are entering the editorial phase and implementations have begun. They support a full XML data model for meter model		

		and data exchange, as well as, full support for encryption and authentication of all messaging and network management. In fact, in the ANSI C12.19 revision (this is the first update to the standard first published in 1997) there is an excellent complete meter model in an annex that can be used as a building block for interoperable and standardized metering. Note that these standards comprise everything that has been learned in the implementation of AMR using ANSI standards over dozens of years and hundreds of developers. These versions build on and extend the existing protocols and address crucial extended requirements for security and network management. Base metering on ANSI C12.19 200X (meter data model) and ANSI C12.22 200X (meter communications). The meter model for all views of metering data is based on the AEIC recommendations on the application of C12.19. In addition the C12.22 external interface and the C12.22 internal interface (if exposed) is utilized. For 61850, a translated version of the C12 meter model is used. **Common Application Layer Interface:** ACSE is a common standard for the representation and encoding of the transfer of application layer semantics to the application layer. There are two key advantages to the use of this at the present time – First, it is part of 61850, DLMS, ANSI C12.22. Second, it provides a standard way of conveying a minimum set of semantics to the application layer that might otherwise be lost to the communications stack filtering. Among the key elements of this "header" are – access role, encryption mechanism, application globally unique identifier.
	Modular Design and Scalability	The use of any of the standards specified in this sample guideline help achieve a level of modular design. For example if an AMR system that conforms to C12 is deployed and a 61580 SCL model of that system is exposed then replacement of the vendor specific implementation of the AMR system or components should be trivial. Also, interoperability between different products conforming to a given standard provides the ability to interchange products without adverse affects. Each of the standards specified in this guideline accommodates scalability through communications and addressing techniques (identifiers) that impose no restrictions on deployment sizes.

Table 5-15
Satisfying Requirements for "Manageability"

<table>
<tr><th></th><th>Requirement</th><th>Satisfied by</th></tr>
<tr><td rowspan="3">Manageability</td><td>Develop Systems and Network Management Requirements Up Front</td><td>Network Management and Security requirements in this guideline satisfy this requirement. See sections "0 Device and Network Management" and "0 Security".</td></tr>
<tr><td>Manage Devices</td><td>See "Manage Networks", "Manage Configuration", "Manage Change".</td></tr>
<tr><td>Synchronize Time</td><td>Time synchronization with end devices may be accomplished through the references citing in the following table.

The standards cited in this guideline require enhancements regarding clock resolution and clock uncertainty. These capabilities appear to be minimally supported in the standards cited.

<table>
<tr><th>Standard</th><th>References</th></tr>
<tr><td>61850</td><td>61850-7-2/Ed2 Draft © IEC(E) section "18 Time and time-synchronization model"

61850-8-1 Section "20 Time model"

"SCSM Specified time synchronization mechanism - The Simple Network Time Protocol (SNTP) shall be used for synchronization (see clause 5.5)."

Specifies SNTP RFC 2030 and NTP

Time Master – STIM

For the accuracy of time requirements, five classes are defined in 13.7.6 of this part of IEC 61850.

time master STIM, device clock in LLN0.</td></tr>
<tr><td>BACnet</td><td>BACnetNISTR6392.pdf Sections:

A.5.13 BIBB - Device Management - UTCTimeSynchronization - A (DM-UTC-A))

A.5.14 BIBB - Device Management - UTCTimeSynchronization - B (DM-UTC-B))</td></tr>
</table>
</td></tr>
</table>

			ANSI/ASHRAE Standard 135-2004 (135_2004new.pdf): K.5.13 BIBB - Device Management-UTCTimeSynchronization-A (DM-UTC-A) K.5.14 BIBB - Device Management-UTCTimeSynchronization-B (DM-UTC-B) 16.8 UTCTimeSynchronization Service
		C12	Table 00 General Configuration Table, tm_format Table 51 Actual Time and TOU Table Table 52 Clock Table Table 53 Time Offset Table Table 55 Clock State Table C12.19 Meter model does not expose the quality of its time, just its precision.
	Manage Networks		

Standard	References	Notes
61850	LPHD and LLN0 may provided a basis for device and network management models Additionally, 62351 Part 7 conveys relevant data model elements	Does not have but will have NM SNMP uses the same encoding as ASN.1 / MMS set, get, trap SCL can be used to model NM data elements. RMON should outline details. May need to extend LPHD and LLN0 following RMON/SNMP examples
BACnet	22.2.1.5 Device and Network Management K.5 Device and Network	Control devices are modeled as a collection of objects.

