A STRAWMAN REFERENCE DESIGN FOR DEMAND RESPONSE INFORMATION EXCHANGE

DRAFT

CONSULTANT REPORT

Prepared For:
California Energy Commission

Prepared By:
EnerNex Corporation

EnerNex
CORPORATION

10/31/2004
PUBLICATION # HERE

Prepared By:
EnerNex Corporation
Erich W. Gunther
Knoxville, Tennessee
Contract No. C-03-06

Prepared For:
California Energy Commission

Michael Magaletti
Contract Manager

Mark Rawson
Project Manager

Laurie ten Hope
Program Team Lead
Pier Energy Systems Integration

Name,
Terry Surles
Pier Program Director

Robert L. Therkelsen
Executive Director

DISCLAIMER

This report was prepared as the result of work sponsored by the California Energy Commission. It does not necessarily represent the views of the Energy Commission, its employees or the State of California. The Energy Commission, the State of California, its employees, contractors and subcontractors make no warrant, express or implied, and assume no legal liability for the information in this report; nor does any party represent that the uses of this information will not infringe upon privately owned rights. This report has not been approved or disapproved by the California Energy Commission nor has the California Energy Commission passed upon the accuracy or adequacy of the information in this report.

TABLE OF CONTENTS

Acknowledgements

EnerNex Corporation would like to thank our sponsors – the California Institute for Energy and the Environment (CIEE) and the California Energy Commission (CEC) – and the CIEE/CEC project manager – Ron Hofmann – for their support and guidance during this project.

We would especially like to thank our technical advisory group who provided us with valuable guidance and feedback throughout the project. The advisory group members are:

Ray Bell – Silver Springs Networks (formerly with Cisco Systems)
Dave Cohen – Infotility (formerly at Silicon Energy)
Joe Desmond – Deputy Secretary for Energy, State of California (CEO of Infotility during project)
Dale Fong – Itron (formerly Silicon Energy)
Joe Hughes – Electric Power Research Institute (EPRI)
Nicholas Kardas – Infotility (formerly with Microsoft)
James Pace – Silver Springs Networks
Dave Watson – Lawrence Berkeley National Laboratory
Gaymond Yee – CIEE

We also like to thank EPRI, the Electricity Innovation Institute (E2I), the Consortium for Electric Infrastructure to Support a Digital Society (CEIDS), and the Integrated Energy System Communications Architecture (IECSA) project team for their support and contributions to this effort.

Finally, we would like to thank all of the stakeholders we contacted during the course of the project for taking the time to answer our questions and providing valuable input and guidance.

1.0 Executive Summary

In "Dynamic Pricing, Advanced Metering, and Demand Response in Electricity Markets" [R1][1], Borenstein, Jaske, and Rosenfeld presented a vision of an infrastructure that will enable cost effective implementation of demand response programs in the 21st century and articulated the benefits it will provide to our society. The Demand Response Infrastructure (DRI) will have a profound effect on the State of California by making energy and value added services readily available to all Californians at affordable prices and balancing that with sound environmental policy and the need to effectively manage California's power delivery system.

This vision leads to the following premise:

1) ***Demand Response (DR) will become a major resource to deal with California's future electricity problems,***
2) ***an advanced metering infrastructure will be deployed on a large scale throughout the state,***
3) ***price signals will be used to induce load response when contingencies and market imbalances exist, and***
4) ***technology will act as a proxy for end users.***

If the premise is true, then information exchange will be required between several organizations and systems and numerous applications that create and consume information will exist. This leads to the need to develop a conceptual model for describing information flows necessary to support demand response applications related applications.

The entities [D5] requiring open information exchange for DR applications are well known. They include:

- CAISO
- Utility Distribution Companies (PG&E, SCE, SDG&E)
- Load Serving Entities (LSEs)
- Municipally Owned Utilities (e.g., City of Palo Alto, LADWP)
- Energy Service Providers (e.g., Green Mountain Energy, Pilot Power Group)
- Utility Power Plants (e.g., Diablo Canyon, Humbolt, Hunters Point)
- Independent Power Producers (e.g., CALPINE, Green Power Partners)
- Distributed Generation Resources (e.g., Pomerado Hospital, Qualcomm)
- Customers (HVAC, information portal, meters, distributed generation)
- Regulators (e.g., CPUC, CEC)
- Service Companies (e.g., billing, meter reading – Invensys IMServ)

These entities all interact to implement a variety of DR related applications such as grid management, market operations, advanced metering, operations management, DR and DG (distributed generation)

[1] The labels within square brackets are citations that indicate that either a definition for the word preceding the label can be found in Section 12 or the statement prior to the notation is attributed to a source that is fully referenced in Section 13.

dispatch, maintenance management, load aggregation, and billing. These applications consist of a number of discrete functions each with their own information requirements where uniformity is desired. These functions include meter data exchange, price distribution and management, load control signal exchange, customer information exchange, geographical information systems (GIS) information exchange, security management of data, customer enrollment and settlement.

An analysis of the applications and functions described above in the context of the vision for a widespread demand responsive infrastructure leads us to the following conclusion:

> ***For there to be seamless exchange of information in ways that we can't fully define today, there has to be a common reference design for California's demand response infrastructure.***

1.1 What is a reference design?

A reference design is a framework for understanding significant relationships among the entities within some environment, and for the development of consistent standards or specifications supporting that environment. In general, a reference design is based on a small number of unifying concepts that may be used as a basis for education and explaining standards to a non-specialist.

For example, a reference design that we can all relate to is that for a cellular telephone (Figure 1.1). The reference design provides for several human interface components (e.g., keyboard, display) that we can expect to find on any implementation of a cell phone. The reference design doesn't specify exactly how to implement what is behind these elements, but only how it is expected to interact with its environment. It does this by defining key points of interoperability between the device and its environment through well defined and in many cases standardized interfaces and behaviors.

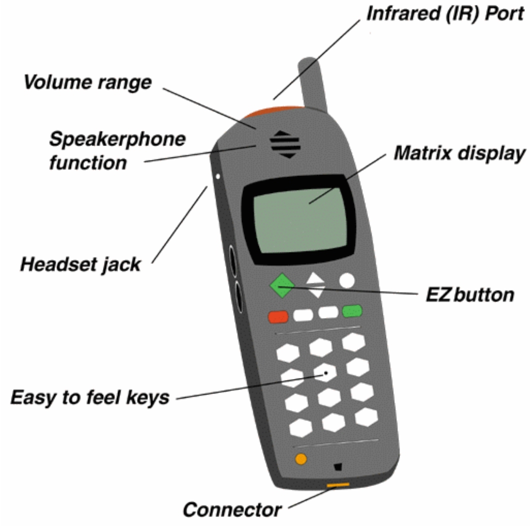


Figure 1.1 – Cellular Phone Reference Design

1.2 A Strawman Demand Response Reference Design

The impetus to start the process of developing a strawman [D2] demand response information exchange reference design is in response to concerns related to the imminent widespread deployment of demand response information exchange supportive systems. These concerns are based on observations that the various stakeholders all have their own independent views and approach on how a demand response infrastructure could be deployed. These different approaches may be incompatible with each other and fail to adequately consider scaling up demand responsive endpoints from the thousands to the millions.

There are several fundamental benefits for implementing a demand response information exchange reference design. Such a reference design establishes a common starting point for implementing open information exchange for a demand responsive infrastructure and it guarantees regulatory bodies the ability to develop tariffs, programs and other currently unknown initiatives. It also ensures that demand response can fulfill its promise of protecting the integrity of California's power delivery system by facilitating cost-effective system deployments and supporting an open market. A reference design also provides a tangible framework for rulemaking.

1.2.1 Purpose

The purpose of this reference design is initially to establish a common starting point for implementing open information exchange that leverages existing infrastructures in other industries. Once it is in place, it will give disparate standards groups a set of focused goals so that they can their harmonize their overlapping and conflicting standards initiatives; allow investment in and use of proprietary intellectual property without fears of being stranded from either perspective; and makes mandatory a minimum common information back door that guarantees regulatory bodies the ability to develop tariffs, programs and other currently unknown initiatives that may be necessary in the future to protect the integrity of California's power delivery system.

1.2.2 Assumptions

The strawman reference design is based upon the following assumptions:

1. A reference design is needed for deploying the physical (hardware and software) infrastructure to support dynamic pricing and its related (connected) energy delivery (electricity, gas, water) information systems.

2. There will always be legacy systems coexisting with new products/technology and there will always be change.

3. Innovation (cheaper, better, faster) often comes bundled in proprietary packaging that protects investments in intellectual property development.

4. Ultimately, we want interoperable information systems but not necessarily "plug and play"; secure and open data/information exchange but not fixed communications protocols [D6] (physical and procedural); and standards that respond to design but do not exist for their own sake.

5. A reference design for DR and other electricity industry applications can be developed from other existing successful interoperable data/information exchange models (e.g., credit card information gathered at point-of-sale, computers and distributed to banks for invoicing; file exchange between

PCs, Macs, Linux servers; etc.) which means an information exchange reference design can be achieved quickly and at shared cost.

6. It is extremely unlikely that the traditional standards process will provide a solution in time to facilitate the imminent rollout of widespread demand response infrastructure. Industry groups such as the UCA International Users Group and consortia such as E2I's Consortium for Electric Infrastructure to Support a Digital Society (CEIDS) can be much more effective in gathering the human and financial resources necessary to address the technical details of implementing solutions quickly before handing the work off to standards organizations.

In addition to these specific assumptions, there is an implied assumption that there is a business case to be made for demand response and a reference design. This report does not address this issue directly, but a presentation made by Joe Desmond to the technical advisory group and an update of it can be found in Appendix D.

1.2.3 High Level View

Figure 1.2 illustrates the high-level view of the strawman [D2] demand response reference design. The reference design defines two zones of **Systems Interoperability**. The first zone is an **Open Systems Domain**. This means that within this logical zone, a well defined set of technologies based on open standards are deployed that allow a free flow of information to occur between applications without the complexity and expense of extensive protocol conversion and translation. Interoperability within this zone is an inherent property of the open systems implementation.

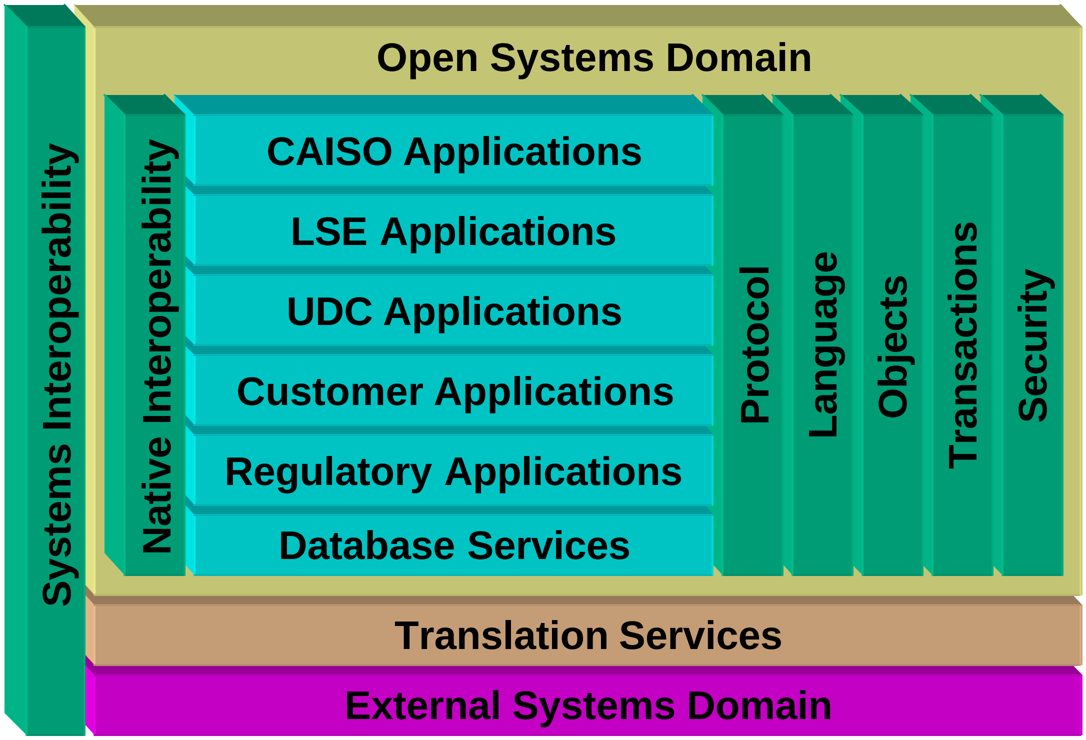


Figure 1.2 – Strawman Demand Response Reference Design – High-Level View

The second zone is the domain of **External Systems** that implement proprietary protocols, languages, and unstructured information. These systems may represent pre-existing installations or new installations that are not able to directly participate in the open systems domain. Bridging the boundary between the two domains is a **Translation Services** layer that facilitates interoperability between these external systems and the open systems domain. This design approach facilitates an inclusive versus an exclusive policy necessary to prevent stranding assets and allows for innovation and rapid technological change.

The heart of the reference design is the choice of technologies used to implement the five elements of **Native Interoperability** shown in Figure 1.2 – protocol, language, objects, transactions, and security. Suitable technologies already exist in the form of national and international standards as well as various industry group recommended practices. The main body of this report describes an initial list of candidate technologies for consideration in the reference design.

1.3 Recommendations

This reference design will begin at a very high-level so that it will not be a problem for any vendor, utility, user, etc., to adopt. It is expected to evolve over time as other industry reference designs have done.

There are three specific recommendations for moving forward:

1. **Form / utilize an industry-driven working group to work out the details of the reference design and set up the mechanisms for already existing standards bodies to contribute**
2. **Devise method of measuring compliance and benefits of implementation**
3. **Consider implementing DR systems according to a reference design through rulemaking (for example CEC load management authority)**

The process of implementing these recommendations involves these steps:

- Identify precedents (a template)
- Form an advisory group
- Hold workshops
- Involve stakeholders
- Determine if new working group(s) required
- Establish relationship with other working groups
- Leverage other funded research (e.g., CEC, CEIDS, LBNL, DOE, etc.)
- Implement demonstration projects

Of the elements above, the core of the technical work would likely take place within the context of workshops and eventually the industry working group recommended above. The technical work would require the integration of two fundamentally different disciplines – domain experts who understand the fundamental requirements for implementing demand response programs, and information technology experts who understand how to architect, design, and implement large information system infrastructures. A third discipline could arguable be included to cover the physical networking infrastructure and its management but for the purposes of these comments we include those domain experts in the information technology domain.

The latter group would be responsible for working out the details of the specific implementation technologies. That work would be based on the requirements agreed upon by the domain expert group. Note that there are already suitable industry groups in existence that could be used to facilitate these new work items without creating a new organization.

2.0 Introduction

The following discussion describes the elements of a demand response infrastructure and information exchange architecture in some detail. This discussion sets the foundation and core principles used to develop a preliminary (strawman) reference design to support demand response applications. The architecture discussion draws heavily (in most cases directly) from the work of the Cross-Industry Working Team (XIWT) and the Consortium for Electric Infrastructure to Support a Digital Society (CEIDS). The XIWT was a multi-industry coalition committed to defining the architecture and key technical requirements for a powerful and sustainable National Information Infrastructure (NII) – an initiative of the Clinton/Gore administration. CEIDS is an organization whose mission is to transform the current infrastructure into a new electric delivery system that integrates advances in communications, computing and electronics to meet the energy needs of the digital society.

A core work product of CEIDS is the Integrated Energy Communications System Architecture (IECSA) which was released just as the final draft of this report was being prepared. Since the CEC is a member of CEIDS and has contributed to the development of the IECSA, it is anticipated that the principles put forth in this report will evolve to more closely line up with the IECSA architecture terminology in any follow on work based on this report. Where there is a conflict or potential for confusion between the XIWT and IECSA terminology, it is noted in the report and then the IECSA terminology is used.

2.1 The Demand Response Infrastructure

In " Dynamic Pricing, Advanced Metering, and Demand Response in Electricity Markets" [R1], Borenstein, Jaske, and Rosenfeld presented a vision of an infrastructure that will enable cost effective implementation of demand response programs in the 21st century and articulated the benefits it will provide to our society. The Demand Response Infrastructure (DRI) will have a profound effect on the State of California by making energy and value added services readily available to all Californians at affordable prices and balancing that with sound environmental policy and the need to effectively manage California's power delivery system.

The DRI will evolve as user demands for capability and services are determined in a free competitive environment. The evolution of computing and information technology suggests that the DRI will support a great diversity of uses and users. It will be extraordinarily flexible, with many levels of functionality and capability and a huge variety of applications and services from which providers and users may select according to their needs, capabilities, and resources.

Achieving this vision will require the collaborative efforts of government, academia, and industry, including information technology manufacturers, communications network service providers, and information service providers. For these efforts to be effective, they must refer to a common framework. This document represents a first step to lay a conceptual foundation for the DRI and to posit a working reference design for information exchange.

2.2 Architectural Vision

Information technology planners refer to abstract technical descriptions of systems as "architecture." A system's architecture, unlike a building's architecture, is conceptually based and does not include the level of detail needed for construction. Such an architecture would be more like a conceptual map of a transportation system on which freeways and toll roads, highways and byways, airports and seaports, rivers, multiple points of access, and provider jurisdictions would be plotted. To create such a map, planners need not know all routes, specific construction technologies, forms of vehicles, and usage patterns. They can assume that these components will exist within broad, reasonably well-defined, parameters of physical dimensions and performance.

Similarly, planners of the DRI do not need to know every possible use for its routes and information-carrying vehicles; they do not need a precise definition for "demand response infrastructure" in order to think about the foundations and support systems it will require. System architecture provides the basic framework for the creation, movement, distribution, use, and management of information.

This document provides a vocabulary and context for discussing an architecture for the DRI as well as describing a basic reference design that may be used to help express that architecture. It identifies some necessary fundamental DRI components and services and examines ways to expand and evolve the infrastructure. It identifies key interfaces and protocols where standards are required. It is not, and indeed cannot be, a blueprint for implementing the DRI. Instead, this architectural framework allows utilities; LSE’s; ESP’s; IOU’s; communications, computer, and information providers; application developers; meter manufacturers; regulators; and other stakeholders to work separately while implementing elements of a common vision.

2.3 Structure of This Document

The next section of this report describes the requisite characteristics of a demand response infrastructure. Next, we present a set of guiding principles and specific goals for DRI development. An architectural framework satisfying these goals is outlined in sections 5.0, 6.0, 7.0 and 8.0; this framework consists of a Functional Services Framework model, a Reference Architecture model, and a Reference Design.

The Functional Services model describes the DRI's building blocks, or components; particularly an "enabling services layer" that must exist to facilitate the rapid development and deployment of applications and the integration of all components. These enabling services include common capabilities needed by most applications; specialized services for specific application domains (such as billing, bidding, settlement, etc.); and inter-application communications that allow developers to build continuously upon existing applications.

The DRI must provide openness and interoperability among its components to enable users to interact effectively and let providers create services efficiently. The Reference Architecture model addresses these needs by identifying key DRI interfaces, protocols, and components. The Demand Response Information Exchange Reference Design builds on this model by identifying key points of interoperability needed to support demand response applications.

Much of the envisioned DRI will be achieved through the evolution of today's information infrastructure and information services. Two scenarios in section 9.0 describe hypothetical future applications. They point out underlying capabilities that will be desirable in the DRI, and are used to illustrate how the framework can aid in thinking about the DRI.