			Management BIBBs	BACnet provides object access services. BACnet should be supplemented with 61850 SCL concepts. The BACnet structured view object allows acquisition of device model information. May need to extend BIBBs following RMON/SNMP examples
		C12	C12-22DocumentforBallot7-07.doc Annex C C.1 Decade 12 TABLE 127 Network Statistics Table	The network management services such as the <register>, <deregister>, <resolve> and <trace> services may be transmitted authenticated but not encrypted. May need to extend network statistics table following RMON/SNMP examples
	Manage Configuration	Section "0ACSE and Conveyance to the Application Layer" describes the use of ACSE AP-Title OID as a means up standardizing globally unique identifiers. Each device model should expose an OID conveying or representing device-specific standard configuration settings.		

Standard	References
61850	ACSE AP-Title for end point id LN0 model should include configuration ID (OID) as a base data element for all IEDs Additionally, 62351 Part 7 conveys relevant data model elements
BACnet	object_identifier/BACnetObjectIdentifier 12.10 Device Object Type

			BACnet should be augmented with ACSE OIDs.
		C12	C12.22 AP-Title for end point id, and Table 0 meter class for configuration ID.
	Manage Change	Remote image change may be provided through the use of Trivial File Transfer Protocol (TFTP) as specified in the following standards: RFC 1350 THE TFTP PROTOCOL (REVISION 2) RFC 1785TFTP Option Negotiation Analysis RFC 2347 TFTP Option Extension RFC 2348 TFTP Blocksize Option RFC 2349TFTP Timeout Interval and Transfer Size Options Alternatively, 61850 provides file transfer mechanisms which may be used where supported, specifically, 61850-7-2_Ed2_Complete_R0-02_2007-05-05.pdf "Section 20 File transfer."	

6
SUMMARY AND CONCLUSIONS

This report identifies some of the key points and concepts that utilities and energy service providers should consider when specifying or building systems. The questions and examples should be considered starting points for how to think about requirements for next generation metering and customer communication systems. While there is significant standards and infrastructure work that can be adopted by the implementers, there is more work to do in some key areas related to integration of systems and development of industry level networks.

This report endeavors to encourage deployment of advanced metering and customer communications technologies that are open, standard, upgradeable, and interoperable. It does this by focusing on key requirements and key points of interoperability for application integration.

The two principal quantitative components of the document are a set of "no regrets" requirements along with a checklist to assess these criteria, and, a sample guideline suggesting a set of open standards that can substantially meet the "no regrets" requirements.

The paper "walks a line" between describing key points of interoperability where standardization is extremely valuable, and preserving the capability for the discretion, innovation and diversity on the part of vendors and project managers necessary for robust applications development.

In general, these recommendations represent a framework within which system integration can be achieved in a way that is cost effective, enables multiple vendors equipment to be deployed in the field, reduces time to implement, and improves the chances of project success. These attributes allow system integration to be used to connect what were once islands of automation into a much larger intelligent system that can address the increasing demands being placed on the electric power infrastructure.

Recommendations for Future Work

- Detail required implementation agreements for the type of implementation example described here. Results of this extension could result in documents developed and maintained within appropriate users groups. Such documentation should be supported by actual implementations demonstrating the concepts and boundaries of the key points of interoperability. Examples of such documents would be agreements about:
    - How to automatically provide gateways or adaptors between technologies
    - When certain protocol features must be enabled
    - How objects defined in one information model map to those in another
    - What values certain addresses or protocol timing parameters must be set to.

- An overall agreement for a complete profile similar to the one provided as sample guidelines here. This overall agreement would ideally be ratified by a group of utilities in addition to a group of vendors.
- In order to implement the sample guidelines suggested here, the BACnet protocol choices should be augmented with ASCE allowing for role based security and access rights ACSE OIDs. This might be developed and conveyed to the ASHRAE SPC135 committee for incorporation as an addendum.
- Clock resolution and uncertainty appear to be minimally supported in some of the standards cited. For instance, extensions to C12.19 and ASHRAE BACnet could be proposed and conveyed to the corresponding standards organization.
- Modeling techniques allowing for "role" based access definitions and data access rights within the data modeling language or data models themselves would be beneficial to the industry. While the assertion of role can be conveyed through some of these standards, its use and management is not yet a part of the standards that might utilize it to constrain messaging based on access role.
- An area open for improvement in the standards cited in this guideline is that of network address translation. A means of standardizing translation from application layer addresses to communications addresses at the various networking layers would be beneficial. It is additionally valuable to resolve how OIDs and IPv6 addresses can integrated so that a homogeneous applications and communications addressing scheme can be achieved.

7
REFERENCES

This section lists references used or relevant to the contents of this report.