The DRI will not be static, but instead will evolve to meet the changing needs of its users and to accommodate new technologies and applications. This report concludes by suggesting steps for managing this evolution.

3.0 Characteristics of Infrastructure

According to Webster's *Ninth New Collegiate Dictionary*, infrastructure is "the underlying foundation or basic framework of a system or organization." Transportation, energy, water and sewer systems, and telephone systems are examples of societal infrastructures, used in varying forms and degrees by everyone. Useful, well-planned infrastructure generally has in varying degrees the following characteristics:

Shareability - Common resources offer economies of scale, minimize duplicative efforts, and if appropriately organized encourage the introduction of competing innovative solutions.

Ubiquity - All potential users can readily take advantage of the infrastructure and what it provides.

Integrity - The infrastructure operates at such a high-level of manageability and reliability that it is often noticeable only when it ceases to function effectively.

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

Cost effectiveness - The value provided must be consistent with cost or the infrastructure simply will not be built or sustained.

Standards - The basic elements of the infrastructure and the ways in which they interrelate are clearly defined and stable over time.

Openness - The public infrastructure is available to all people on a nondiscriminatory basis.

Security – An infrastructure must be trustworthy and enable those who use it to do so without fear of interference from others.

3.1 Today's Information Infrastructure

The computing resources and communications networks in the United States today make up a rich information infrastructure. Some parts of this infrastructure, such as the voice telephone network, are well-integrated. Other parts of the communications network, such as electronic mail systems, are less well-integrated. Similarly, document processing, accounting, and database software have limited capabilities for faithfully exchanging data. Thus, it is often difficult to combine capabilities found within the present information infrastructure so they interact efficiently and spontaneously within application areas or create new applications.

The developmental state of a technology affects our understanding of its importance. When a technology is in an early development stage, its potential use as the basis for a new infrastructure may not be appreciated. Information processing technologies have reached a stage of maturity and deployment that makes thinking about their application in a DRI important. In evolving to the DRI, today's information infrastructure must not only become more powerful through the introduction of new technologies, but it must also become more integrated. It must be made easier to use and more tolerant of faults throughout its vast system of interacting devices and pathways. Fortunately, the trajectory of technical improvement in information technology promises the capability to achieve these ends.

3.2 The Internet

Today's Internet is often cited as the model or solution for any new network infrastructure. It is a shared resource providing an estimated 730 million users worldwide with access to hundreds of thousands of information and computing resources such as libraries, data archives, bulletin boards, supercomputers, information directories, and databases. It enables general-purpose computers and information appliances (such as workstations, PCs, routers, and network switching systems) to connect to one another. It presently has more than 250 million host computers interconnected through standard protocols throughout the nation and around the world. The Internet architecture provides a framework into which new networks, different kinds of computer systems, and innovative applications may readily be added.

The Internet offers many of the characteristics desired in an DRI, such as shareability and broad availability. It does not, however, yet provide other desired DRI capabilities such as ease of use; high integrity; guaranteed grades of service; privacy safeguards; mechanisms for detecting and preventing fraud and abuse; usage and measures suitable for billing; application addressability; or the linkages into transaction based services required for many commercial applications. The DRI will build upon the Internet's best aspects as well as upon public and private sector computer, communications and information product and service alternatives.

It is important to note the fundamental difference between Internet technologies and the public Internet infrastructure itself. Huge investment has been made to develop the technologies used to implement the Internet and these technologies have been successfully deployed in private networks with reliability statistics of 5 nines (99.999%) or better. These technologies are low in cost, ubiquitous, and reliable.

4.0 DRI Principles and Goals

The DRI we envision must satisfy demands for new end-user services that greatly exceed the capabilities of today's demand response systems. This increased demand will be stimulated by the product innovations made possible by the new, cheaper, and much more capable information processing technology of the near future; it will result in as yet unknown requirements for increased network bandwidth and addressability to accommodate the two way command, control, and information access required to support the desired demand response feature set.

Despite these many unknowns, we have identified six guiding principles to determine the overall shape and form of the DRI:

- The DRI must serve all consumers.
- The DRI must promote the principles of free enterprise.
- The DRI must protect the rights of users and stakeholders.
- The DRI must promote interoperability and open standards.
- The DRI must provide high-quality, high-capability services.
- The DRI must provide an information marketplace.

For each guiding principle, we have identified specific goals for the DRI; these are listed below. The degree to which individual DRI applications, enabling services, or products will achieve these goals will depend on many factors, including application requirements, user needs and economics, technological progress, and social conditions.

4.1 Serve All Consumers

Every consumer must have access to an essential subset of DRI capabilities. The DRI will enable a new plateau of service capabilities. While not all users will want or need all these capabilities (a fixed rate is just fine thank you), the DRI should support the expansion of these capabilities over time.

The DRI must be easy to use, with intuitive and consistent interfaces. The DRI will provide a variety of capabilities supporting diverse user communities. Its internal complexities should be hidden from most users.

4.2 Promote the Principles of Free Enterprise

The DRI must be structured to promote open and fair competition among information, technology, and service providers. Companies and ideas should compete in an open marketplace where users are afforded maximum choice based on value and price. This arrangement will ensure innovation and affordable prices.

The DRI must be designed to encourage entrepreneurship and private ownership. Entrepreneurial individuals and enterprises will provide the innovation needed to evolve the DRI. This innovation will in turn provide a stimulus to the California economy, meet societal needs, and fuel competitiveness as DRI capabilities are used by all.

4.3 Protect the Rights of Users and Stakeholders

The privacy of end users and intellectual property rights of the owners of DRI data (information) must be protected. The value of the DRI will derive from the rich set of rate options and energy services available to users, and their ability to access and manage this information to meet their individual needs.

The DRI must provide a means for verifying the authentic identity of users, service providers, and information. Without such a mechanism, the DRI cannot be sufficiently trusted to fulfill its potentially significant role in managing California's energy demand. Users should be protected from intrusions such as unwanted solicitations and information distribution. For certain types of services, anonymous access should be supported. Users must be assured that transactions on the DRI will be free from unauthorized interception, alterations, or use.

The DRI must minimize opportunities for and permit redress of fraudulent use or abuse of facilities and services. In particular, rules and regulations such as those that apply to truth in advertising, unsolicited inquiries, or accuracy of general representations of capability should be adopted. Both DRI users and service providers will have control of and be accountable for their interactions in the DRI.

4.4 Promote Interoperability and Open Standards

The DRI must support a wide variety of user equipment through a limited number of standard or widely accepted interfaces, protocols, and objects. To the extent possible, these will be general purpose, so that the same interface, protocol, or object can be used to access many different types of services.

National and international standards must be used, where appropriate, to promote interoperability, wide equipment availability, and low costs. Where standards do not exist, they will be developed by relevant standards-setting bodies. Where existing standards are not appropriate, but widely accepted methods are, the latter will be used.

The DRI must seamlessly link multiple public and private networks. Like the Internet, the DRI will be based upon a "network of networks" interconnecting numerous public and private networks. DRI users will be best served if these networks are linked, thereby providing them with seamless access to all other services available.

4.5 Provide High-Quality, High-Capability Services

The DRI must provide the availability and performance needed to support a wide range of present and future applications and services. System designers should be able to select appropriate performance qualities (e.g., speed, reliability, security) relevant to the specific services offered.

The DRI must provide high-dependability, high-integrity performance. It will include sufficient integrity, resiliency, redundancy, and fault detection and isolation capabilities to provide highly dependable operations despite equipment failures, natural disasters, acts of sabotage, periods of unusual emergency conditions, and very high-volume demand – all situations where demand response actions are more likely to be needed. Individual systems may require, and will have available to them, different levels of reliability in using the DRI depending on the services implemented (e.g. emergency load shed).

The DRI must be scalable. It will be able to grow flexibly in capacity and performance as needs increase and be extensible to millions of simultaneous users and devices. Further, the DRI will not be constrained by specific assumptions of applications or traffic but will instead provide a flexible structure that can meet, or can evolve to meet, all needed applications.

The DRI must support a wide variety of billing and payment options. Providers will be able to collect data in order to prepare, among other types, usage and time-of-day-sensitive bills. Users will be able to accurately estimate in advance the charges they incur for using various services, control their usage, pay in real time, use multiple billers and billing services, and choose from a variety of payment options ranging from cash to credit and debit arrangements.

The DRI must evolve from current information infrastructure resources. The envisioned DRI can be brought about quickly and cost effectively by building upon today's computing and communications infrastructure and evolving this infrastructure as appropriate while adding new capabilities.

4.6 Provide an Information Marketplace

The DRI must let users know what services, information, and capabilities are available at any time. It will provide this information through a variety of mechanisms; these will allow for automated reporting and updating.

The DRI must provide easy entry for new providers and users. To foster a rich array of services and tools that meet user needs, the DRI will provide an inviting environment that facilitates applications and service creation and enables easy entry by new network and information providers and users.

The DRI must promote the integration of existing applications to create new products and services. The DRI will support mechanisms that allow providers and users to combine current DRI applications and services to create new applications.

The DRI must include mechanisms to ensure orderly and effective reprovisioning of services during transition periods. These mechanisms will help protect users who rely on particular DRI capabilities; it will also allow transition to new versions of widely deployed services, application interfaces, and associated technologies.

5.0 DRI Architectural Framework: Overview

As used here, "architecture" is an abstract description of a system; numerous actual system implementations could be built that meet that architecture's specified principles and goals. For example, an architectural goal for a musical instrument might be that anyone trained on it be able to play any new variant. Thus, specifications for a keyboard instrument would include the number of keys, their physical relationship, and the mapping of notes on the scale to the keys. Characteristics not relevant to the architectural goals (color, size of the enclosure, etc.) do not need to be specified.

The DRI combines today's computing and communications network architectural concepts. For example, its architectural goals include *software portability and interoperability*. Software portability means that a program will yield the same result when executed on different implementations of a computing system. Interoperability means that the interconnection of different implementations of a system will yield the same result as the interconnection of identical implementations. The DRI will be a highly distributed network of networks that links diverse devices.

Network architectures are typically specified in terms of *interfaces* and *protocols*. Interfaces constitute points of connection or interaction among system components. They often refer to places where entities may offer services or link systems; they also may refer to the links at boundaries of layers of various functions. Protocols specify sets of rules and formats that determine the communication behavior between entities. Any new system capability will have to connect via an existing or standard interface, even if some of the properties are tailored to the specific nature of the service. It is thus essential that the system's key interfaces and protocols be open to future evolution and development. It is also important to specify both the underlying services and the information objects exchanged across the infrastructure.

5.1 DRI Service Users and Providers

The DRI architecture must support the various and simultaneous roles of its users. People and organizations interact with a system in different ways depending on the role they play with respect to the system. In fact, people and organizations may play multiple roles as consumers and producers of information and information services; these roles can be combined in different ways. The requirements of these various roles may be very different; the principal roles include the following.

- **Energy consumers and providers, who use information services -** These are the primary consumers of the system information services.
- **Information service providers , who provide information services -** Commercial, governmental, or private providers of information services.
- **Network and information system service providers, who provide connectivity -** These are the owners of the wire, cable, fiber, and switching systems; satellites; value-added networks; and of the facilities and services that are employed to manage and provide these. These providers include brokers and other intermediaries, as well as originators of services who add value by packaging, building on, or otherwise enhancing services provided by others.
- **Hardware and software vendors, who provide physical devices, appliances, and software platforms -** These vendors provide the physical devices, appliances, and platforms employed by service providers and users. These include service creation and application tools.

These roles may be combined for a given individual or enterprise. Thus, an LSE may, for example, concurrently be information service providers to energy consumers as well as a consumer of a load profile database.

5.2 Architecture Models

There are many ways in which a DRI architecture can be presented. Two models are particularly useful for identifying fundamental technology issues. The DRI Functional Services model provides a logical model of the relationships between applications and the underlying services that support their development and use. The DRI Reference Architecture for Information Exchange identifies the major functional elements of the infrastructure and their interfaces and protocols.

6.0 DRI Architecture: Functional Services Model

The DRI ultimately will be driven by the demands of its users and the value it provides them. Users are primarily interested in information processing applications, which they may own or gain access to as end-user services via communications networks. These services will be "enabled" by other underlying, transparent services provided by information and network service providers. Applications and enabling services will employ various information processing machinery, ranging from common appliance-grade devices to specialized computers and data transport technology systems distributed throughout the DRI. Thus, the DRI's structure consists of three basic components: applications, enabling services, and physical infrastructure.

These components can be understood within the Functional Services Framework model. This framework is not specific to any particular type of organization, technology, or use. It is portrayed here in layers (see figure 6.0.1), similar to models of network protocols, but is more generally intended as a way to think about the components of a feature-rich, flexible, open, and distributed infrastructure.

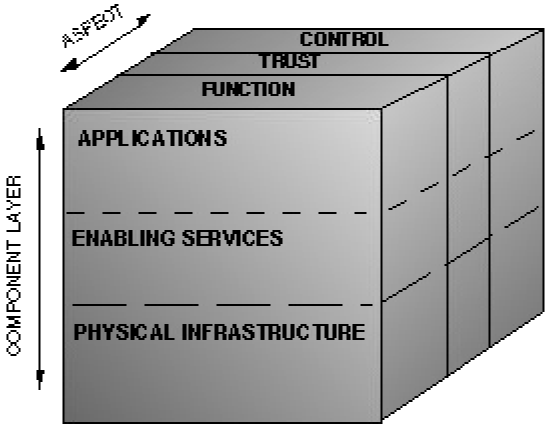


Figure 6.0.1 – DRI Function Services Framework

The Functional Services Framework model is used to characterize the DRI by function and by certain key characteristics (described below); it does not provide any details about these functions. For example, while the general framework might be used to locate supporting software for handling accounting information in an information access service, it would not give any details of expected performance or of a particular implementation, which would be dependent on its capability and design. The detail required for such a particular instance would be described in a domain-specific architecture for a service or application.

6.1 Layers

As noted earlier and in Figure 6.0.1, the DRI's overall structure can be viewed in three component layers: physical infrastructure, enabling services, and applications. Each of these layers has several characteristics or aspects consisting of function, trust, and control.

6.1.1 *Physical Infrastructure*

Physical infrastructure contains the basic processing and communications components of an information system. These components comprise the computing and communications platforms or hardware (and associated low-level systems software) of computers, peripherals, switching systems, meters, sensors, controls, telephones, and information processing devices, together with the communications media, such as fiber, cable, and electromagnetic spectrum. The physical connectivity and layout of the network and component systems are described in the physical infrastructure layer. These would include specialized devices as well as standard, general-purpose, widely available information appliances.

6.1.2 *Enabling Services*

Enabling services provide general system-related functionality for applications performed using the physical infrastructure. These services are those essential for the DRI to meet its goals and requirements (these are specified in section 3.0). Enabling services must create an environment in which new services and applications can be easily introduced and integrated with existing services and applications. This layer is thus expected to be an especially dynamic one, with technical innovations and new services continually emerging and competing. Enabling services are classified as generic and domain-specific.

There will be common requirements for components at all levels of the framework. In addition, communities of like-interest users or organizations conducting similar activities or using similar services will require domain-specific application and service features to incorporate specialized terminology or handle particular legal or financial instruments. Such domain-specific features would enable associated components to handle domain attributes such as terms and conditions, reference and accounting rules, etc. For example, fee-for-service and financial applications may have similar special transaction and security requirements, while sensitive personal services, such as medical care, might place stringent demands on privacy to transport diagnostic data and patient records. The nature of specialized enabling service offerings would reflect value to their users.

Figure 6.1.2.1 shows several examples of classes of enabling services. They are described as follows.

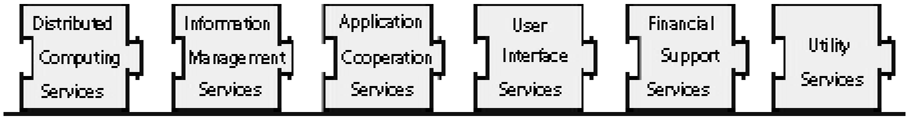

Distributed Computing Services
Information Management Services
Application Cooperation Services
User Interface Services
Financial Support Services
Utility Services

Figure 6.1.2.1 – Example Enabling Services

Distributed computing services provide the functionality that links multiple separate nodes into one distributed system. They include network services, invocation services, location services, security services, and system coordination services.

Information management services organize, store, and retrieve information. These services employ file systems, access methods, database systems, document stores, and information semantics.

Application cooperation services enable applications to "cooperate" to create common multiple end-user activities. Typical services include transaction processing managers; enhanced messaging services (e.g., event management, reliable message queues);object request brokers; and workflow managers, agents, and encapsulation facilities.

User interface services will provide the link between the DRI and its users. These services will present information to, and acquire information from, the user. Present-day examples include Windows, Linux, and other workstation based applications, and web based applications. In the DRI's distributed processing environment, a given user interface may employ components in various layers and at various points in the DRI, e.g., partially in the information service provider's equipment and partially in the user's information appliance (e.g. consumer portal, end user PC, intelligent devices, etc.)

Financial support services support all manner of commercial and personal financial transactions.

Utility services facilitate system use or help it function. They may incorporate spooling systems, resource accounting services, language run-time systems, and common libraries. Specialized utility services might support specific domains such as business and finance, education, or medicine.

6.1.3 Applications

Applications are information processing tools that "do something" for a user. The underlying enabling services and physical infrastructure supply the means by which applications deliver their functionality. Examples of applications include direct load control; rule based load control; bill estimation and review; market interaction; invoicing; and interacting with other persons or computer systems.

DRI applications will be built in part from a combination of service capabilities. To facilitate the development of applications, the DRI's enabling services layer should present well-defined application programming interfaces (APIs). Like the user interfaces described above, a given application may, in the distributed processing environment provided by the DRI, exist in part at various points in the DRI. For example, some parts might reside in information service provider's equipment, and some parts in user's information appliances. APIs must be defined at all points in the DRI where portions of applications can exist.

6.2 Aspects

Each of the component layers should be considered from the three related aspects of functionality, trust, and control. For example, one component of trust is to protect a system from unauthorized access; every system should have the degree of such protection that is appropriate for its purposes. Thus, the DRI should be examined to ensure that adequate protection is achieved within each of its component layers.

Functionality describes each component's responsibility to the system as a whole. Directly or indirectly, each component must help users accomplish a task. Functionality suggests the interfaces, usability, and localization required for each functional component.

Trust has three major sub-elements: security, integrity, and assurance of performance. Security describes a system's ability to ensure adequate protection, accessibility, and integrity of information. Integrity includes such concepts as graceful degradation of performance in the event of failure, recovery after failure, and fault tolerance. In some environments, not meeting required performance levels is equivalent to failure. Requirements for performance must also consider issues such as acceptable performance and cost.

Control includes four major sub-elements: manageability, serviceability, measurement, and adaptability. Manageability involves controlling the component or system under normal situations. Serviceability deals with being able to recover and fix things when they break or to protect them from breaking. Measurement includes performance statistics and descriptions of component states, as well as accounting functions. Adaptability covers a component's ability to evolve with a new technology in a predictable way to meet changing demands.

7.0 DRI Reference Design for Information Exchange: Reference Architecture

7.1 Reference Architecture Framework

A critical element in developing any large and complex entity is to develop an organizing structure or framework to define and categorize the elements. Such a framework was developed for the IECSA Reference Architecture to capture the requirements of the power system functions, and to organize these requirements in a manner that the results are useful to diverse types of users. The IECSA architecture and framework is completely reusable for the DRI Architecture since it is a superset of the basic architectural requirement of the DRI.

This framework was structured to integrate the Business Needs for power system operations, a Strategic Vision based on High-Level Concepts, a Tactical Approach, using technology independent techniques to accommodate legacy systems, the multiplicity of vendors, and rapidly changing technologies, and recommends specific standards, technologies, and best practices.

Before discussing this framework further, some definitions of the terms used must be clarified.

7.1.1 What Is A Reference Architecture?

Reference: Reference *books*, like dictionaries, encyclopedias, and compendia of famous quotations, provide users with a means to search a well-organized structure to find the answers to their questions. These reference books are structured so that words and articles are easy to find (generally alphabetically) and include many cross-references so that a user can navigate among many different entries. Not only are these reference books well organized; they also represent the combined wisdom of experts.

Architecture: An architecture is the fundamental organization of a system embodied in its components their relationships to each other and to the environment, and the principles guiding its design and evolution.[2]

Reference Architecture: A *reference architecture* for an enterprise-level infrastructure is organized by the common types of requirements found across the many different functions and systems (such as response timing or security needs), and by high-level concepts of system engineering. Experts assess each commonality to determine the best solutions to meet its requirements in accordance with the high-level concepts, and these solutions are then described. A project engineer can then navigate this reference architecture by selecting what common abstractions are required, and then for every common abstraction focus in to the appropriate solutions.

7.1.2 What is a Framework of an Architecture?

Framework: A framework outlines the structure of the final entity, like the steel girders that outline the final structure of a building. For an enterprise-level infrastructure, the framework provides the organizing

[2] IEEE STD 1471, 2001

structure that starts with the business needs and identifies the information necessary to operate the business. From those business needs, the framework should develop a strategic vision and possible tactical approaches to implementing the vision, along with the standards, technologies, and best practices that are necessary to support the business operations.

Architecture Framework: Such an Architecture Framework provides a sustainable mechanism for identifying, developing, and documenting architecture descriptions of high priority areas built on common business areas and designs that cross-organizational boundaries within an industry

7.1.3 What is the IECSA Reference Architecture Framework?

Framework of the IECSA Reference Architecture : The Framework of the IECSA Reference Architecture was constructed from the above-mentioned concepts. The IECSA Reference Architecture is based on an Architecture Framework bounded by the information infrastructure requirements of the power system industry. The framework includes the business needs of the power system industry, the strategic vision based on high-level concepts of distributed information, the tactical approaches based on technology independent techniques, the standards, technologies, and best practices that could be used in the power industry, and a methodology for project engineers to use to create a coherent syste m out of the individual pieces.

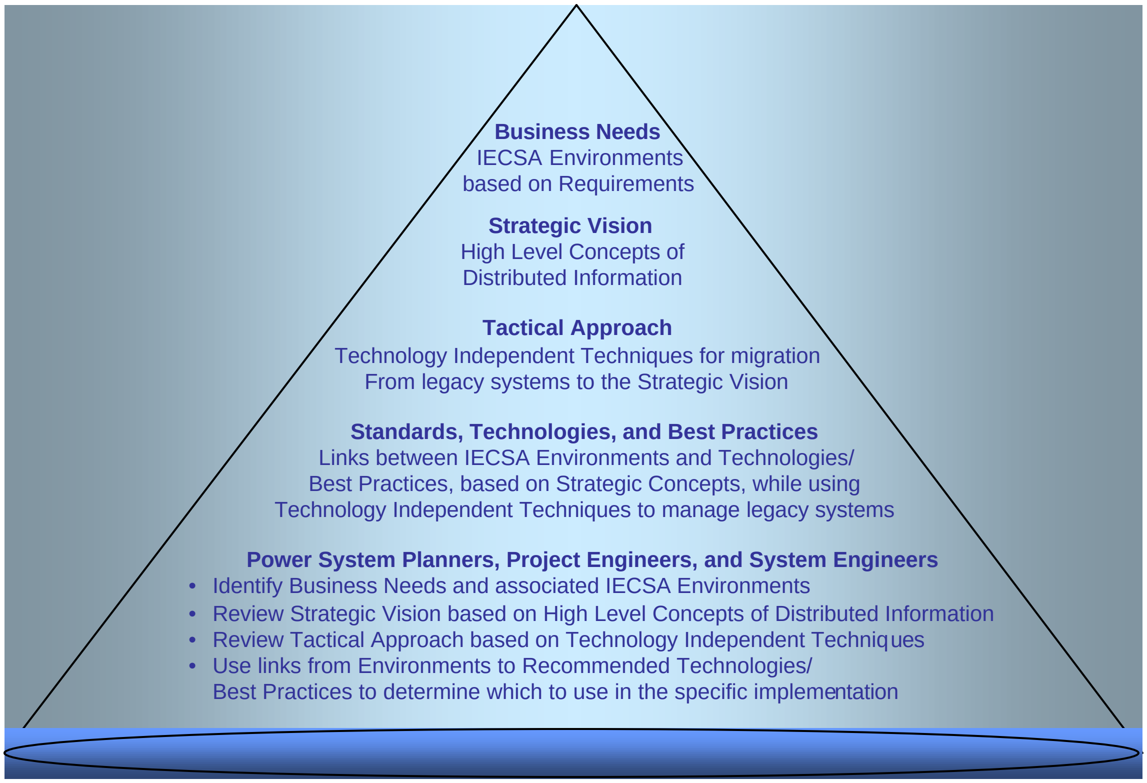
7.1.4 IECSA Reference Architecture Framework Contents

The IECSA Reference Architecture Framework was constructed from the above-mentioned concepts. The reference architecture is based on an Architecture Framework bounded by the information infrastructure requirements of the power system industry. The framework includes:

- **Business Needs** of the power system industry, as captured in the power system operations functions, and categorized into the **IECSA Environments** (Annex B)
- **Strategic Vision** based on **High-Level Concepts** of distributed information
- **Tactical Approach** based on **Technology Independent Techniques** of common services, information models, and interfaces.
- **Standard Technologies** and **Best Practices** that could be used in the power industry
- **Methodology** for automation architects, power system planners, project engineers, information specialists, and other IECSA users to zone in on the exact parts of the IECSA Architecture that is directly relevant to them, and to quickly access the IECSA recommendations.

The IECSA Reference Architecture framework generalizes and extracts the architecturally significant requirements by cross-cutting energy industry requirements involving distributed information, and provides a technology-independent architecture for project engineers to use as they determine solutions for specific implementations.

FigureFigure 7.1.1 depicts the IECSA Reference Architecture Framework and clearly identifies how these concepts fit together. The individual concepts shown in the figure are discussed below.



Business Needs
IECSA Environments
based on Requirements

Strategic Vision
High Level Concepts of
Distributed Information

Tactical Approach
Technology Independent Techniques for migration
From legacy systems to the Strategic Vision

Standards, Technologies, and Best Practices
Links between IECSA Environments and Technologies/
Best Practices, based on Strategic Concepts, while using
Technology Independent Techniques to manage legacy systems

Power System Planners, Project Engineers, and System Engineers

- Identify Business Needs and associated IECSA Environments
- Review Strategic Vision based on High Level Concepts of Distributed Information
- Review Tactical Approach based on Technology Independent Techniques
- Use links from Environments to Recommended Technologies/
  Best Practices to determine which to use in the specific implementation

Figure 7.1.1: IECSA Reference Architecture Framework – Top Down View

7.2 Platform Independent Information Model

The DRI architecture must use Information Object Models, Common Services and Generic Interfaces to provide technology independent solutions for implementing interoperable systems and for managing the migration from legacy systems toward fully integrated systems.

This approach allows systems to operate in concert while avoiding excessive interdependence, and provide mechanisms for handling legacy systems more easily. The term ‘Platform Independent Model’ identifies the separation between semantics (the meaning and purpose of message exchange) and implementation (those specific technologies that can carry out the message exchange). The Platform Independent Model (PIM – Figure 7.2.1) is that former specification that is independent of any specific technology.

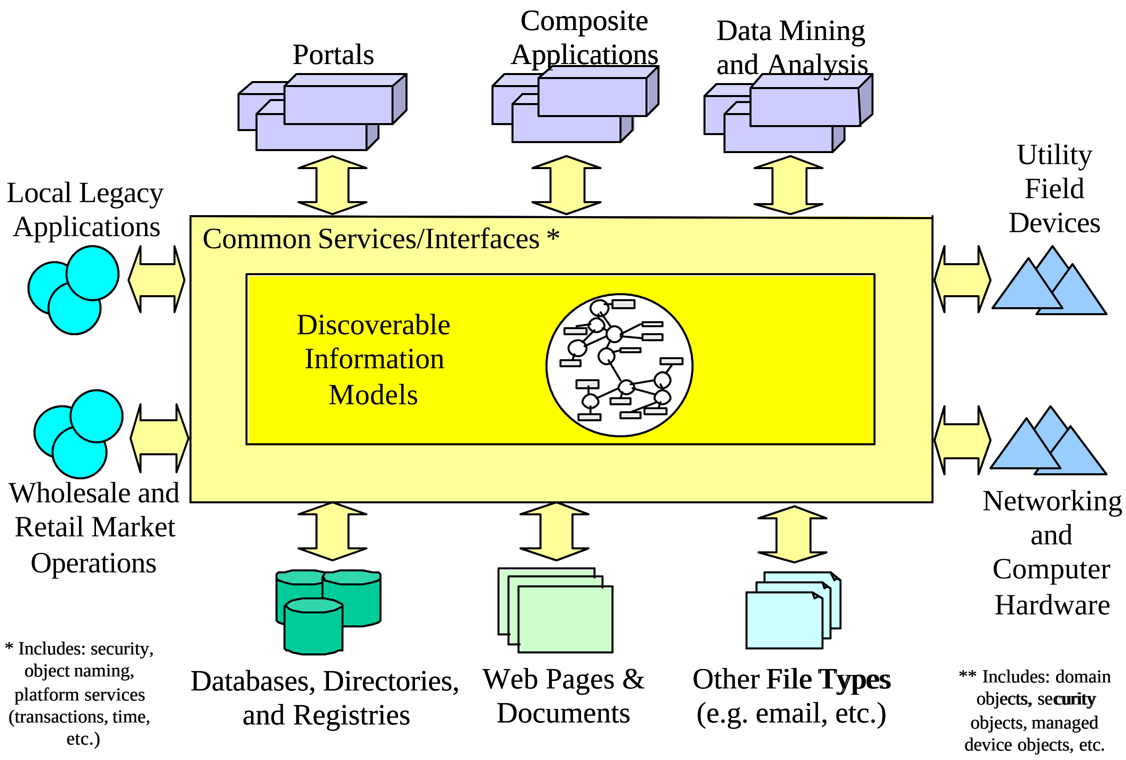

Portals
Composite Applications
Data Mining and Analysis
Local Legacy Applications
Utility Field Devices
Common Services/Interfaces *
Discoverable Information Models
Wholesale and Retail Market Operations
Networking and Computer Hardware
* Includes: security, object naming, platform services (transactions, time, etc.)
Databases, Directories, and Registries
Web Pages & Documents
Other File Types (e.g. email, etc.)
** Includes: domain objects, security objects, managed device objects, etc.

Figure 7.2.1: Platform Independent Model
Common Information Models, Common Services and Interfaces. This model manifests the desired technology independent features described in this section.

The use of a technology independent design for communications and integration of intelligent equipment is one of the more important concepts in the development of interoperable systems and equipment today. This design is independent of the physical media and networking protocols so the same language can be used in a variety of different distributed computing environments.

The concept of technology 'layering' is a powerful concept that enables flexibility in the integration of complex distributed computing systems. In simple terms, layering enables the messages in communications to be independent of the technologies that deliver the messages to the devices and equipment that will comprise the future energy system. It is possible, for instance, to have the same message carried over different communications media and different types of networks. The ability to separate the transport of messages from the content and meaning of the messages enables the powerful concept of a 'common language' described below. Layering also can enable the industry to make use of new physical communications media that has not yet been developed. This can provide a level of 'extensibility' for future systems.

Figure 7.2.2 illustrates the consequences of not using a platform independent approach. Without a PIM, every device, applications, information source, and information sink must know something about each like entity that it wishes to communicate with. This generally results in costly and difficult to maintain systems that are generally quite fragile in that the overall system is sensitive to a change in any one component.

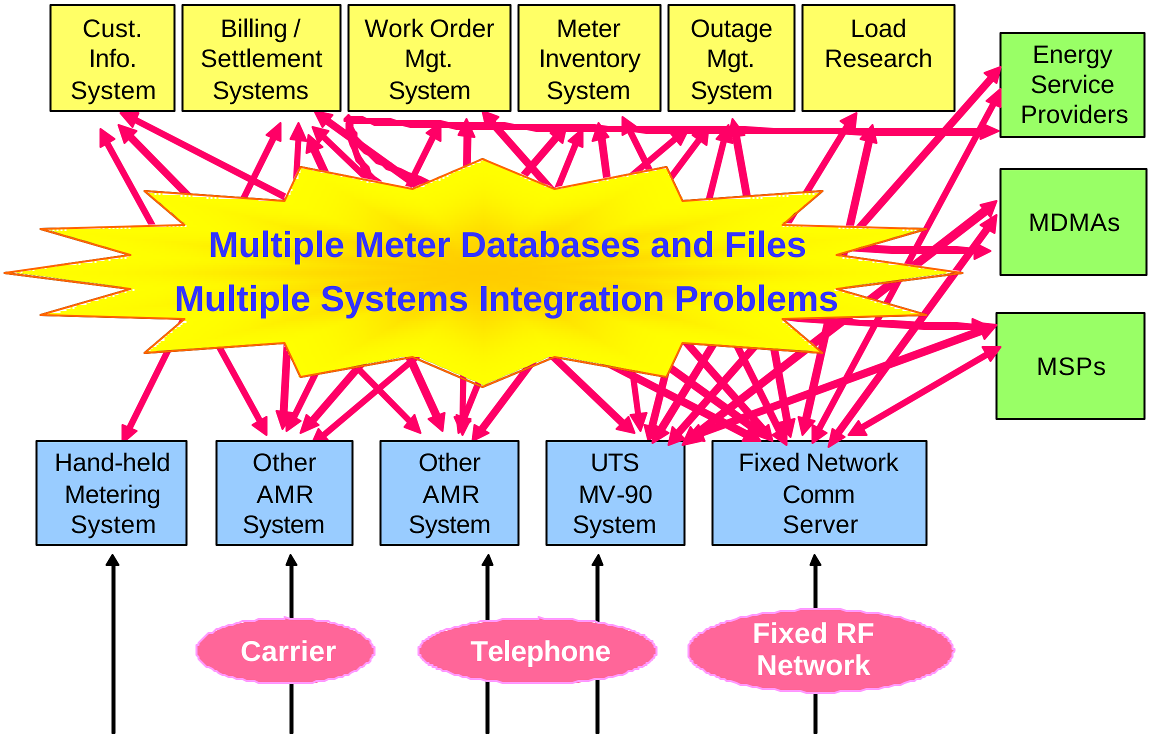


Figure 7.2.2 – Consequence of not using a Platform Independent Model

A more structured approach as illustrated in Figure 7.2.3 shows how information flows can be streamlined by identifying clearly the entities that must exchange information, a set of interfaces to access that information, and a standardized set of services to implement against those interfaces.

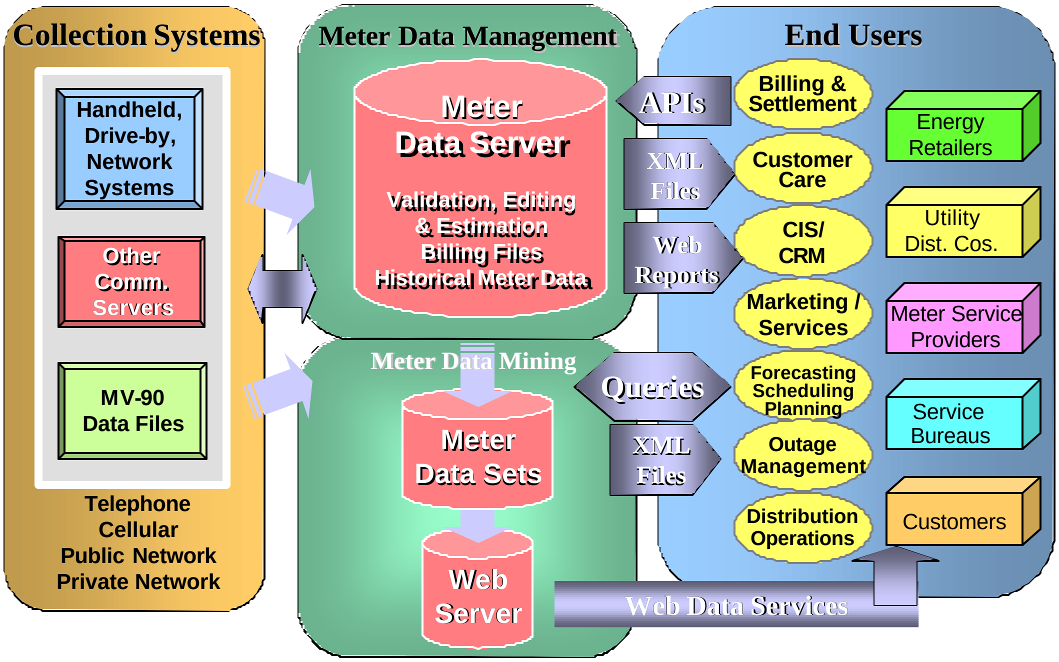


Figure 7.2.3 – Clear, well defined interfaces simplify system integration

7.3 Functional Elements

The DRI Architecture Reference model identifies the following functional elements.

7.3.1 Appliances

Information appliances are the equipment by which an end user or system employs the DRI. These typically have input and display capabilities for communication with other users or service providers, processing capabilities, and interfaces to communications networks and services. Information appliances could be single-purpose or multipurpose devices structured as a platform for supporting various applications. Current examples include thermostats, intelligent gateways with embedded web servers, computers, televisions and set-top boxes, and remote sensors.

7.3.2 Networks

Networks typically consist of transmission facilities, routers, switches, multiplexers, protocol conversion equipment, interworking units, and directories. Examples of communications networks are broadcast radio and television, cable television distribution systems, public telecommunications networks, wireless data networks, value-added networks, and private corporate networks. These networks are intermediate systems employed by users and application and service providers.

7.3.3 Resources

Information resources i.e., the content, are the "guts" and the goal of the DRI. Examples are meter data repositories, customer GIS and billing data, on-line financial transaction systems, and electronic transaction frameworks for business and industry databases.

7.3.4 Control points

Network service control points contain the means for managing networked elements of all kinds, including the physical infrastructure, services, and applications that use them. Network or service providers (or others) could choose to offer these control points, thereby providing a highly distributed set of mechanisms to manage the underlying capabilities of an open communications network and the use of other DRI enabling services. These management mechanisms will provide advanced capabilities such as custom addressing or routing, updating links to mobile or relocated destinations or resources, and the integration and management of diverse applications and services.

7.3.5 Applications

Numerous software applications are at the core user of the DRI. These applications implement all key aspects of the demand response system. Many of these applications are illustrated in Figure 7.3.5.1 below. This figure illustrates how all of these applications need access to meter data. How these applications access the meter data, through what interfaces, and in what formats is the realm of the reference design.