North American Standards

[1] ANSI C12.18 Protocol Specification for ANSI Type 2 Optical Port

[2] ANSI C12.19 2007: Utility Industry End Device Data Tables (note: not yet formally released)

[3] ANSI C12.21 Protocol Specification for Telephone Modem Communication

[4] ANSI C12.22 2007 Protocol Specification for Data Communication Networks (note: not yet formally released)

[5] ANSI C12.23 Compliance Testing for ANSI C12.19-1997, IEEE 1377-1997, MC

[6] RP1011: ASHRAE research project 1011, Utility/Energy Management and Control Systems (EMCS) Communication Protocol Requirements

[7] FIPS PUB 180, Secure Hash Standard

[8] FIPS PUB 46-2, Data Encryption Standard

[9] FIPS PUB 186, Digital Signature Standard (DSS)

[10] FIPS PUB 197, Advanced Encryption Standard (AES)

[11] CMIP: X.700 Management framework for Open Systems Interconnection (OSI) for CCITT applications

[12] ITU X.217: Information technology - Open Systems Interconnection - Service definition for the Association Control Service Element

[13] ITU X.227: Information technology - Open Systems Interconnection - Connection-oriented protocol for the Association Control Service Element: Protocol specification

[14] ITU X.237: Information technology - Open Systems Interconnection - Connectionless protocol for the Association Control Service Element: Protocol specification

Trade Groups

[15] AEIC Guidelines for implementing ANSI C12.19-1997, “Utility Industry End Device Data Tables”. http://www.aeic.org/meter_service/GuidelinesWGFinal.doc

[16] Open AMI. http://sharepoint.ucausersgroup.org/OpenAMI/

ISO/IEC

[17] ISO 9506-1:1990, ISO 9506-2:1990: Industrial automation systems -- Manufacturing Message Specification

[18] IEC 61850-6: Communication networks and systems in substations – Part 6: Substation automation system configuration language

[19] IEC 61850-7-420 Ed.1: Communication networks and systems in substations - Part 7-420: Communications systems for distributed energy resources (DER) - Logical nodes

[20] IEC61970: Energy management system application program interface (EMS-API)

[21] IEEE 37.118 IEEE Standard 37.118-2005, Standard for Synchrophasors for Power Systems, approved by IEEE Board but not yet published. The IEC60870-6 Telecontrol Application Service Element 2 (TASE.2)

[22] ISO/IEC 10731:1994 Information technology -- Open Systems Interconnection -- Basic Reference Model

[23] ISO/IEC 7498-1 Information Technology - Open Systems Interconnection - Basic Reference Model: The Basic Model.

[24] ISO/IEC 13239:2002 Information Technology - Telecommunications and information exchange between systems - High-level data link control (HDLC) procedures - Frame Structure, Annex A Explanatory Notes On Implementation of the Frame Checking Sequence.

[25] ISO/IEC 8824-1:2002 Information technology - Abstract Syntax Notation One (ASN.1): Specification of basic notation.

[26] ISO/IEC 8824-2:2002 Information technology - Abstract Syntax Notation One (ASN.1): Information Object Specification.

[27] ISO/IEC 8824-3:2002 Information technology - Abstract Syntax Notation One (ASN.1): Constraint specification.

[28] ISO/IEC 8824-4:2002 Information technology Abstract Syntax Notation One (ASN.1): Parameterization of ASN.1 specifications.

[29] ISO/IEC 8825-1:2002 Information technology - ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER).

[30] ISO/IEC 8650-1:1996 Information Technology – Open Systems Interconnection – Connection-Oriented Protocol for the Association Control Service Element: Protocol Specification.

[31] ISO/IEC 15954:1999 Information technology – Open Systems Interconnection – Connection-mode protocol for the Application Service Object Association Control Service Element.

[32] ISO/IEC 15955:1999 Information technology – Open Systems Interconnection – Connectionless protocol for the application service object Association control service.

[33] ISO/IEC 10035-1:1995 Information Technology – Open Systems Interconnection – Connectionless Protocol for the Association Control Service Element: Protocol Specification

[34] ISO/IEC 646: 1991 ASCII character set.

[35] ATIS T1.667-1999 ATIS T1.667-2002 Intelligent Network (Revision of T1.667-1999): May 2002.