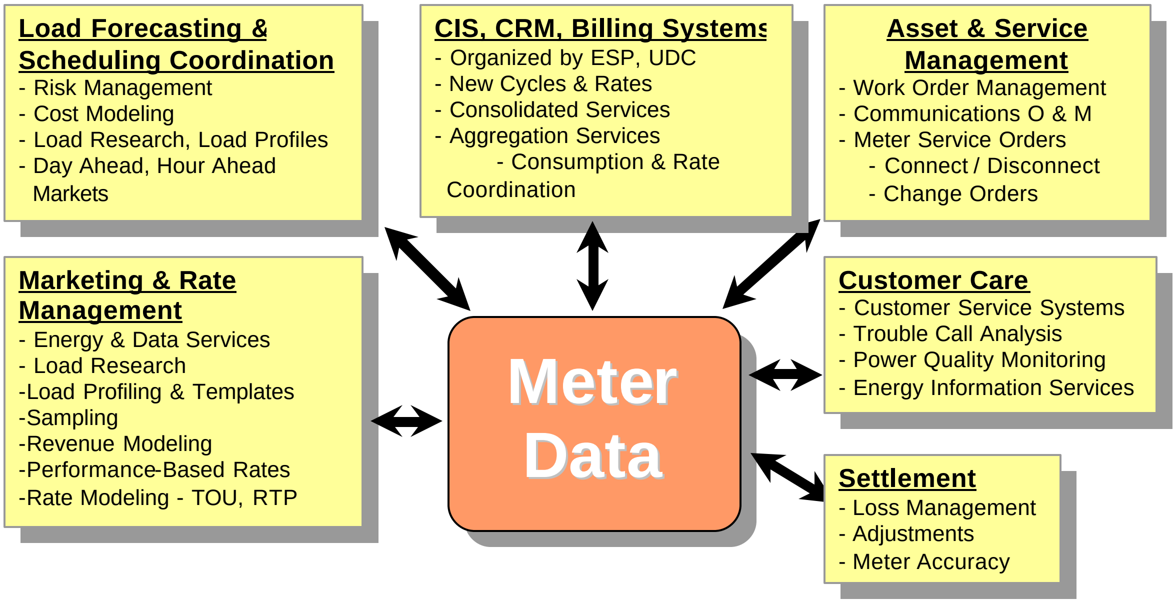


Figure 7.3.5.1 - Applications Needing Access to Meter Data

7.4 Interfaces and Protocols

Interfaces between the elements of the DRI's component layers must be well-defined so that information can efficiently move across and make use of capabilities located in each layer. There should be open specifications at least for some critical set of interfaces and protocols to facilitate competition and entry and promote interoperability. Thus, the boundaries between the layers must be permeable in this high-level conceptual rendering. For example, end-user applications (which may be marketed as a service to customers) can be built from combinations of enabling services, and may employ specific physical devices. Similarly, specialized applications may evolve, by broad adoption, into enabling services. Moreover, where the function of interfaces can be provided effectively in an integrated way by equipment operated by a given service provider or user, the methods and interfaces it employs do not need to be open or standardized.

The following interfaces and protocols will exist in the DRI in multiple instances and open, well-defined specifications should be developed for them.

1. Information appliance to communications network
2. Information resource to communications network
3. Communications network to communications network
4. Information resource to information appliance
5. Information appliance to information appliance
6. Information resource to information resource
7. Network service control point to communications network interface

It may be possible for information appliances and information resources to use the same interface to communications networks. This could allow individual users to take on the role of information providers. However, a relatively simpler communications-network-to-information-processing-device interface may be more cost effective.

A well-defined application-to-platform interface in information appliances could facilitate the development of applications that partly exist in an information resource and partly in an information appliance. Application programming interfaces are examples of such interfaces.

While the Reference Architecture defines points at which interfaces and protocols will be defined, this is not to imply that they will be uniquely defined at each point. To meet the varying needs of different users, service providers, applications, and domains, a large and evolving set of interfaces and protocols will need to be created. To achieve a true demand responsive infrastructure, interoperability and compatibility must be preserved. In addition to these interfaces and protocols, it will be important to define objects (documents, contracts, tokens, etc.) that are exchanged within the DRI and the formats in which these objects are coded for exchange. Other objectives that should drive the specification of DRI interfaces, protocols, and objects include the following:

- Interfaces, protocols, and objects in the DRI should be extensible whenever possible; this will allow for backward compatibility as new functionality is added. One method for attaining extensibility is to make extensions to interfaces self-describing.
- Interfaces and protocols should provide a well-defined set of management functions.
- DRI protocols should support a well-defined means of identifying the prices charged for commercial services. In this way, software agents, for example, could search for the best price for a given service.
- Protocols should provide for standard ways to find, access, retrieve, and store information in the DRI.
- DRI protocols must support portability and mobility of users and applications.
- Interfaces to communications networks should support a wide class of information processing devices with differing requirements in terms of bandwidth, delay, and reliability. These interfaces may support service negotiation characteristics including protocol conversion within the communication connection. For example, an information processing device could request data compression services of a communications network to allow the user to access multimedia information more efficiently.
- At its lowest layers, DRI protocols must provide a transparent and efficient means of transferring information. More complex, feature-rich protocol capabilities should only be evoked where needed and desired.
- The DRI should provide a high degree of protocol transparency so both old protocol suites and new emerging ones can be accommodated.

Figure 7.4.1 illustrates the overall process of mapping business rules to specific technologies and standards using a top down approach. The key concept here is to map the fundamental business rules and application requirements to a common set of interfaces and information models using technologies well suited to those tasks. In most cases, standards and technologies already exist to support these requirements (e.g. Figure 7.4.2 – the IEC TC 57 reference model) but this is not always the case.

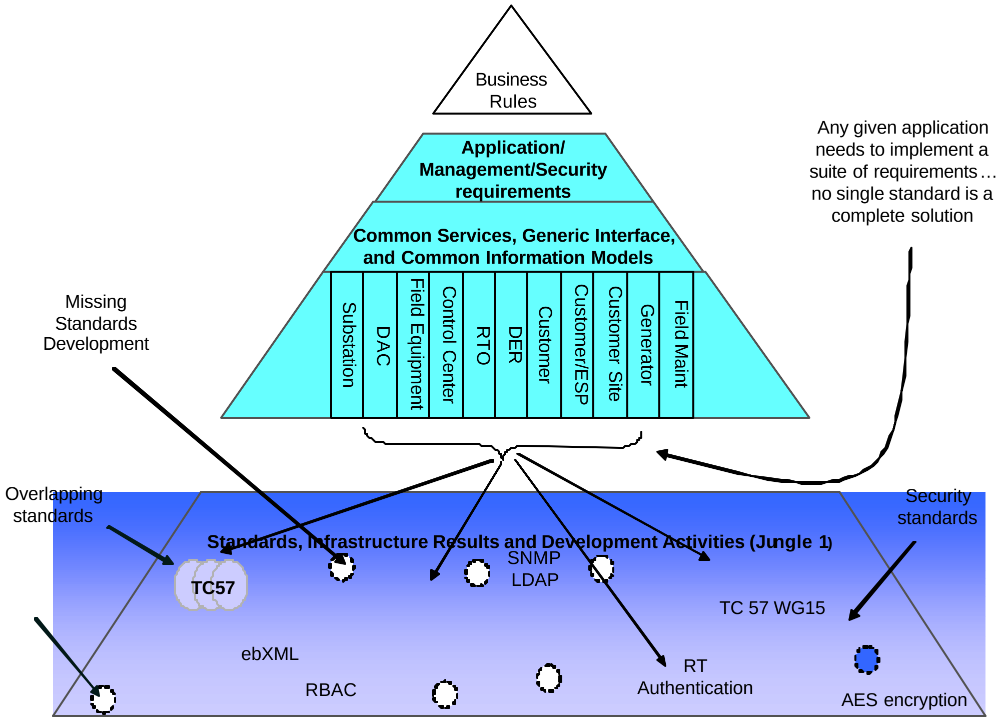


Figure 7.4.1 – From Business Rules to Supporting Standards

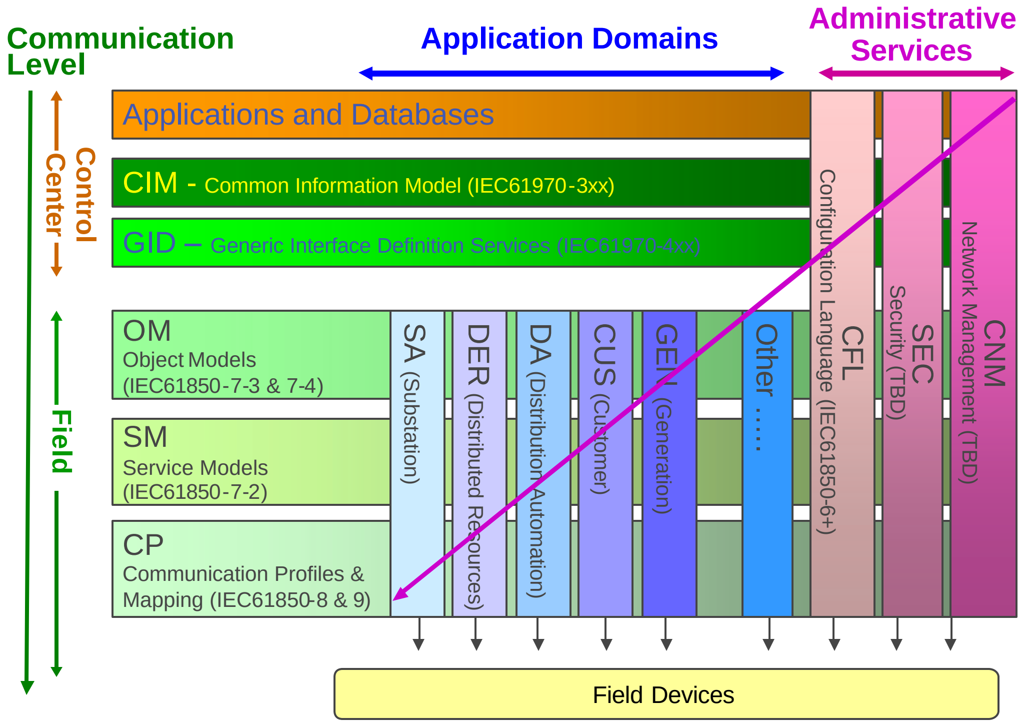


Figure 7.4.2 – IEC TC 57 Reference Model

8.0 Reference Design

It is recognized that something as forward thinking and far reaching as the DRI needs more concrete examples of what might constitute the DRI as well as to solve problems in the near future. A reference design can accomplish this goal in a way that is compatible with the longer term goals of the DRI.

8.1 What is a Reference Design?

A reference design describes a system in terms of the interconnection of basic functional elements and the interfaces between them. It clarifies where communication protocols must be defined and identifies groupings of functionality. It does not imply a physical implementation.

Unlike a reference architecture which is very abstract, a reference design can be thought of as an example of one possible implementation of the principles set forth in a reference architecture. A reference design may be as simple as a diagram illustrating core features of a cell phone (Figure 8.1.1), or more elaborate as a block diagram of a communications appliance (Figure 8.1.2), or as extensive as the sample circuit design for a set top cable box (Figure 8.1.3). In each case, the target audience is provided with common points of reference that indicate how the components of the system are expected to interact among themselves and with the outside world through clear definitions of standardized interfaces and points of interoperability.

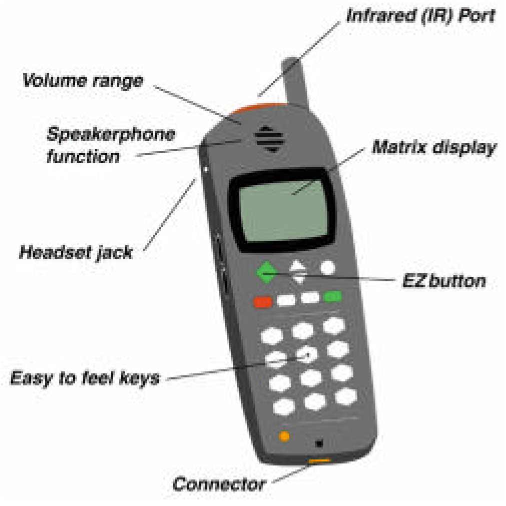
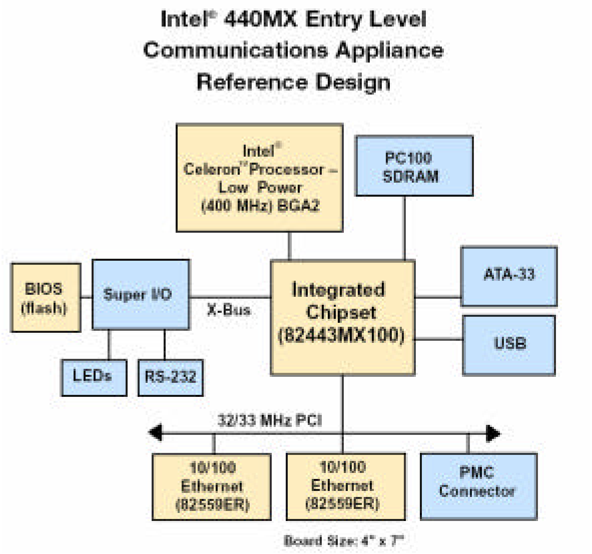


Figure 8.1.1 – Cellular Phone Reference Design



Intel® 440MX Entry Level Communications Appliance Reference Design
Intel® Celeron™ Processor – Low Power (400 MHz) BGA2
PC100 SDRAM
BIOS (flash)
Super I/O
X-Bus
Integrated Chipset (82443MX100)
ATA-33
USB
LEDs
RS-232
32/33 MHz PCI
10/100 Ethernet (82559ER)
10/100 Ethernet (82559ER)
PMC Connector
Board Size: 4" x 7"

Figure 8.1.2 – Communications Appliance Reference Design

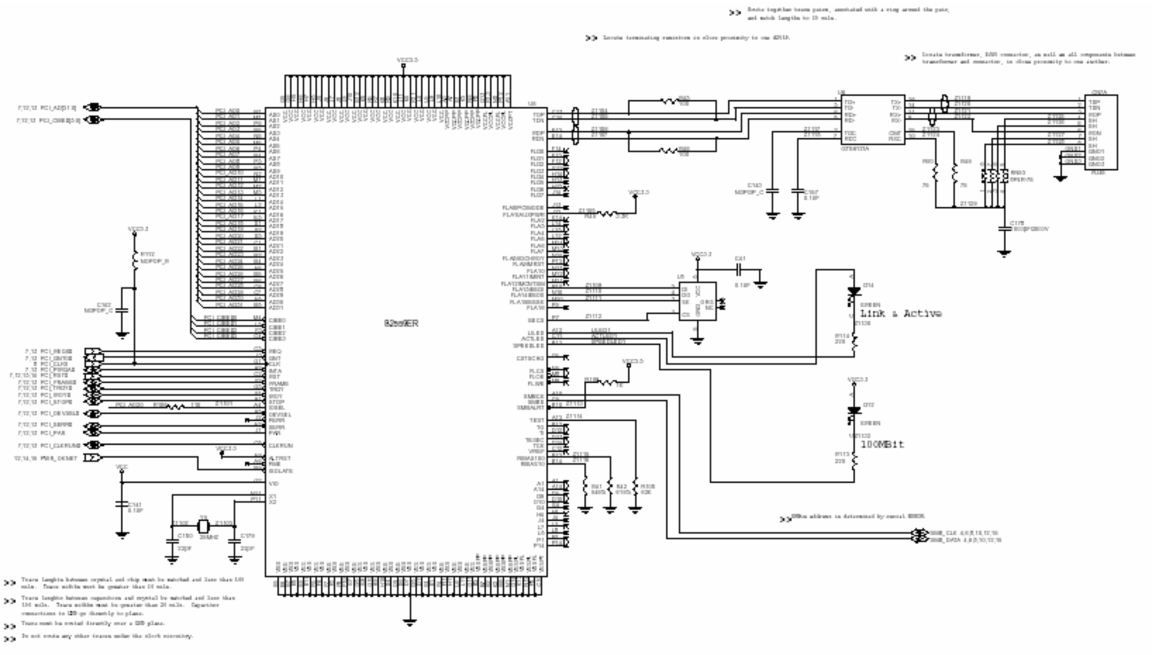


Figure 8.1.3 – Cable Box Reference Design

8.2 A Strawman Demand Response Reference Design

There are several key components of this strawman [D2] reference design:

- **Actors** the entities that need to exchange information (e.g., CAISO, LSE's, and UDC's)
- **Applications** the functions that need to be performed by the actors
- **Protocol** the underlying communication methods used to move bits and bytes
- **Language** a common language to facilitate information exchange
- **Objects** high-level definitions of objects that are independent of protocol and language
- **Translation** services that provide a way to allow information exchange with external systems
- **Security** overarching methods to ensure confidentiality, integrity, and availability

Figure 8.2.1 provides a graphical depiction of the strawman reference design and these components. The cloud in the figure depicts the domain of open information exchange. This means that within this logical zone, a well defined set of technologies based on open standards are deployed that allow a free flow of information to occur between applications without the complexity and expense of extensive protocol conversion and translation. Interoperability within this zone is an inherent property of the open systems implementation.