[36] ISO/IEC 10731:1994 Information technology -- Open Systems Interconnection -- Basic Reference Model

[37] IEC61850-7: Communications Networks and Systems in Substations – Part 7: Basic Communication Structure for Substations and Feeder Equipment

[38] IEC60870-6 Telecontrol Application Service Element 2 (TASE.2)

[39] International Organization for Standardization, *Open Distributed Processing – Reference Model - Part 1: "Overview"*, ITU-T X.901 and ISO 10746-1

[40] International Organization for Standardization, *Open Distributed Processing – Reference Model - Part 2: "Foundations"*, ITU-T X.902 and ISO 10746-2

[41] International Organization for Standardization, *Open Distributed Processing – Reference Model - Part 3: "Architecture"*, ITU-T X.903 and ISO 10746-3

[42] International Organization for Standardization, Open Distributed Processing – Reference Model - Part 4: "Architectural Semantics", ITU-T X.904 and ISO 10746-4

Internet RFCs

[43] RMON1: RFC 2819 Remote Network Monitoring Management Information Base

[44] RMON2: RFC 2021Remote Network Monitoring Management Information Base Version 2 using SMIv2

[45] SNMPv3: RFC 3411 An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks

[46] SNMPv3: RFC 3418 Management Information Base (MIB) for the Simple Network Management Protocol (SNMP)

[47] CMIS: RFC 1095: The Common Management Information Services and Protocol over TCP/IP

[48] CMIS: RFC 1189: The Common Management Information Services and Protocols for the Internet

[49] RFC 1350 THE TFTP PROTOCOL (REVISION 2)

[50] RFC 1785TFTP Option Negotiation Analysis

[51] RFC 2347 TFTP Option Extension

[52] RFC 2348 TFTP Blocksize Option

[53] RFC 2349TFTP Timeout Interval and Transfer Size Options

Other

[54] Integrated Energy and Communications System Architecture (IECSA), Volume I-IV, Electricity Innovation Institute Consortium for Electric Infrastructure to Support a Digital

Society (CEIDS). (Note: the term IECSA is being phased out; the new name for this effort is “IntelliGrid Architecture” and it continues to be sponsored by CEIDS.

[55] Booch, Jacobson, Rumbaugh; *The Unified Modeling Language User Guide*, Second Edition Addison-Wesley, 2005

[56] EPRI Technical Report: Harmonization of IEC 61970, 61968, and 61850 Models, EPRI, Palo Alto, CA, 2006.

A
APPENDIX A: POTENTIAL BENEFITS OF AMI AND DR

This list was generated as part of EPRI's Dynamic Energy Management initiative and is intended as a resource for utilities considering implementing advanced metering and demand response. This is a short summary; more information is available from EPRI on the details of each benefit and regarding which AMI functions enable which benefits.

Enhance Revenue

Benefits in this category indicate increased revenue for the utility, either because the AMI system creates the opportunity for new products, services and business ventures, or because the AMI system permits the recovery of revenue that would otherwise be missed.

- Improve billing accuracy
- Target customer marketing
- Reduce "idle usage"
- Improve billing cash flow
- Recover missing revenue
- Add new revenue source
- Add new business venture
- Add new product
- Add new service
- Better identify energy theft
- Increase revenue program participation

Improve Reliability

Benefits in this category indicate improved reliability in the power system because the AMI system enhances demand response programs, outage management, advanced distribution automation, and integration of distributed generation.

- Detect outages sooner
- Locate faults sooner
- Avoid emergency load shedding
- Reduce grid instability
- Resolve outages more quickly
- Shift demand to off-peak
- Add to capacity buffer

- Switch fuels dynamically
- Integrate distributed generation
- Increase reliability program participation

Improve Service

Benefits in this category indicate improved service to customers, business clients, and society at large.

- Improve billing timeliness
- Permit customized billing date
- Lower customer bills
- Customer feels more control
- Add billing option
- Add rate option
- Customer is more aware of service
- Customer has more choices
- Comply with laws or regulations

Reduce Management Costs

Benefits in this category indicate reduced costs in areas not directly related to operations, such as capital equipment, planning, inventory costs, legal and tax costs.

- Reduce meter reader equipment
- Reduce maintenance equipment
- Reduce meter procurement costs
- Reduce office support expenses
- Better identify unbilled account errors
- Reduce costs of resolving disputes
- Improve system planning
- Defer building additional generation
- Defer building additional T&D
- Reduce net emissions
- Reduce meter inventories
- Reduce inventory expenses
- Improve tax position

Reduce Operational Costs

Benefits in this category indicate reduced costs in areas related to the daily operation of the utility, such as labor, transportation, maintenance, installation, and energy procurement.

- Reduce meter reader labor
- Reduce maintenance labor
- Reduce installation labor
- Reduce customer service labor
- Reduce site visits
- Better identify broken meters
- Better identify failed meters
- Better identify misconfigured meters
- Better identify communications failures
- Better identify meter location
- Reduce installation errors
- Automatically perform load survey
- Reduce energy procurement costs
- Reduce system energy losses
- Reduce meter energy losses
- Reduce battery replacement
- Reduce calendar resets
- Reduce meter reprogramming
- Increase cost reduction program participation

B
APPENDIX B: INDUSTRY ACTIVITIES

AEIC: Association of Edison Illuminating Companies

Website: http://www.aeic.org/

About AEIC: AEIC has six technical committees. The Meter and Service Technical Committee provides direction for the industry by studying new technology and reporting operating experience of electric metering equipment and the introduction of service entrance conductors into customer facilities. The Committee maintains representation on ANSI, EPRI, UL, and industry committees to promote metering standardization and research. AEIC's Meter and Service Committee conducts a Joint National Metering Conference with EEI Metering Committee twice a year.

AMI-Enterprise

Website:http://sharepoint.ucausersgroup.org/AM-Ent/ (under construction)

About AMI-Enterprise: AMI-Enterprise is a user community affiliated with the UCA International Users Group, a non-profit organization whose members are utilities, vendors, and users of communications for utility automation. (More info required.)

AMI-SEC: AMI Security

Website:http://sharepoint.ucausersgroup.org/AMISec/ (under construction)

About AMI-Sec: AMI-SEC is a user community affiliated with the UCA International Users Group, a non-profit organization whose members are utilities, vendors, and users of communications for utility automation.

AMRA

Website: http://www.amra-intl.org/

About AMRA: AMRA is a nonprofit association providing utilities information about innovative technologies that lead to improved operations, customer service and resource utilization. Its membership represents more than 800 international utilities and corporations in gas, water and electric industries. AMRA members develop and implement automated resource-management technologies as well as participate in standardization and regulatory activities.

Vision: To be the premier advocate for automated metering technologies and the value they bring to utilities and their customers.

Mission Statement: AMRA is an industry association whose members own, manage, provide and/or support automated metering systems, related technologies and the data acquired. AMRA's purpose is to foster a favorable business, regulatory and technical environment in which its members will succeed.

AMRA strives to accomplish this for its members by being:

- A leader in identifying automated metering system solutions and facilitating business and operational opportunities in a changing environment.
- A primary provider of education and information.
- A forum for the exchange of ideas and experiences.
- An advocate on technological, business, legislative and regulatory issues.

AMRA Members: AMRA is designed to be a resource for corporations, utility departments or authorities, associations, public interest groups and others interested in the development and application of advanced metering and communications services. Members include representatives of ...

- Electric, gas, and water utilities
- Telemetry service users
- Communications carriers
- Manufacturers of communications systems and components
- Standards organizations
- Industry associations
- Regulatory agencies
- Vendors of utility automation products and services
- Consulting companies
- Research organizations
- Investment analysis

DOE GridWise Architecture Council

Website: http://www.gridwise.com

About GridWise: GridWise is an entirely new way to think about how we generate, distribute and use energy. Using advanced communications and up-to-date information technology, GridWise will improve coordination between supply and demand, and enable a smarter, more efficient, secure and reliable electric power system.

The Challenge: The nation's prosperity and the American way of life depend upon efficient and affordable energy. Without a major shift in the way the energy system is planned, built and

operated, the U.S. will invest nearly $500 billion in conventional electric infrastructure over the next 20 years to meet expected growth. Minimizing the cost of new electric infrastructure is key to strengthening the U.S. economy.

In the spring of 2000, technical leaders at PNNL began to think about how energy systems would evolve in the first decades of the 21st Century. Experts in the electric power grid, skilled in transmission system dynamics and analyses of blackouts, had also been engaged in trying to understand and shape the potential influence of broadly integrated distributed resources, such as distributed generation and load management. In parallel, energy scientists had seen the enormous opportunity for automated diagnostic systems to identify energy waste in commercial building energy systems. The backdrop of California's electricity crisis highlighted how existing energy markets frustrated the introduction of new technologies that could really make a difference.

The convergence of these ideas led to the notion that information technology is the key catalyst and enabler for realizing the potential of new energy technologies to transform the electric power system. Information technology is vital to transforming the electric power system from a rigid, hierarchical system to a collaborative, distributed, commerce-driven "society" of devices that would enhance the utilization of expensive assets and simultaneously increase reliability and security.

Vision: GridWise seeks to modernize the nation's electric system – from central generation to customer appliances and equipment – and create a collaborative network filled with information and abundant market-based opportunities. Through GridWise, we can weave together the most productive elements of our traditional infrastructure with new, seamless plug-and-play technologies. Using advanced telecommunications, information and control methods, we can create a "society" of devices that functions as an integrated, transactive system.

Stakeholders: Secure, reliable and affordable energy is critical to the nation's prosperity, yet national security concerns as well as power blackouts and other recent events have focused attention on the vulnerabilities of our energy infrastructure and on the substantial impact of large power outages on the nation's economy and our quality of life.