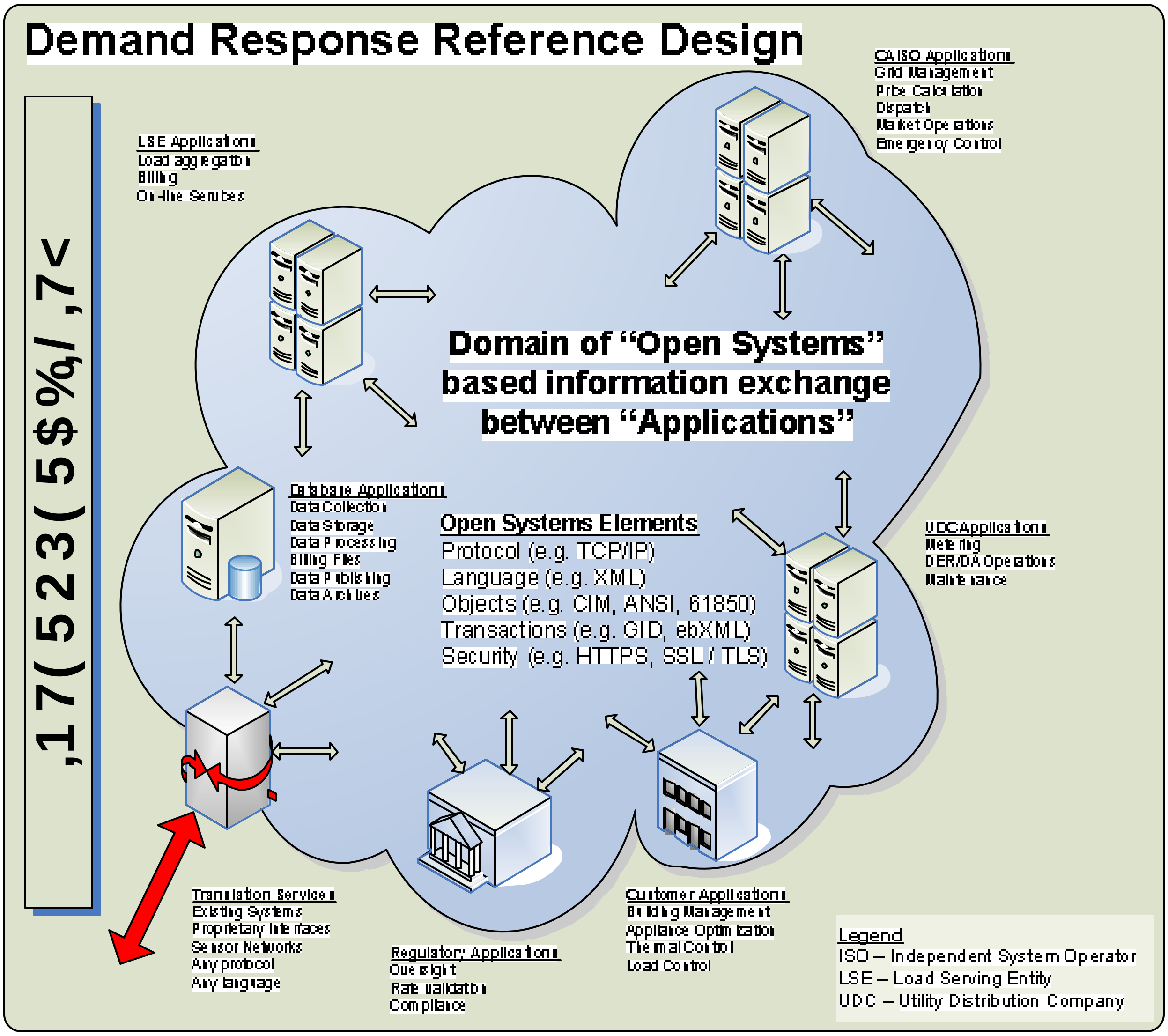
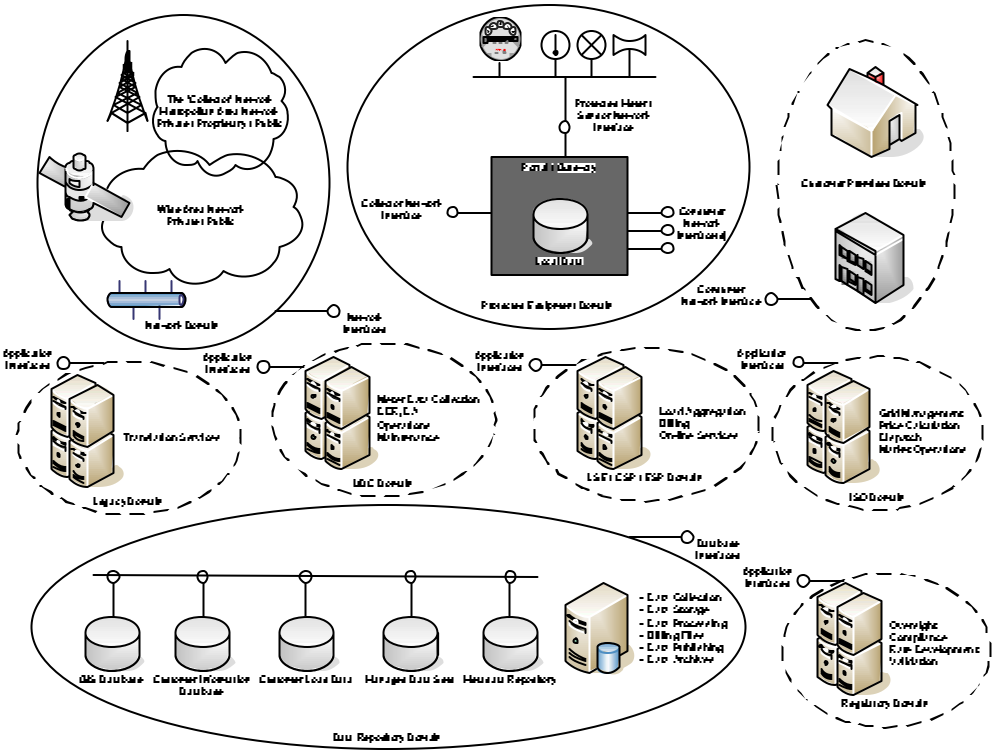
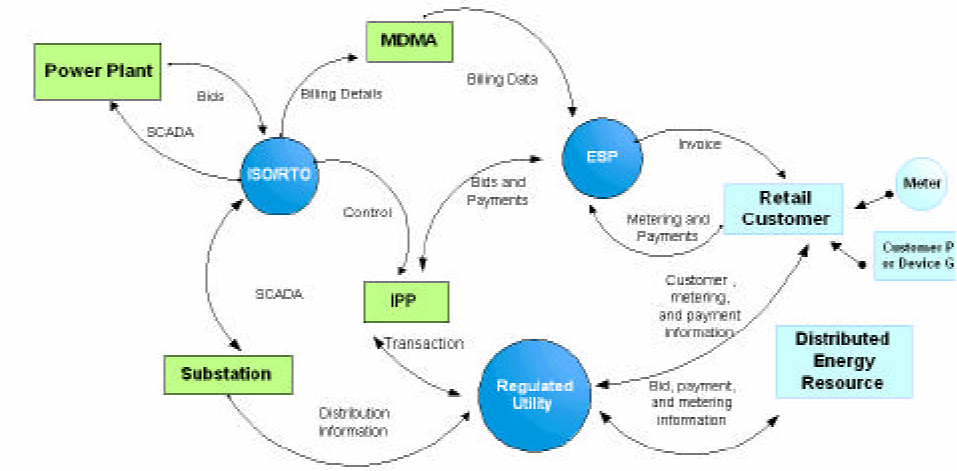


Figure 8.2.1 – Strawman Demand Response Reference Design

The area outside the cloud in the figure is the domain of external systems that implement proprietary protocols, languages, and unstructured information. These systems may represent pre-existing installations or new installations that are not able to directly participate in the open systems domain. Bridging the boundary between the two domains is a translation layer that facilitates interoperability between these external systems and the open systems domain. This design approach facilitates an inclusive rather than an exclusive policy necessary to prevent stranding assets and allows for innovation and rapid technological change.

A key aspect of the reference design is the concept of well defined points of interoperability between a more granular breakdown of actor and application domains. Figure 8.2.2 illustrates these domains and interface points.


The 'Collector' Network
Metropolitan Area Network
Private / Proprietary / Public
Wide Area Network
Private / Public
Network Domain
Network Interface
Premises Meters
Sensor Network
Interface
Portal / Gateway
Local Data
Collector Network
Interface
Consumer
Network
Interface(s)
Premises Equipment Domain
Consumer Premises Domain
Consumer
Network Interface
Application
Interfaces
Translation Services
Legacy Domain
Application
Interfaces
Meter Data Collection
DER, DA
Operations
Maintenance
UDC Domain
Application
Interfaces
Load Aggregation
Billing
On-line Services
LSE / CSP / ESP Domain
Application
Interfaces
Grid Management
Price Calculation
Dispatch
Market Operations
ISO Domain
Database
Interfaces
GIS Database
Customer Information
Database
Customer Load Data
Manager Data Sets
Metadata Repository
- Data Collection
- Data Storage
- Data Processing
- Billing Files
- Data Publishing
- Data Archives
Data Repository Domain
Application
Interfaces
Oversight
Compliance
Rate Development
Validation
Regulatory Domain


Power Plant
MDMA
Bids
SCADA
Billing Details
Billing Data
ISO/RTO
ESP
Invoice
Bids and
Payments
Retail
Customer
Meter
Metering and
Payments
Control
Customer P
or Device G
SCADA
IPP
Customer ,
metering,
and payment
information
Distributed
Energy
Resource
Transaction
Substation
Regulated
Utility
Bid, payment,
and metering
information
Distribution
Information

Finally, an important aspect of the reference design is its ability to support pre-existing proprietary and site-specific communication methodologies and protocols. Figure 8.2.4 shows a simplified version of the reference design given in Figure 8.2.1. This figure clearly shows how interoperability is achieved within the open systems domain by use of the common protocols, languages, objects, transactions, and security mechanisms discussed earlier (the platform independent information model). As mentioned earlier, interoperability with pre-existing proprietary and site specific systems is achieved through the use of translation services.

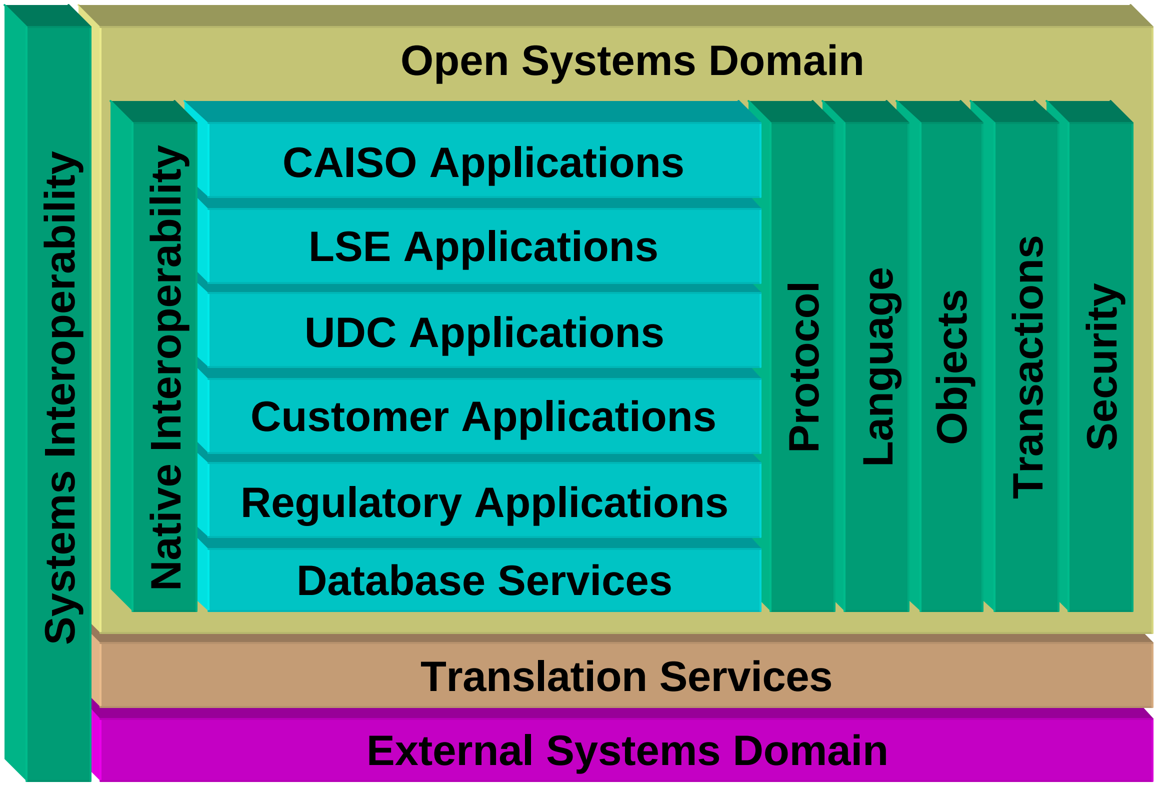


Figure 8.2.4 – Simplified Strawman Demand Response Reference Design

Figure 8.2.5 shows an example of how this might be implemented when implementing a demand response infrastructure at several different sites – each with unique, pre-existing hardware and software that will utilize the demand response control signals differently. In this example, the Polling Client and Business Logic blocks in the diagram are responsible for providing these translation services [R8]. Everything to the left of these blocks exposes a platform independent information model such that the Price Server application in this example does not have to be concerned with the communication details within each facility.

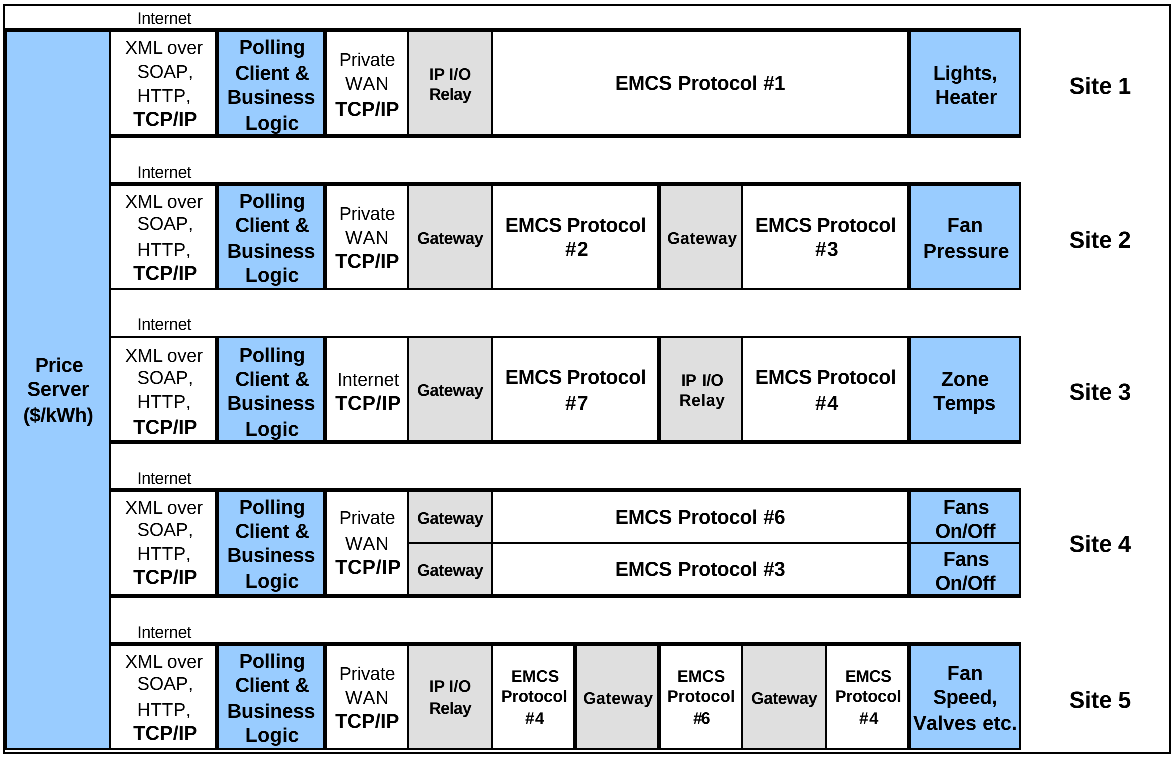


Figure 8.2.5 – System Architecture Overview, LBNL Automated Demand Response Test 2003. Example of proprietary and site specific communications that can still interoperate with the open systems domain.

At this point it is worthy to summarize by explicitly stating that:

> **"It is the definition of these actor and application domains, their points of interoperability, the transactions between then, and the requirement that standardized interfaces and services exist to facilitate information transfer that constitutes the reference design."**

8.3 Candidate Implementation Technologies

The strawman reference design depicted in figure 8.2.1 hints at several candidate implementation technologies. Although the DRI architecture as defined in earlier sections of this report can support a wide variety of technologies, practical implementations of the reference design must narrow down the technology set to a modest number of interfaces in order to accomplish the goal of seamless, low cost interoperability. We have identified several technologies that bear initial consideration by the working group that is eventually assigned the task of finalizing the details of the reference design. In summary, these technologies as related to each of the five areas of interoperability are:

Protocol

TCP/IP , HTTP – the protocol suite used on the Internet
ANSI Meter Protocols - ANSI C12.18, C12.21, C12.22
ASHRAE SSPC 135 building automation and control protocol (BACNet)
Intercontrol Center Communication Protocol - ICCP/TASE.2

Language

Hypertext Markup Language (HTML)
Extensible Markup Language (XML)
ANSI Meter Tables - ANSI C12.19

Object Modeling

ANSI Meter Tables - ANSI C12.19
IEC 61850 – Comprehensive platform independent information model
IEC 61970 – Common Information Model (CIM)

Transaction

SOAP, XML Web Services
ebXML
IEC 61970 - Generic Interface Definitions (GID)

Security Specific Protocols, Languages, Objects and Transactions

X.509 – Public Key Infrastructure
Transport Layer Security (TLS)
HTTPS – Secure Hypertext Transport Protocol
SCP – Secure Copy Protocol
SSH – Secure Shell

Throughout this report, physical media has been assumed to be totally independent of any of the above technologies and classifications. It is however helpful to narrow the field somewhat in this area as well – especially given the growing number of wireless and power line carrier technologies.

Physical

Wired Ethernet – common twisted pair and fiber forms
Digital Subscriber Line (DSL) and variants (e.g. ADSL)
Cable Modem (CableLabs reference design compatible)
Wireless Ethernet - IEEE 802.11b (WiFi, WIMAX)
Power Line Carrier – HomePlug Alliance compatible schemes

Detailed descriptions of these technologies and their architectural significance can be found in Volume IV, Appendix D (Technologies, Services, and Best Practices) of the Integrated Energy Communications System Architecture final report [R10].

9.0 Scenarios

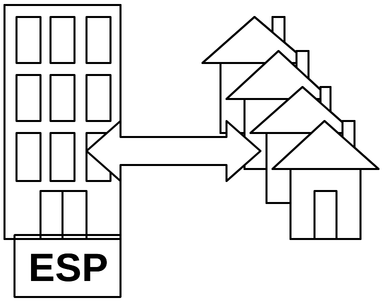
This section presents scenarios describing realistic applications that may become available with the envisioned DRI. They illustrate some of the substantive benefits the DRI can bring to society, and are accompanied by descriptions of the role of new DRI technology and its organization according to the proposed architectural framework.

9.1 Scenario I: Customer to Energy Service Provider Communication

The reference design defines several domains as shown in Figure 8.2.1. The use of the domain construct allows information exchange discussions in regards to particular types of application/business exchanges. However, security constructs need to be applied to this model. It could be convenient to discuss security in regards to a collaboration of integrated security functions that cross all domains, but the definition of such a collaborative environment is difficult and often fails, in reality, since multiple business entities are involved. The difficultly could exist even within a single domain.

To solve the issue of security granularity, boundaries, and security management responsibility, the model of Security Domains has been introduced (see Annex A). Based upon the Security Domain construct, each DRI domain could encompass one or multiple security domains; but the important security issue is whether the security services are required for information crossing multiple security domains (inter-domain) or are strictly for information within one security domain (intra-domain).

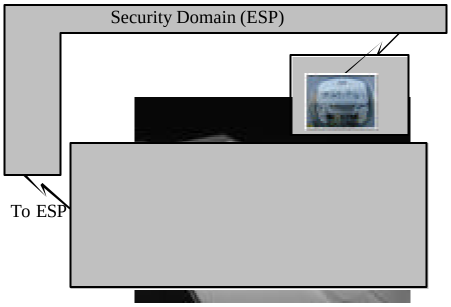
Since there is not a one-to-one relationship between DRI Domains and Security Domains, an example may be useful to illustrate how to use the recommendations set forth in this document. For the purposes of this example, interaction between the Customer and ESP domains is considered. This interaction is referred to as an environment in the IECSA Reference Architecture.



This environment encompasses communications between end customers and the utility, aggregator, or Energy Service Provider (ESP) to which they are connected. This environment includes the requirements for what is traditionally known as Automatic Meter Reading (AMR).

Typical applications: Customer metering, management of distributed energy resources on customer sites, real-time pricing and demand response.

The "demand response" application of this Environment will be used in the example as it provides a relevant example of the required coordination between more that one security domain. However, "demand response" can be implemented in two different manners:



1. The ESP provides information requesting energy consumption curtailment and the customer takes action based upon the supplied information.
2. The ESP acts on behalf of the customer and actually takes the curtailment action (e.g. controls customer owned assets). This is the mechanism that will be investigated in the example.

There are several steps involved with applying the security concepts put forth in this appendix to this example. The following sections will attempt to describe each step.

9.1.1 Example of Security Domains

Upon initial inspection, a simplistic Security Domain model of the example would lend itself to a three (3) security domain model. The three potential domains could be:

1. ESP: The Energy Service Provider is its own security domain. It has its own security policy and security management. The ESP would need to be able to communicate with the Meter (e.g. for meter reading) and to the building's Gateway for demand management.
2. Meter: This includes the metering, AMR system, and communication infrastructure. It represents the system that allows the ESP or other entities to access the readings of the meter.
3. Gateway: This represents a boundary for communication from external systems to systems within the customer premises.

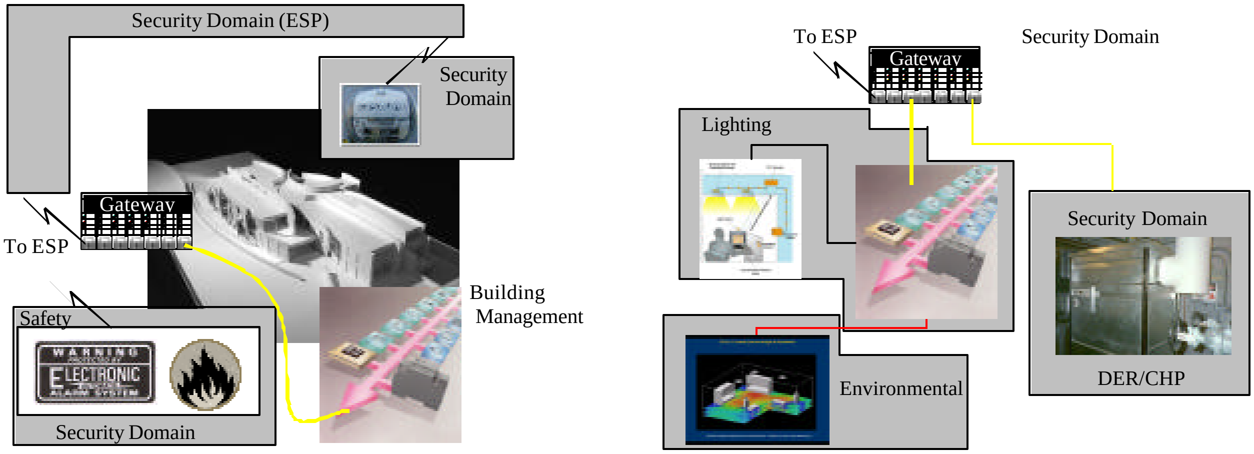


Figure 9.1.1 - Example Security Domain Choices

However, Figure 9.1.1 clearly depicts that there are more security domains than the simplistic model conveys. The more developed model adds the following domains:

- Safety and Physical Security: Most buildings and other customer premises will have a separately managed domain that is involved with safety and physical security (e.g. fire, physical intrusion, etc.). Some ESP's may offer to monitor the information provided by this domain as a tertiary service (e.g. Home Security Services), but for the purposes of the example, this information will be exchanged with the entity that is responsible for maintaining and configuring the safety devices. Therefore, by definition, the Safety domain includes the management entity that is external to the customer premises. However, the information from the safety domain may be accessed by entities within the building (excluded from the example).

- Lighting and HVAC Domains: This domain covers lighting, HVAC, and other building and campus environmental systems.
- DER: This domain includes the controls of any Distributed Energy Resources (DERs) within the customer premises, of which Combined Heat and Power (CHP) distributed energy would be prevalent in most industrial facilities. It is the CHP resource that is justified as being its own security domain and this will be used in the example. The inclusion of DER also causes the inclusion of another IECSA Environment.

For the purposes of the example, there are two interesting exchanges: ESP to/from the Gateway and the Lighting/HVAC security domains, and ESP to/from the DER security domain.

For this example, in both scenarios, it is assumed that the ESP to Gateway communication will be via the Internet. It is also assumed that the Gateway to either of the other domains will be via TCP/IP and Ethernet. However, it would be typical that the internal communication infrastructure for Lighting/HVAC domains and the DER/CHP security domains would be different.

Communication	**ESP to Gateway (Inter-domain)**	**Gateway to Customer Premises Security Domains (Inter-domain)**	**Customer Premises Network (Intra-Domain)**
ESP to Lighting/HVAC	Internet, Web Services	TCP/IP and Ethernet, IEC 61850	BACnet LonWorks
ESP to DER	Internet, Web Services	TCP/IP and Ethernet, IEC 61850	Modbus/TCP

Figure 9.1.2 - Summary of Example Communication Technologies

For each of the identified security domains, full security policies and Security Management Infrastructures (SMI) needs to be developed. The first issue that needs to be decided is which security services to implement for Intra-domain communications and then selecting the types of credentials that will be used for intra-domain and inter-domain identification purposes.

Step 1: Establish Identity Establishment Policies

It is recommended, in previous section of this appendix, that each security domain establish its own identity establishment policies and procedures. The basic issue to be resolved is whose credentials are acceptable for identity establishment. There are two options for inter-domain exchanges:

1. The target security domain (e.g. the one to which the connection/request is being issued) issues the appropriate credential(s) to the entity that it will allow to connect.
2. In the case of certificate-based credentials, this allows the security domain to issue time-limited certificates that expire naturally and therefore would be a good mechanism to provide temporary access.

There are two sets of credentials that need to be issued by the security domain if this process is used: one to identify the external domain entity and the other that identifies the security domain entity (e.g. gateway). This is needed since identity establishment is required by both entities.

The target security domain accepts the external entity's credential (e.g. the domain does not issue the credential) but does supply the credential to establish identity of the security domain.

It is recommended that, when possible, the security domain issue both credentials. However, security domain boundaries must be able to handle either method.

Besides the management of the credentials, the credential type needs to be identified for use by the security domains. This is often based upon the communication infrastructure that the security domain supports.

For the example, the following could be the selected inter-domain credentials and how to exchange the certificates:

Inter-Domain Exchange	**Communication Method**	**Credential to use**	**Exchanged by**
ESP to Gateway	Internet, Web Services	X.509 Certificate	W3C - SOAP Security Extensions
Gateway to Customer Premises Network	TCP/IP, IEC 61850	X.509 Certificate	IEC 62351-4 (ACSE Authentication)

Figure 9.1.3 - Example Certificate and Certificate Exchange choices

Step 2: Establish Confidentiality Policies

Once the appropriate selections have been made on a policy basis, the next policy issue is if confidentiality needs to be provided and if so how it should be provided.

Inter-Domain Exchange	Communication Method	Confidentiality Needed	Provided by
ESP to Gateway	Internet, Web Services	Yes	Secure HTTP (HTTPS)
Gateway to Customer Premises Network	TCP/IP, IEC 61850	Questionable	IEC 62351-3 and IEC 62351-4

Figure 9.1.4: Example Confidentiality Policy

Once the confidentiality decision has been made, the tokens/credentials required to establish and maintain confidentiality need to be decided upon. In the case of this example, both HTTPS and IEC 62351-3 (e.g. TLS) make use of X.509 certificates and therefore could be managed in a similar fashion to the identity establishment credentials.

Note: If the tokens/credentials required to establish confidentiality are determined to be different than the identity establishment credentials, it may be advisable for the policy to attempt to align the credentials in order to minimize maintenance issues. In some cases, this alignment may not be possible, and thus the SMI will become more complicated.

Step 3: Establish Message Integrity Policies

Message integrity is the next policy issue. In the IEC 62351-3 specification, the TLS Message Authentication Code (MAC) use is mandatory. It is recommended that the policy decision for HTTPS also mandate the use of the TLS MAC capability.

Step 4: Establish Firewall Transversal Policies

The next policy issue is that of Firewall Transversal. Should the inter-domain boundary be protected by a firewall and what is the mechanism for allowing transversal of the firewall if implemented? In this example, each domain boundary (e.g. the building gateway and the Customer Premises Network protocol conversion gateways) offers a potential to implement a firewall. The policy must decide what functions the firewall is to provide (see page 38 in Annex A for the function definitions). For the example, the following decisions could be made:

Firewall Function	ESP to Building	Building to Customer Premises Network	Comment
Media Isolation	Yes	Yes	
Address Translation	Yes	Yes	Building to Customer Premises Network Naturally requires this since the addressing structure of the intra-net is different.
Protocol/Port Restriction	Yes	Yes	
Audit	Yes	Yes	
Identity Establishment	No	No	The use of HTTPS (for end-to-end confidentiality) becomes problematic for identity establishment at a firewall boundary. The use of IEC 62351-3 (TLS) makes identity establishment problematic.
Access Control	No	No	Could be done by the building firewall based upon address.
Confidentiality	No	No	Since the policy desire is to have confidentiality provided from the ESP to the Customer Premises Network gateway, confidentiality is being provided by another mechanism (e.g. HTTPS and IEC 62351-3).
State based Inspection	No	No	With encryption encapsulating the actual protocol that could be analyzed, state based inspection is not possible.

Figure 9.1.5 – Example Firewall Traversal Policy

Step 5: Establish Role-Based Access Control Policies

One of the next policy issues that need to be address is that of roles versus access control once identity is established. It would be recommended that Role Based Access Control be the preferred mechanism. It is further recommended that the following privileges be considered: Read, write, configure, execute, control, and view. Based upon these privileges, the following Roles could be defined.

Role	**Assigned Privileges**					
	Read	**Write**	**Configure**	**Execute**	**Control**	**View**
Monitor	x					x

Role	**Assigned Privileges**					
	Read	**Write**	**Configure**	**Execute**	**Control**	**View**
Maintenance	x	x	x	x		x
Control	x	x			x	x
Super	x	x	x	x	x	x

Figure 9.1.6 - Suggested Roles vs. Privileges

Step 6: Determine Audit Policies and Information
It is important to realize that the audit policies and the information available in the audit records constitute the information that can actually provide repudiation/non-repudiation capability of particular transactions. In this example, the types of information that needs to be placed in the audit records vary by security domain.

In general, the audit records should contain the information as recommended in the Audit Service section of Annex A. There is a need to be special attention given to the audit capabilities associated with the different access control privileges. However, the recommendations are the audit section is non-specific in regards to the issue of writes, configuration, and control privileges (these privileges may vary based upon policy).

It is extremely important that any interaction where that can cause a potential change in the process behavior, that the information regarding that transaction be placed within an audit record. Such a policy/audit record combination would allow audit trails to be created that could provide a non-repudiation function for control actions or configuration changes that cause damage or mis-operation. With such a policy, the direct control of the DER resource or HVAC system could be audited and allow thereby allowing secure and auditable exchanges that would truly facilitate demand load functionality and potentially real time pricing based control of the system.

Step 7: Select Deployment Architecture and Equipment
Once all of the associated policy issues with inter-domain information exchanges have been documented, it is now an issue of selecting a deployment architecture and equipment that meet those requirements.

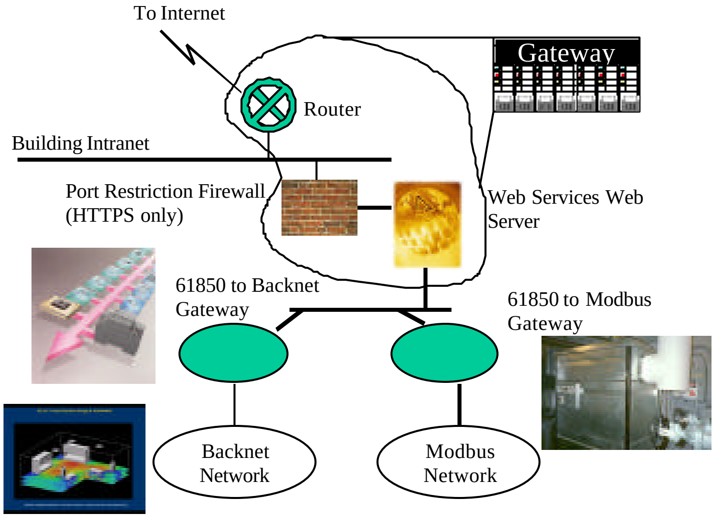


Figure 9.1.7: Web Service based Customer Interface Example

It is worthwhile to note that there could be alternate choices that could better facilitate communication and diagnostics. The use of web services as the gateway to the building is only truly required for the load demand commands from the ESP (this is the typical mechanism used). Alternate architectures could allow direct access through the use of IEC 61850 and or Modbus/TCP. However, since Modbus/TCP does not currently have the capability to utilize TLS or true authentication, the latter is not recommended until/unless TLS and authentication capabilities are added to Modbus/TCP. The following shows an alternate architecture.

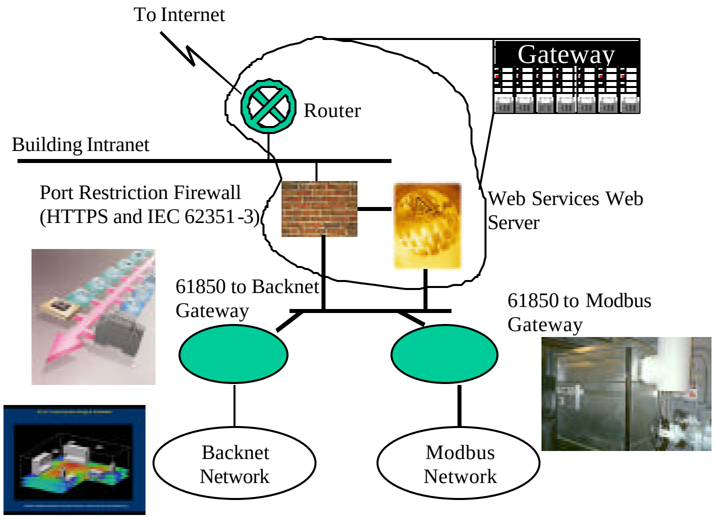


Figure 9.1.8 - Alternate Architecture that could allow direct 61850 communications

In general, implementation of security requires that the policy be established first, deployment architecture second, deployment equipment third (not addressed in this example), development of security test strategies/monitoring, re-evaluation, and then deployment.

One such issue, raised in the alternate architecture, is the issue of confidentiality for both the BACnet and Modbus gateways.

Figure 9.1.4Figure 9.1.4 (Example Confidentiality Policy) shows the need for Confidentiality marked “Questionable”. However, the alternate architecture clearly allows communication from the Internet, through the firewall, to be exchanged directly with either the DER or Lighting/HVAC security domains. Without the confidentiality and integrity services being mandated/available for such exchanges security will be compromised. Thus for the alternate architecture, the policy would need to specify:

Inter-Domain Exchange	**Communication Method**	**Confidentiality Needed**	**Provided by**
ESP to Gateway	Internet, Web Services	Yes	Secure HTTP (HTTPS)
Gateway to Customer Premises Network	TCP/IP, IEC 61850	Yes	IEC 62351-3 and IEC 62351-4

Figure 9.1.9 – Alternate Confidentiality Policy

Since IEC 62351-3 specifies the use of the TLS MAC, the integrity service is implemented via default. The SMI's, in the example, would be required to retrieve and analyze the audit records on an interval set by the policy. Additionally, the ability to have a firewall alert upon non-authorized access attempts could prove useful.

9.2 Scenario II: Extending the Example: Real Time Pricing

There are two scenarios through which demand load control (e.g. discussed in the previous example) can be extended to incorporate real time pricing (RTP). The RTP scenario involves an agent issuing the pricing signal (e.g., a pricing agent) and a load management agent (including DER dispatch) that understands how to manage load/generation based upon the price signal.
The location of the agents could be:

Co-located in the ESP security domain.

> In this particular scenario, the ESP would issue the load control commands and has already been accommodated in the example.

Distributed locations of agents.

> The pricing agent is located externally to the set of security domains that are contained within the building/campus. There are two logical locations for the pricing agent: the ESP, some government/state regulatory entity, or both. For the purpose of the extended example, the example will assume that the pricing agent is located within the ESP's security domain and the load management agent is located within the building/campus security domain infrastructure.

This deployment strategy allows two potential methods to deliver the pricing signal: the ESP sends the pricing information to the load management agent or the load management agent polls for pricing information.

If the ESP sends the pricing information to the load management agent and uses the same Web Service exchange approach (typical), then the security domains previously discussed already cover this case.

If the load management agent is required to poll for the data (not typical), then the ESP must take appropriate measures at its security domain boundary. This case will not be discussed as the policies and technologies that would be used are similar to those already discussed in 9.1.

10.0 DRI Evolution

The move from today's jumble of proprietary demand response implementations to the envisioned DRI will be achieved through the evolution of four fundamental building blocks:

- Computing and information appliances
- Communications networks
- Information and computing resources
- The architecture itself

10.1 Evolution of Computing and Information Appliances

Computing and information appliances will become vastly more powerful, affordable, and plentiful.

10.2 Evolution of Communications Networks

Access to networked resources will become more flexible as transport media are linked, and as fundamental data carrying and interchange standards emerge for various applications. Cable and DSL based Internet connectivity are becoming ubiquitous. Spurred by new frequency allocations, wireless personal communications services networks are emerging providing a wide range of options for data service delivery. Speed and flexibility will provide the foundation for information flows of a scale and degree of complexity far greater than what we see today.

10.3 Evolution of Information and Computing Resources

Database technology and navigation techniques will evolve to enable users and systems to locate information resources quickly and efficiently. Security capabilities of the infrastructure will be enhanced with mechanisms to protect the rights of both users and suppliers of information. User interfaces to the infrastructure will improve to allow easier and more natural interaction throughout the DRI, and integrated accounting, coordination, management, and billing mechanisms will create the environment for both commercial and other activity, such as government services, which require formal accountability and oversight.

10.4 Evolution of the DRI Architecture

A DRI architecture must be capable of complex and unpredictable change. It must adapt to the introduction of new technologies and to new needs and requirements generated over long periods of time by the producers and consumers that rely on it. Many factors will be essential to the DRI's successful development and future evolution. Fundamental elements, interfaces, protocols, objects, and facilities must be identified and then managed throughout their operational life. Procedures for maintaining as well as for phasing the introduction and withdrawal of critical elements must be developed.

It will not be acceptable for organizations to rely on DRI elements only to find them unavailable in any form. Procedures need to be developed for phasing transitions from one set of elements to another. Backward compatibility should be maintained in orderly transitions. Meters and embedded systems must not be rendered unusable when changes occur. Not everyone can be expected to make changes instantaneously. Therefore, all DRI elements must be carefully and thoroughly documented, including rationale, technical designs, implementation details, user interfaces and capabilities, etc.

As a framework consisting of standardized interfaces and protocols, a DRI architecture will provide the foundations, hooks, and handles for others to build upon. Thus, no single individual or organization is likely to be *the* DRI architect. Rather, many varied individuals and organizations will contribute to and guide its evolution. Many of these will be driven by the content that flows throughout the infrastructure in their roles as information services, facilities, and equipment providers. They, and many more individuals and organizations, will constitute the users and customers of the DRI. The DRI will thus be shaped by the evolution of the commercial, noncommercial, public, and private applications that will depend on it.

To achieve coherent and consistent performance in the DRI and to allow for a logical evolutionary progression, an enduring public process is required that allows for the best ideas about the infrastructure's current and future performance to be collected, analyzed, reformulated, and used as a basis for continual upgrading and improvement. This effort cannot be the province of any single interest group. A potential mechanism for effectively addressing this need could be the formation of a representative body drawn from developers, users, service providers, and policy makers from all sectors.