By achieving an end-to-end transformation of our energy system, GridWise will create new business opportunities for products and services as well as deliver secure, reliable and cost-effective energy. This will benefit businesses and industry, the government, individual consumers, and the country as a whole.

Architecture Council: The GridWise™ Architecture Council assembles a focused team of experts to articulate the guiding principles that constitute the architecture of a future, intelligent, transactive, energy system and see that GridWise evolutionary directions remain true to these principles.

The Architecture Council comprises practitioners and leaders with broad-based knowledge and expertise in power, information technology, telecommunications, financial systems, and additional relevant sectors working together toward a coordinated GridWise vision—the transformation of the nation's energy system into a rich, collaborative network filled with decision-making information exchange and market-based opportunities.

DOE GridWise Program

Website: http://www.electricdistribution.ctc.com/

About the Program: The Electric Distribution Program supports distribution grid modernization through development and use of advanced sensor, communication, control, and information technologies to enable GridWise™ operations of all distribution systems and components for interoperability and seamless integration.

The term GridWise denotes the operating principle of a modernized electric infrastructure that provides open but secure system architecture. Communication techniques and associated standards are used throughout the electric grid to provide value and choices to electricity consumers.

The Electric Distribution Program addresses critical technology areas - Distributed Sensors, Intelligence, Smart Controls, and Distributed Energy Resources– identified in the National Electric Delivery Technologies Roadmap, which defines technology pathways to achieving the Grid 2030 Vision.

The Electric Distribution Program operates the Electric Distribution Transformation (EDT) Program and the GridWise Initiative, both within the U.S. Department of Energy Office of Electricity Delivery & Energy Reliability (OE), which is leading a national effort to help modernize and expand America's electric delivery system to ensure economic and national security.

EPRI IntelliGrid

Website: http://www.epri.com

About EPRI: The Electric Power Research Institute (EPRI), with major locations in Palo Alto, California; Charlotte, North Carolina; and Knoxville, Tennessee, was established in 1973 as an independent, nonprofit center for public interest energy and environmental research. EPRI brings together members, participants, the Institute's scientists and engineers, and other leading experts to work collaboratively on solutions to the challenges of electric power. These solutions span nearly every area of electricity generation, delivery, and use, including health, safety, and environment. EPRI's members represent over 90% of the electricity generated in the United States. International participation represents nearly 15% of EPRI's total research, development, and demonstration program.

The IntelliGrid Vision (http://www.epri.com/intelligrid)**:** The vision of an intelligent grid (or IntelliGrid) is the vision for the electric delivery system of the future. Taken as a whole, reaching this vision will yield unprecedented benefits for the industry -- utility, consumers and society will all see rewards through increased reliability, reduced O&M costs, avoidance of new capacity, and increased customer satisfaction. The new intelligent electric delivery infrastructure will offer unprecedented flexibility and functionality; heightened levels of power security, quality, reliability, and availability; enhanced customer satisfaction and choice; and expansive

opportunities for economic and business development. The power delivery system of the future will be integrated, self-healing, and electronically controlled – offering extraordinary resiliency and responsiveness. Such an evolution requires a resistance to the lure of easier short-term solutions made with a "silo" mentality – one without regards to the needs of other parts of the grid. The process is the key to our success. Success requires adoption by the industry. Adoption requires buy-in by industry leaders. Buy-in requires active participation by leaders at each step along the way.

IntelliGrid provides the methodology for deploying intelligent grid systems, with specific support provided for guiding system *integration*, *interoperability*, and *management*. A utility's requirements can be abstracted into a *technology-neutral architecture*. The architectural components include *common services*, *information models*, and *system interfaces*. From that point, utilities have the freedom to choose among recommended, mainstream technologies to fulfill the architectural framework, while constructing *common technology infrastructure* that best meets their business needs.

Applicability to the Utility/Customer Interface: In particular, IntelliGrid applies to the environment that encompasses communications between end customers and the utility, aggregator, or energy service provider (ESP) to which they are connected. This environment includes traditional Automatic Meter Reading applications and newer ones supported by Advanced Metering Infrastructure (AMI). Newer applications include remote meter management, real-time pricing, management of distributed energy resources on customer premises, and demand response.

GridWise Alliance

Website: http://www.gridwise.org

About the GridWise Alliance: The GridWise Alliance is a consortium of utilities and vendors promoting DOE's vision for smart grids. The Alliance members recognize that emerging energy and information technologies have the potential to radically improve the efficient use of the nation's energy system. The Alliance and its members advocate change locally, regionally, and nationally to promote new policies and technology solutions that move us closer to this vision.