Such a body must work under a sufficiently broad substantive and legal charter to enable forthright deliberation and the maintenance of consensus on fundamentals. Its charter must include enduring coordination of interests rather than responsibility for implementing programs or undertaking of operational activities. The group can succeed only if it is endowed with a sufficiently independent resource base, which is guaranteed for a sufficient period. Then, the group can truly be above the short-term issues that plague present attempts at collaboration within and across industry and government, and can be adequately staffed to achieve its mission.

11.0 Next Steps

After achieving broad consensus on this framework for a DRI architecture and an intermediate reference design, we need to focus upon the following issues in order to refine and extend it:

Interoperability What minimum set of agreed-upon interfaces, protocols, and objects must exist to enable the DRI? Which of these already exist? What forums and mechanisms can be used to obtain agreements on the remaining set?

Services specification What are the critical services in each of the layers of the DRI Functional Services Framework model?

Scenarios What scenarios, and detailed technical descriptions of how the elements of the DRI work to enable them, would be useful to better define and explain the DRI?

Pilot projects What pilot projects would help verify the proposed DRI architecture, identify further issues in DRI definition, and focus industry efforts on DRI development?

Migration What are the roadmaps for evolving from the current computing and communications infrastructure to the envisioned DRI?

Answering these questions will be the task of one or more workshops, working groups, or industry organizations that take on the task of working out the details of the reference design.

12.0 Definitions

[D1] Architecture

1. The software architecture of a program or computing system is the structure or structures of the system. This structure includes software components, the externally visible properties of those components, the relationships among them and the constraints on their use. (based on the definition of architecture in [R6])

2. A software architecture is an abstraction of the run-time elements of a software system during some phase of its operation. A system may be composed of many levels of abstraction and many phases of operation, each with its own software architecture. [R3]

[D2] Strawman

A strawman is an object, document, person, or argument that temporarily stands in for and is intended to be "knocked down" by something more substantial.

In software development, a crude plan or document may serve as the strawman or starting point in the evolution of a project. The strawman is not expected to be the last word; it is refined until a final model or document is obtained that resolves all issues concerning the scope and nature of the project. In this context, a strawman can take the form of an outline, a set of charts, a presentation, or a paper. [R7]

[D3] Reference Architecture

A reference architecture is the generalized architecture of several end systems that share one or more common domains. The reference architecture defines the infrastructure common to the end systems and the interfaces of components that will be included in the end systems. The reference architecture is then instantiated to create a software architecture of a specific system. The definition of the reference architecture facilitates deriving and extending new software architectures for classes of systems. A reference architecture, therefore, plays a dual role with regard to specific target software architectures. First, it generalizes and extracts common functions and configurations. Second, it provides a base for instantiating target systems that use that common base more reliably and cost effectively. [R4]

[D4] Reference Model

A reference model is a framework for understanding significant relationships among the entities of some environment, and for the development of consistent standards or specifications supporting that environment. A reference model is based on a small number of unifying concepts and may be used as a basis for education and explaining standards to a non-specialist. [R5]

[D5] Entity, Entities – synonymous with Actor

A system, person, place or thing that is involved in information exchange with other systems, persons, places or things. Also referred to in the information technology and modeling world as an actor.

[D6] Protocol

1. A formal set of conventions governing the format and control of interaction among communicating functional units. Note: Protocols may govern portions of a network, types of service, or administrative procedures. For example, a data link protocol is the specification of methods whereby data communications over a data link are performed in terms of the particular transmission mode, control procedures, and recovery procedures. **2.** In layered communications system architecture, a formal set of procedures that are adopted to facilitate functional interoperation within the layered hierarchy. **3.** [In INFOSEC, a] set of rules and formats, semantic and syntactic, permitting information systems (IS's) to exchange information. [INFOSEC-99] [R9]

13.0 References

[R1] Borenstein, Jaske, and Rosenfeld , "Dynamic Pricing, Advanced Metering, and Demand Response in Electricity Markets" , The Hewlett Foundation Energy Series Foundation monograph, September 2002

[R2] W3C Glossary **-** http://dev.w3.org/cvsweb/~checkout~/2002/ws/arch/glossary/wsa-glossary.html

[R3] *Architectural Styles and the Design of Network-based Software Architectures*, PhD dissertation, R. Fielding, 2000 (See http://www.ics.uci.edu/~fielding/pubs/dissertation/top.htm.)

[R4] *Using the Architecture Tradeoff Analysis Method(SM) to Evaluate a Reference Architecture: A Case Study*, B. Gallagher, June 2000 (See http://www.sei.cmu.edu/publications/documents/00.reports/00tn007/00tn007.html .)

[R5] http://ssdoo.gsfc.nasa.gov/nost/isoas/us04/defn.html

[R6] *Software Architecture in Practice*, ISBN 0201199300, L. Bass, P, Clements, R. Kazman, 1997

[R7] SearchCRM Glossary **-** http://www.searchcrm.com/

[R8] Piette, M.A., O. Sezgen, D.S. Watson, N. Motegi 2004 “Development and Evaluation of Fully Automated Demand Response in Large Facilities”, Lawrence Berkeley National Laboratory

[R9] American National Standard for Telecommunications - Telecom Glossary 2000 - T1.523-2001 - http://www.atis.org/tg2k/

[R10] “Integrated Energy Communications System Architecture Final Report”, 2004, Electricity Innovation Institute (E2I) Consortium for Electric Infrastructure to Support a Digital Society (CEIDS). http://www.iecsa.org/

14.0 Acronyms

This section contains definitions of all of the acronyms found in this report. Where full definitions beyond the actual words behind the acronym are not given here, they are either considered self evident and/or can be found defined within the report in context.

AES Advanced Encryption Standard

A symmetric key encryption technique which will replace the commonly used DES standard. It was the result of a worldwide call for submissions of encryption algorithms issued by NIST in 1997 and completed in 2000. The winning algorithm, Rijndael, was developed by two Belgian cryptologists, Vincent Rijmen and Joan Daemen. AES provides strong encryption in various environments: standard software platforms, limited space environments, and hardware implementations.

AMR Automatic Meter Reading

ANSI American National Standards Institute

The American National Standards Institute (ANSI) is a private, non-profit organization (501(c)3) that administers and coordinates the U.S. voluntary standardization and conformity assessment system. The Institute's mission is to enhance both the global competitiveness of U.S. business and the U.S. quality of life by promoting and facilitating voluntary consensus standards and conformity assessment systems, and safeguarding their integrity.

API Application Programming Interface

A formalized set of software calls and routines that can be referenced by an application program in order to access supporting computational and network services.

ASHRAE American Society of Heating, Refrigerating and Air-Conditioning Engineers

CAISO California Independent System Operator

The California Independent System Operator Corporation (ISO) was created as part of the restructuring of the California electric industry established by Assembly Bill 1890 in 1996. The ISO manages the energy grid that supplies electricity to three-quarters of California. It operates Day-Ahead and Hour-Ahead Markets for ancillary services and transmission, and a Real-Time Market for balancing energy supply and demand. With authorization from the Federal Energy Regulatory Commission (FERC), the ISO commenced operation in 1998.

CEC California Energy Commission

CEIDS Consortium for Electric Infrastructure to Support a Digital Society

A public/private partnership managed by the Electricity Innovation Institute (E2I) and Electric Power Research Institute (EPRI). A diverse group of stakeholders - including domestic and international energy companies, federal and state agencies, and information technology companies – that has come together with a visionary goal: to help today's electric power system evolve into an intelligent infrastructure that integrates major changes in functionality and advances in communications, computing, and electronics to meet the energy needs of the digital society.

CIEE The California Institute for Energy and Environment

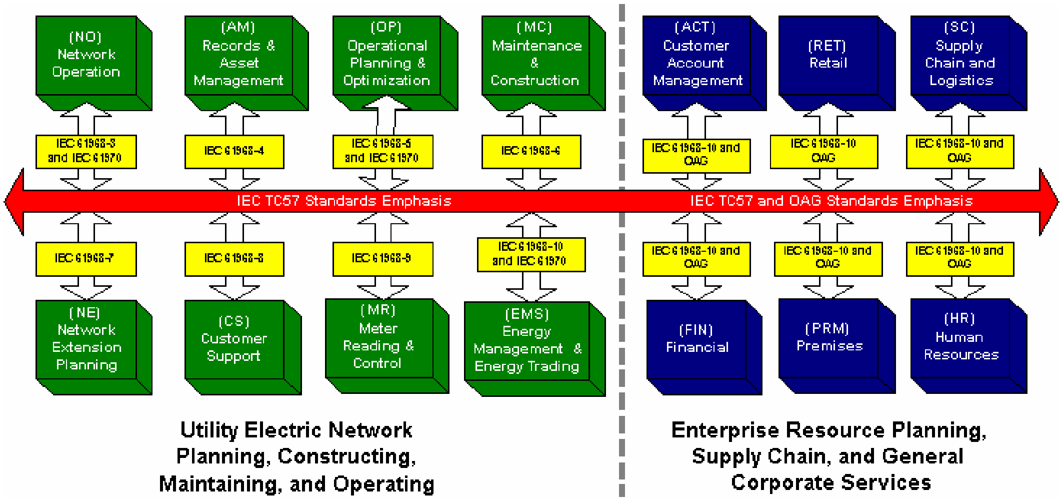
An innovative University of California partnership of energy agencies, utilities, building industry, non-profits, and research entities designed to advance energy efficiency science and technology for the benefit of California and other energy consumers and the environment. CIEE is a branch of the University of California Energy Institute California Institute for Energy and the Environment.

CIM Common Information Model

Under the auspices of the International Electrotechnical Commission (IEC), Technical Committee (TC) 57, Working Group 14 (WG14) is developing a series of standards (IEC 61968 / 61970) that facilitate application-to-application (A2A) and business-to-business (B2B) integration for electric utilities. These standards facilitate information exchange among systems supporting business functions for planning, constructing, maintaining, and operating the electric transmission and distribution (T&D) network. Standards play an important role in establishing markets; they reduce risk for suppliers and consumers of business automation solutions. These solutions are vendor neutral and allow business processes to be configurable and scaleable.

Organizing the data among applications has always been a convoluted matter for utilities. Overlapping information requirements among functional organizations results in prolonged implementation schedules and higher maintenance costs due to the complexities in building and maintaining point-to-point interfaces. This developing series of IEC standards provides a major integration component that is already being used by several utilities in concert with Extensible Markup Language (XML) and Enterprise Application Integration (EAI) technologies. The goal of an EAI solution is to semantically integrate business processes, addressing critical integration requirements such as communication and data integration, real-time analysis, and business process automation. XML is human and machine-readable and enjoys large and growing support by suppliers of automation products. The IEC standards provide the "common language" among applications, which is based on semantics defined in the Common Information Model (CIM) that is being jointly standardized by IEC TC 57 WG13 (Energy Management System) and WG14.

An overview of the recommend standards for enterprise integration is depicted in the following diagram. These IEC standards focus on information exchange among systems for the engineering and operation of T&D networks. To facilitate seamless integration between these systems and those supporting Enterprise Resource Planning (ERP) and Supply Chain Management, WG14 is collaborating with the Open Applications Group (OAG). WG14 is also collaborating with NRECA's MultiSpeak Initiative.


(NO) Network Operation
(AM) Records & Asset Management
(OP) Operational Planning & Optimization
(MC) Maintenance & Construction
(ACT) Customer Account Management
(RET) Retail
(SC) Supply Chain and Logistics
IEC 61968-3 and IEC 61970
IEC 61968-4
IEC 61968-5 and IEC 61970
IEC 61968-6
IEC 61968-10 and OAG
IEC 61968-10 OAG
IEC 61968-10 and OAG
IEC TC57 Standards Emphasis
IEC TC57 and OAG Standards Emphasis
IEC 61968-7
IEC 61968-8
IEC 61968-9
IEC 61968-10 and IEC 61970
IEC 61968-10 and OAG
IEC 61968-10 and OAG
IEC 61968-10 and OAG
(NE) Network Extension Planning
(CS) Customer Support
(MR) Meter Reading & Control
(EMS) Energy Management & Energy Trading
(FIN) Financial
(PRM) Premises
(HR) Human Resources
Utility Electric Network Planning, Constructing, Maintaining, and Operating
Enterprise Resource Planning, Supply Chain, and General Corporate Services

CIS Customer Information System

CPUC California Public Utilities Commission

Regulates privately owned telecommunications, electric, natural gas, water, railroad, rail transit, and passenger transportation companies. The CPUC is responsible for assuring California utility customers have safe, reliable utility service at reasonable rates, protecting utility customers from fraud, and promoting the health of California's economy.

CRM Customer Relationship Management

CRM is an integrated approach to identifying, acquiring, and retaining customers. By enabling organizations to manage and coordinate customer interactions across multiple channels, departments, lines of business, and geographies, CRM helps organizations maximize the value of every customer interaction and drive superior corporate performance.

DOE Department of Energy

The United States Department of Energy has an overarching mission to advance the national, economic and energy security of the United States; to promote scientific and technological innovation in support of that mission; and to ensure the environmental cleanup of the national nuclear weapons complex.

DER Distributed Energy Resource

DG Distributed Generation

DR Demand Response

DRI Demand Response Infrastructure

ebXML Electronic Business using eXtensible Markup Language

ebXML is a joint initiative of the United Nations (UN/CEFACT) and OASIS, developed with global participation for global usage. It is a set of specifications that together enable a modular electronic business framework. The vision of ebXML is to enable a global electronic marketplace where enterprises of any size and in any geographical location can meet and conduct business with each other through the exchange of XML based messages.

E2I Energy Innovation Institute

E2I, the Electricity Innovation Institute, is a non-profit corporation established to build public and private R&D partnerships to assure the availability of clean, efficient, and affordable electricity for the 21st Century. E2I, an affiliate of EPRI, conducts strategic research in the areas of electricity supply, delivery, and utilization technologies. EPRI established E2I three years ago as a separate non-profit corporation with its own board of directors, advisory structure, and staff. As an affiliate of EPRI, E2I has full access to the technical capabilities of EPRI. http://www.e2i.org/e2i/about/faq.html

EMCS Energy Management and Control System

EPRI Electric Power Research Institute

EPRI, the Electric Power Research Institute, was founded in 1973 as a non-profit energy research consortium for the benefit of utility members, their customers, and society. Our mission is to provide science and technology-based solutions of indispensable value to our global energy customers by managing a far-reaching program of scientific research, technology development, and product implementation. To learn more, read our Company History or Introduction to EPRI. http://www.epri.com/

FTP File Transfer Protocol

GID Generic Interface Definition

GIS Geographical Information System

HTML Hypertext Markup Language

The authoring language used in the creation of documents for the World Wide Web. HTML was initially created for use as a universal common document language for the World Wide Web. It indicates the type of information rather than the exact way it is to be presented. The actual presentation is left to the software that converts the contents to a suitable format for viewing. Text in an HTML document can be translated on-the-fly by a machine translator whereas text embedded in images and graphics must be localized.

HTTPS HyperText Transport Protocol (Secure)
The standard encrypted communication mechanism on the World Wide Web. This is actually just HTTP over SSL. See: SSL/TLS Encryption

ICCP Inter Control Center Protocol

An application layer protocol specifically tailored to the needs of electric utilities for exchange of data between control centers. Technically speaking, it is a Companion Standard to MMS that is under standardization by IEC (International Electrotechnical Committee).

IEC International Electrotechnical Commission

The International Electrotechnical Commission (IEC) is the leading global organization that prepares and publishes international standards for all electrical, electronic and related technologies. These serve as a basis for national standardization and as references when drafting international tenders and contracts. Through its members, the IEC promotes international cooperation on all questions of electrotechnical standardization and related matters, such as the assessment of conformity to standards, in the fields of electricity, electronics and related technologies. The IEC charter embraces all electrotechnologies including electronics, magnetics and electromagnetics, electroacoustics, multimedia, telecommunication, and energy production and distribution, as well as associated general disciplines such as terminology and symbols, electromagnetic compatibility, measurement and performance, dependability, design and development, safety and the environment.

IECSA Integrated Energy Communications System Architecture

The Integrated Energy and Communications Systems Architecture (IECSA), is a roadmap to a next generation power system consisting of automated transmission and distribution systems that support efficient and reliable supply and delivery of power. The goal is to create a "self healing" power system capable of handling emergency and disaster situations while able to accommodate current and future utility business environments, market requirements, and customer needs. IECSA is an open, standards-based set of blueprints for integrating power and communications systems to improve the reliability, quality, and security of our electricity.

INFOSEC Information Security

ISO International Organization of Standards

ISO is a network of the national standards institutes of 148 countries, on the basis of one member per country, with a Central Secretariat in Geneva, Switzerland, that coordinates the system. ISO (International Organization for Standardization) is the world's largest developer of standards. Although ISO's principal activity is the development of technical standards, ISO standards also have important economic and social repercussions. ISO standards make a positive difference, not just to engineers and manufacturers for whom they solve basic problems in production and distribution, but to society as a whole.

LADWP Los Angeles Department of Water and Power

LBL
LBNL Lawrence Berkeley National Laboratory

Lawrence Berkeley National Laboratory (Berkeley Lab) has been a leader in science and engineering research for more than 70 years. Berkeley Lab is a U.S. Department of Energy (DOE) National Laboratory managed by the University of California. It has an annual budget of nearly $480 million (FY2002) and employs a staff of about 4,300, including more than a thousand students. Berkeley Lab conducts unclassified research across a wide range of scientific disciplines with key efforts in fundamental studies of the universe; quantitative biology; nanoscience; new energy systems and environmental solutions; and the use of integrated computing as a tool for discovery. It is organized into 17 scientific divisions and hosts four DOE national user facilities.

LSE Load Serving Entity

MAC Message Authentication Code

A code that can be used to verify the integrity of information that is transmitted over or stored in an unreliable medium.

MDMA Meter Data Management Agent

In a deregulated energy market, an MDMA is an entity that is certified to collect and distribute metering information on behalf of utilities, energy service providers or end customers.

MMS Manufacturers Messaging Specification

MMS is an international standard for real-time client/server communications per the ISO 9506 standard. Used in power system automation, industrial control, and material handling for postal automation.

MSP Meter Service Provider

In a deregulated energy market, an MSP is an entity that is certified to purchase, install and maintain meters.

PC Personal Computer

PG&E Pacific Gas and Electric

PIER Public Interest Energy Research

The PIER Program supports public interest energy research, development and demonstration (RD&D) that will help improve the quality of life in California by bringing environmentally safe, affordable and reliable energy services and products to the marketplace.

PIM Platform Independent Model

PIIM Platform Independent Information Model

POS Point of Sale

RTO Regional Transmission Operator

Independent entities, established by FERC Order 2000 issued in December 1999, that will control and operate regional electric transmission grids free of any discriminatory practices.

RBAC Role Based Access Control

Form of identity-based access control where the system entities that are identified and controlled are functional positions in an organization or process.

RCP Remote Copy Program

RFC Request for Comment

In the Internet community, Request For Comments are the working notes of the Internet research and development community. These documents contain protocol and model descriptions, experimental results, and reviews. All Internet standard protocols are written up as RFCs.

RTP Real Time Pricing

SCE Southern California Edison

SCP Secure Copy

A program to copy files between hosts on a network. It uses SSH for authentication and data transfer, thus gaining the features of strong authentication and secure encrypted communications. Replacement for FTP and RCP.

SDG&E San Diego Gas and Electric

SMI Security Management Infrastructures

SNMP Simple Network Management Protocol

An internet standard defined in RFC 1157 that is used by equipment and software that monitors and controls network devices, and manages configurations, statistics collection, performance and security.