Vision: The vision represents an electric system that integrates the infrastructure, processes, devices, information and market structure so that energy can be generated, distributed, and consumed more efficiently and cost effectively, thereby achieving a more resilient, secure and reliable energy system.

NETL Modern Grid Initiative

Website: http://www.themoderngrid.org/

About the Modern Grid Initiative: The National Energy Technology Laboratory's *Modern Grid Initiative (MGI)* seeks to accelerate the modernization of our nation's electricity grid. To

accomplish this, MGI is fostering the development of a common, national vision among grid stakeholders. The initiative is also working toward a framework that enables utilities, vendors, consumers, researchers and other stakeholders to form partnerships and overcome barriers. Finally, MGI supports demonstrations of systems of key technologies that can serve as the foundation for an integrated, modern power grid.

Our nation is increasingly held back by an outdated power delivery infrastructure. Designed in the 1960s or earlier, much of this critical national asset is well beyond its design life. The financial consequences of interruptions are growing into an enormous threat.

The power grid is increasingly operating at its limit, facing shortcomings in capacity, reliability, security and power quality. Smart investments must occur to replace aging infrastructure and expand capacity where necessary to meet increasing electricity demand. This investment represents a once-in-a-century opportunity to apply new technologies and systems rather than the antiquated designs and technologies of the 1960s and earlier. New advances in power delivery, communications and information technology have laid the groundwork for a modern grid. Proven effective in lab tests and field trials, these cutting-edge solutions offer dramatic improvements in power quality, service and cost savings.The technology is here, the challenges are manageable, and the benefits far outweigh the costs. Through collaboration and cooperation, we can renew the nation's power infrastructure in a phased, affordable way and create the foundation for our country's economic growth and prosperity.

The U.S. Department of Energy's (DOE) Office of Electricity Delivery and Energy Reliability (OE) sponsors the Modern Grid Initiative, aligning its efforts with existing programs such as Transmission Reliability, Electricity Distribution, GridWise Distributed Generation, GridWorks, and others. It builds on a national technology strategy that includes Grid 2030 and the National Electric Delivery Technologies Roadmap.

OpenAMI

Website: http://sharepoint.ucausersgroup.org/OpenAMI/

About OpenAMI: OpenAMI is a user community affiliated with the UCA International Users Group, a non-profit organization whose members are utilities, vendors, and users of communications for utility automation.

Organization: OpenAMI is represented by a Technical Subcommittee focused on OpenAMI issues, working in coordination with the UCA-IUG Technical Subcommittees representing the IEC61850 and CIM user communities.

Coordination: The UCA-IUG's UtilityAMI user community provides the "High-Level Advanced Metering Infrastructure and Demand Response System Requirements Input & Oversight" to the OpenAMI Task Force.

Deliverables: The OpenAMI Technical Subcommittee, which is organized into four cross-functional working groups, is expected to produce the following Advanced Metering & Demand Response deliverables:

- Common Requirements Specification
- Common Information & Data Model Specification
- Standards-based Reference Design Specifications
- AMI & DR System Interoperability Guidelines and Specifications

OpenHAN

Website: http://sharepoint.ucausersgroup.org/OpenHAN/

Overview: Recently, the members of UtilityAMI saw a need to provide direction to the vendor community and other stakeholders on what is needed to implement the utility/consumer communications interface for consumer devices and systems. The new group – OpenHAN - is developing use cases, requirements, security guidelines, and high-level architecture for the home area network and the devices connected to it from a utility applications point of view. This is a very active community that is engaging utilities, vendors, and regulators. The results will likely be seen most clearly when California adopts its mandatory programmable communicating thermostat regulations in late 2008 / early 2009.

OpenHAN is a task force of the UtilityAMI working group, operating under the auspices of the Utility Communications Architecture International Users Group (UCA-IUG).

Guiding Principles: The UtilityAMI HAN membership has unanimously voted to approve the following Guiding Principles upon which the remainder of its work will be based:

1. Support secure two-way communication between the AMI Network and the HAN
2. Support load control integration (e.g. distributed resource dispatch / control / relaying)
3. Provide direct access to usage and other meter data (e.g. kWhr, KW, Voltage, etc.)
4. Provide a platform for future customer-owned products that leverage meter data and utility/grid information
5. Support three types of communications: public price signaling, consumer-specific signaling, and control signaling
6. Support communications to other HAN devices with metering capability (e.g. gas and/or water meter communication, EV sub-metering, PV sub-metering, etc.)
7. Base the 'AMI network interface to HAN interface' on open standards
8. Promote implementation through high value and relatively low cost
9. Reduce the potential for technology obsolescence through use of multiple bridging options

Vision: At the recent OpenHAN meeting in San Diego, the three California IOU's (SCE, SDG&E, and PG&E) made a joint presentation on their vision of the Home Area Network as a means to implement utility end-use applications.

Use Cases & Requirements: SDG&E has contributed use cases and requirements for the Meter Home Area Network and In-Home Displays. These can be found under the Shared Documents section of the OpenHAN website.

UCA International Users Group

Website: http://sharepoint.ucausersgroup.org/

About UCA-IUG: This is the parent organization for OpenAMI, UtilityAMI, OpenHAN, the CIM Users Group, and the IEC 61850 Users Group. All these groups are developing best practices and standards necessary for modern, intelligent grid deployment.

UtilityAMI

Website: http://sharepoint.ucausersgroup.org/UtilityAMI/

About UtilityAMI: UtilityAMI is a forum to define serviceability, security and interoperability guidelines for advanced metering infrastructure (AMI) and demand responsive infrastructure (DRI) from a utility / energy service provider perspective.

Deliverables: UtilityAMI has developed high-level policy statements that can be used to facilitate efficient requirements and specification development using a common language that minimizes confusion and misunderstanding between utilities and vendors. UtilityAMI is coordinating with other industry groups as required to efficiently carry out its mission.

Objectives: UtilityAMI has a goal to utilize the UtilityAMI work products to influence the vendor community to produce products and services that utilities need to support their AMI and DRI initiatives.

High-Level Requirements: The UtilityAMI group associates the following high-level requirements with Advanced Metering Infrastructure (AMI).

7. Standard communications board interface
8. Standard data model
9. Security
10. Two-way communications
11. Remote download
12. Time-of-use metering
13. Bidirectional and net metering
14. Long-term data storage
15. Remote disconnect

16. Network management
17. Self-healing network
18. Home Area Network gateway
19. Multiple clients
20. Power quality assessment
21. Tamper and theft detection
22. Outage detection
23. Scalability
24. Self-locating

Tasks: The following task list defines UtilityAMI's primary objectives. These include development of a common vocabulary, providing policy guidance, identifying security needs, and guiding OpenAMI Working Group priorities.

25. Glossary and Common Language Framework
    - A universal AMI glossary of terms and definitions
    - A framework for technology capability evaluation
    - A common, minimum requirements definition document
26. Modular Meter Interface: Policy for modular communication interfaces in meters
27. Security: Security issues and their relationships to business needs
28. AMI Network Interface: Policy for AMI network to MDMS interfacing
29. Consumer Interface: Policy for Customer Portal interface to customer end user appliances
30. Back Office Interface: Policy for MDMS to enterprise back office system connectivity
31. General Issues Forum

Export Control Restrictions

Access to and use of EPRI Intellectual Property is granted with the specific understanding and requirement that responsibility for ensuring full compliance with all applicable U.S. and foreign export laws and regulations is being undertaken by you and your company. This includes an obligation to ensure that any individual receiving access hereunder who is not a U.S. citizen or permanent U.S. resident is permitted access under applicable U.S. and foreign export laws and regulations. In the event you are uncertain whether you or your company may lawfully obtain access to this EPRI Intellectual Property, you acknowledge that it is your obligation to consult with your company's legal counsel to determine whether this access is lawful. Although EPRI may make available on a case-by-case basis an informal assessment of the applicable U.S. export classification for specific EPRI Intellectual Property, you and your company acknowledge that this assessment is solely for informational purposes and not for reliance purposes. You and your company acknowledge that it is still the obligation of you and your company to make your own assessment of the applicable U.S. export classification and ensure compliance accordingly. You and your company understand and acknowledge your obligations to make a prompt report to EPRI and the appropriate authorities regarding any access to or use of EPRI Intellectual Property hereunder that may be in violation of applicable U.S. or foreign export laws or regulations.

The Electric Power Research Institute (EPRI), with major locations in Palo Alto, California; Charlotte, North Carolina; and Knoxville, Tennessee, was established in 1973 as an independent, nonprofit center for public interest energy and environmental research. EPRI brings together members, participants, the Institute's scientists and engineers, and other leading experts to work collaboratively on solutions to the challenges of electric power. These solutions span nearly every area of electricity generation, delivery, and use, including health, safety, and environment. EPRI's members represent over 90% of the electricity generated in the United States. International participation represents nearly 15% of EPRI's total research, development, and demonstration program.

Together…Shaping the Future of Electricity

© 2008 Electric Power Research Institute (EPRI), Inc. All rights reserved.
Electric Power Research Institute, EPRI, and TOGETHER…SHAPING THE FUTURE OF ELECTRICITY are registered service marks of the Electric Power Research Institute, Inc.

Printed on recycled paper in the United States of America

1016268