SOAP Simple Object Access Protocol

SOAP is a lightweight protocol for exchange of information in a decentralized, distributed environment. It is an XML based protocol that consists of three parts: an envelope that defines a framework for describing what is in a message and how to process it, a set of encoding rules for expressing instances of application-defined data types, and a convention for representing remote procedure calls and responses.

SSH Secure Shell

SSH (or Secure SHell) is a protocol for creating a secure connection between two systems using a client server architecture. SSH provides mutual authentication, data encryption and data integrity.

SSL Secure Sockets Layer

A protocol originally designed by Netscape Communications to enable encrypted, authenticated communications across the Internet. SSL used mostly in communications between web browsers and web servers. URL's that begin with 'https' indicate that an SSL connection will be used. SSL provides 3 important things: Privacy, Authentication and Message Integrity.

TC Technical Committee

In this report, usually refers to a technical committee within the IEC. A TC is a high level organizational unit under which working groups (WG) are formed that perform the technical work related to international standards development.

TC 57 Technical Committee Number 57

The IEC TC responsible for the development of standards for power systems management and associated information exchange.

TOU Time of Use

TLS Transport Layer Security

TLS is the latest version of SSL. It is an enhancement of SSL version 3.0, and is a proposed Internet Standard (see RFC2246).

W3C World Wide Web Consortium

An international consortium of companies involved with the Internet and the Web. The W3C was founded in 1994 by Tim Berners-Lee, the original architect of the World Wide Web. The organization's purpose is to develop open standards so that the Web evolves in a single direction rather than being splintered among competing factions. The W3C is the chief standards body for HTTP and HTML.

WAN Wide Area Network

WG Working Group

In this report, WG usually refers to a working group under a technical committee (TC) within the IEC. A working group is where the technical work related to international standards development is actually performed.

WG 15 Working Group 15

The IEC TC 57 working group responsible for developing standards and best practices related to power system telecommunications security.

XIWT Cross-Industry Working Team

A multi-industry coalition committed to defining the architecture and key technical requirements for a powerful and sustainable National Information Infrastructure (NII) – an initiative of the Clinton/Gore administration.

XML Extensible Markup Language

Extensible Markup Language is a subset of ISO 8879, Standard Generalized Markup Language (SGML). XML has been designed specifically to function on the Web, and both major browsers support it. Currently a formal recommendation from the World Wide Web Consortium (W3C), XML is similar to HTML in that both XML and HTML contain markup symbols to describe the contents of a page or file. HTML, however, describes the content of a Web page only in terms of how it is to be displayed. XML describes the content in terms of what the data is that is being described. For example the <authname><affil> tags could indicate that the data followin g it was an author's name and his affiliation. This allows an XML file to be processed purely as data by a program as well as being displayed in a certain way. XML is "extensible" because, unlike HTML, the markup symbols are unlimited and self-defining.

Annex A IECSA Security Model

This section contains a brief synopsis of the IECSA Security Model. For a more complete description, the reader is referred to Appendix A of the IECSA Final report [R10].

What are security domains and their properties?

There are many potential methods through which to model security. Several involve concrete analysis of particular systems and communication technologies/topologies. It is often difficult to discuss security models in concrete terms since the technology used in deployments typically become limited to the lowest common denominator that is discussed. Such technology based security models tend to be difficult to scale and understand from an enterprise system perspective. Likewise, such concrete models are difficult to extend/scale to address systemic security.

> "The concept of a security domain that is introduced in this paper is not new. Many computer security practitioners have been (either explicitly or implicitly) using the ideas presented here for many years in protecting networks."

Security Domain Definition:

> "A Telecommunications and Network Security domain encompasses the structures, transmission, methods, transport formats and security measures used to provide integrity, availability, authentication, and confidentiality for transmission over private and public communications networks and media."

Additionally:

> "In this report, the term Security Domain is used to describe a network of computer systems that share a specified security level through a common element."

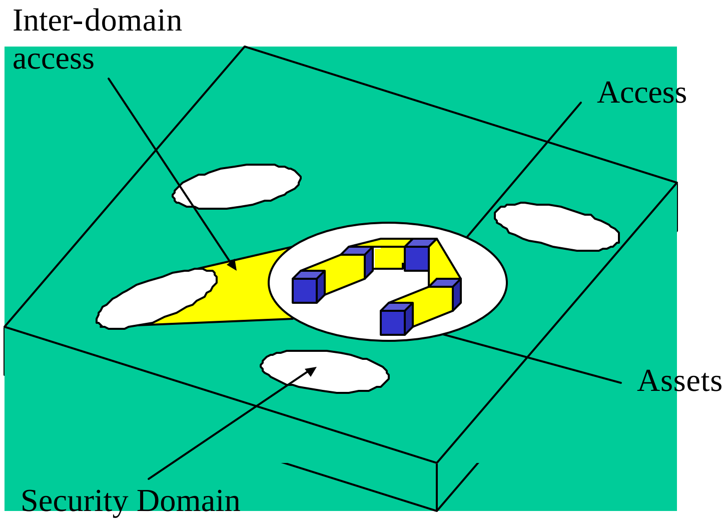


Figure A.1: Representation of Security Domain Concept

A Security Domain (SD) represents a set of resources that is governed/secured and managed through a consistent set of security policies. Additionally, Security Domains provide a well-known set of security services that are used to secure transactions and information within that domain. This notion of Security Domains correlates well to the IECSA concept of distributed computing environments.

General Requirements for security management

Security Management is defined as: "In network management, the set of functions (a) that protects telecommunications networks and systems from unauthorized access by persons, acts, or influences and (b) that includes many sub-functions, such as creating, deleting, and controlling security services and mechanisms; distributing security-relevant information; reporting security-relevant events; controlling the distribution of cryptographic keying material; and authorizing subscriber access, rights, and privileges."[9] Based upon this definition, it is the Security Management of an SD that is responsible for the risk assessment, developing security strategies, and implementing those strategies. A successful SD will define and implement the following security functions:

- Access Control: "The prevention of unauthorized use of a resource, including the prevention of use of a resource in an unauthorized manner."

  There are generally three (3) categories of Access Control that need to be addressed within a SD: Physical; Resource; and Information.

- Trust: "In cryptology and cryptosystems, that characteristic allowing one entity to assume that a second entity will behave exactly as the first entity expects. *Note:* Trust may apply only for some specific function. The critical role of trust in the authentication framework is to describe the relationship between an authenticating entity and a certification authority; an authenticating entity must be certain that it can trust the certification authority to create only valid and reliable certificates. [After X.509]"

Trust is established via Authentication. However, there are two methods of authentication that are prevalent in today's electronic systems: Role Based Authentication and Individual Authentication.

- Confidentiality: "The property that information is not made available of disclosed to unauthorized individuals, entities, or process."

  There are typically two (2) categories of Confidentiality that need to be addressed within a SD: Protection from un-intentional disclosure and overall protection of information.

- Integrity: "The principle that keeps information from being modified or otherwise corrupted either maliciously or accidentally."

- Security Policy: "The set of rules and practices that regulate how an organization manages, protects, and distributes sensitive equipment and information."

  It is the security policy function that determines how to manage residual risk. The policy function then expects the Security Management Infrastructure to allow the actual management of such risk.

- Security Management Infrastructure (SMI): "(I) System elements and activities that support security policy by monitoring and controlling security services and mechanisms distributing security information and reporting security events."

The use of the Security Domain concept allows discussions in regards to how to allow physical access into a domain (e.g. physical access control) and which security services are needed in order to provide a robust physical access control function. Examples of such security services would be: the ability to identify the person attempting access; the ability to make sure that the person is authorized to enter a particular security domain; the ability to log the fact that the person entered/exited the domain; and the need to have established security policies that encompass/manage the other security services set forth.

Whereas, physical access is typically well understood, other security functions are typically discussed/understood at a high-level and therefore do not capture all of the functional/service requirements. The security domain concept allows a more detailed discussion at a high-level. In the case of Trust, it is well understood that in order to establish trust one must determine the identity of the person/entity to which information/resources are being provided. In the case of individuals that you know and are face-to-face with, identity establishment is quite easy.

Therefore, if a person you know requests a piece of information, it is relatively easy to determine if that person should be granted access to that information due to a well established identity. However, is the same true if the same person approaches you for the same information but is executing the request on behalf of a third party (e.g. an Inter-Domain request that is acted upon intra-domain)? Maybe. What if the request for information is nested even further? At some point, although the identity of the immediate requestor is well-known, there may arise an issue of trust in the actual request due to the number of times that the original requestor's identity has been changed (e.g. as it crosses into different security domains). The need to provide a security service that could allow the determination of a metric of how many identity mappings have occurred could prove useful, although not needed in every instance.

Confidentiality is typically thought of as a well-understood security function. When one typically thinks of confidentiality, the first thought is the word "encryption". Encryption is a security service that needs to be provided. However, confidentiality could also be provided/enhanced if the sender of the request/information could specify a path through which to route the information/request.

Analysis based upon the security domain concept indicates that there are several security services that any particular security domain will need to have available. Some functions are not requirements for intra-domain security but are mandatory for inter-domain (e.g. identity and credential mapping) security. These services and their inter-dependencies are described in Section 2 of this document. The development of high-level security service definitions and functional requirements allows for issues of resource type (e.g. physical or informational) to be deferred until technological implementation strategies are evaluated. Thus it becomes possible to discuss the issue of access control for buildings and Simple Network Management Protocol (SNMP) information/services in a common manner. Based upon the understanding of the functions that these services need to provide, technologies (or combination of technologies) can be evaluated as mechanisms of actually implementing such security functions. It is during these evaluations that the distinction of physical or informational resources would be required.

The IECSA architecture attempts to define an architecture that creates an environment for heterogeneous energy industry applications and business functions within that environment. IECSA has defined several enabling architectures and technologies in this regard. However, security and security domains are inherently non-heterogeneous (especially at a technological solution level). It is this dichotomy that is part of the reason that many individuals, when attempting real business functions, perceive security as an impediment to the accomplishment of the primary business function. Thus, there needs to be a balance of providing adequate security versus protecting the primary business functions from security threats. Thus the security services developed in Section 2 are classified as mandatory/optional in order to provide a security function. However, it is the security policy of a specific Security Domain that determines which services must be used. Additionally, it is a specific SD that determines what type of technological solution(s) will be used in order to accomplish a give security function. The technological solutions chosen will typically create interface issues between security domains.

A good example of this is the Trust Function. If SD1 makes use of a username/password based technology to establish trust (e.g. Identity Establishment security service) and SD2 makes use of digital certificates, how should a individual in SD1 establish an identity or role within SD2? The obvious answer is that there needs to be a process to convert from the username/password, managed in SD1, to digital certificate required for SD2. The proposed IECSA security service to provide this capability is named the Credential Conversion security service. Once the service needed is recognized, the next question becomes whose responsibility is it to provide the particular conversion. In our example, it would be SD1 and not SD2 (not quite intuitively obvious).

The abstraction of security functions and services, to some, may not seem to be needed. However, in order to future proof (e.g. to allow applications to migrate to better technologies as they become available), applications will not be able to invoke security technologies directly. Just the knowledge of what services need to be used (if implemented) could have prevented several of the Internet Viruses that attack Outlook, Outlook Express, and IE. These are examples of applications that were designed to accomplish a business function without regards for protecting critical information (in many of the virus cases I would also suggest adding a paragraph about managing residual risk with intrusion detection and audit trails. the contact list) nor do they provide an audit capability to determine when and if the list has been modified/accessed.

The security information contained with IECSA is hoped to provide an infrastructure that allows applications to be created that can make use of various security technologies as required by the security policies of each SD. Additionally, it is hoped that by identifying abstract service requirements that all future applications created for the IECSA environment will make use of such services.

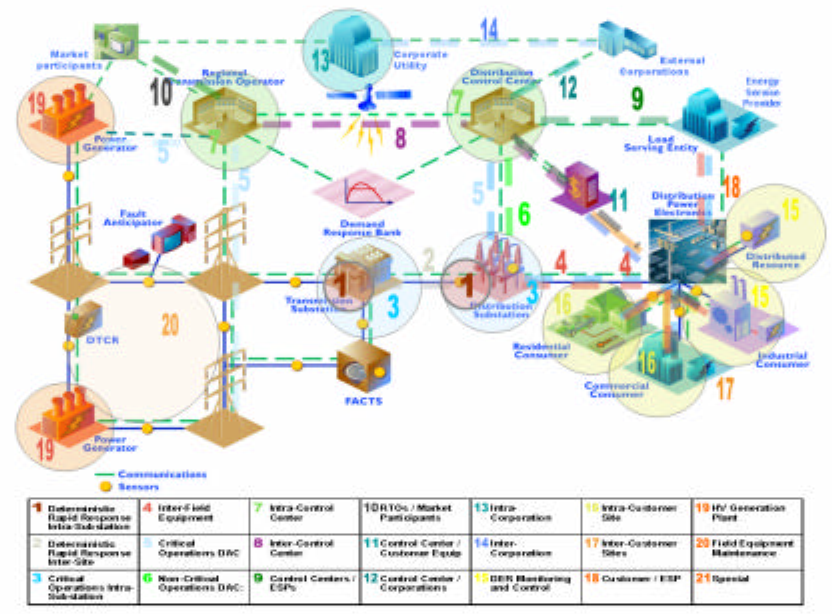
Annex B IECSA Environments

As the key power system functions were analyzed in depth, it became quite clear that one set of recommendations would not fit all situations, even if the basic requirements were similar. One possible solution could have been to develop unique recommendations for each of the functions that were analyzed, but this clearly would not solve the larger issues nor provide an overarching Architecture for the energy industry. Therefore, these and a number of other power system functions were assessed for where information requirements were similar across a number of functions. These situations with similar information requirements were then called IECSA Environments.

An IECSA Environment is defined as an information environment, where the information exchanges of power system functions have essentially similar architectural requirements, including their configuration requirements, quality of service requirements, security requirements, and data management requirements.

IECSA Environments reflect the requirements of the information exchanges, not necessarily the location of the applications or databases (although these may affect the information exchanges and therefore the environment). Since functions can have multiple types of information exchanges, as represented by the steps in the functional descriptions, these functions can be operating across multiple IECSA Environments.

After further analysis of the 400 functions, twenty (20) IECSA Environments were identified. These are shown graphically in Figure B.1 and described in greater detail in Figure B.2



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

Figure B.1: IECSA Environments in Power System Operations

Figure B.2: Descriptions of each IECSA environment.

Environment	Description
1. Deterministic Rapid Response	Deterministic, rapid response intra-substation environment (e.g. protective relaying, direct monitoring of power system parameters by current
2. Deterministic Rapid Response	Deterministic, rapid response inter-substations and beyond substation (e.g. protective relaying, FSM)
3. Critical Operations -	High security intra-substation environment (e.g. monitoring and control of IEDs, setting protective relay and other substation equipment parameters, etc)
4. Inter-Field Equipment	Between equipment in the field that does not require deterministic rapid response (e.g. local interactions between automated switches, equipment monitoring by local data concentrators)
5. Critical Operations - Related DAC	High security interactions (i.e. authentication, confidentiality, protection against denial of service, etc.) between control center and field equipment environment (e.g. monitoring and control by SCADA of substation and DA equipment, monitoring and control of DER devices, monitoring of security-sensitive customer meters, monitoring and control of generation units)
6. Non-Critical Operations - Related DAC	Lower security interactions (i.e. only authentication is possibly required, not confidentiality) between control center and field equipment, including distribution automation equipment, substation equipment, DER equipment, customer sites (e.g. monitoring non-power system equipment, less security-sensitive substations, customer site PQ monitoring, customer metering)
7. Intra-Control Center	Within one control center (e.g. SCADA system, EMS system, ADA functions, real-time operations)
8. Inter-Control Center	Among control centers (e.g. between utility control centers, between RTOs, between remote subsidiary or supervisory centers)
9. Control Centers to ESPs	Between utility control centers and ESPs/Aggregators (e.g. RTP, metering and settlements, market operations)
10. RTOs to Market Participants	Between utility/RTO/ISO control centers and Market Participants (e.g. market operations)
11. Control Center to Customer Equipment	Between customer equipment and utility control centers (e.g. customer metering, demand response interactions, DER management)
12. Control Center to Corporations	Between control centers and external corporations (e.g. weather data, regulators, auditors, vendors)
13. Intra-Corporation	Within corporate utility (e.g. planning, engineering, ADA access to AM/FM and customer information systems, arena addressed by TC57 WG14)
14. Inter-Corporation	Between corporate utility and external corporations (e.g. e-business)
15. DER Monitoring and Control	Between DER and ESP/DER Operator (e.g. ESP as Aggregator performing monitoring and control)
16. Intra-Customer Site	Within a customer site (e.g. building management systems, DER management)
17. Inter-Customer Sites	Between customer sites (e.g. microgrid management)
18. Customer to ESP	Between customers and ESPs, Aggregators, MDMAs (e.g. DER management, customer metering, RTP, demand response)
19. HV Generation	Within an HV Generation Plant site (e.g. within the electrical and physical

Figure B.2: Descriptions of each IECSA environment.

Environment	Description
Plant	site of the generating plant up to the point of common coupling with the area power system)
20. Field Equipment Maintenance	Maintenance monitoring, statistics gathering, testing, diagnostics, asset management (e.g. may require mobile interactions, significantly different types of data, different security role-based-access, asset identification management, etc.)

Key Requirements Used to Define the IECSA Environments

Key distributed computing infrastructure requirements were extracted from the power system functions and used to categorize the IECSA Environments. These requirements, which eventually became termed the 'aggregated requirements,' comprise the following:

Communication Configuration Requirements

- Provide point-to-point interactions between two entities
- Support interactions between a few 'clients' and many 'servers'
- Support interactions between a few 'servers' and many 'clients'
- Support peer to peer interactions
- Support interactions within a contained environment (e.g. substation or control center)
- Support interactions across widely distributed sites
- Support multi-cast or broadcast capabilities
- Support the frequent change of configuration and/or location of end devices or sites
- Support mandatory mobile communications
- Support compute-constrained and/or media constrained communications

Quality of Service Requirements

- Provide ultra high speed messaging (short latency) of less than 4 milliseconds
- Provide very high speed messaging of less than 10 milliseconds
- Provide high speed messaging of less than 1 second
- Provide medium speed messaging on the order of 10 seconds
- Support contractual timeliness (data must be available at a specific time or within a specific window of time)
- Support ultra high availability of information flows of 99.9999+ (~1/2 second)
- Support extremely high availability of information flows of 99.999+ (~5 minutes)
- Support very high availability of information flows of 99.99+ (~1 hour)
- Support high availability of information flows of 99.9+ (~9 hours)
- Support medium availability of information flows of 99.0+ (~3.5 days)
- Support high precision of data (< 0.5 variance)
- Support time synchronization of data for age and time-skew information
- Support high frequency of data exchanges

Security Requirements

- Provide Identity Establishment (you are who you say you are)
- Provide Authorization for Access Control (resolving a policy-based access control decision to ensure authorized entities have appropriate access rights and authorized access is not denied)
- Provide Information Integrity (data has not been subject to unauthorized changes or these unauthorized changes are detected)
- Provide Confidentiality (only authorized access to information, protection against eavesdropping)
- Provide Security Against Denial-of-Service (unimpeded access to data to avoid denial of service)
- Provide Inter-Domain Security (support security requirements across organizational boundaries)
- Provide Non-repudiation (cannot deny that interaction took place)
- Provide Security Assurance (determine the level of security provided by another environment)
- Provide for Audit (responsible for producing records, which track security relevant events)
- Provide Identity Mapping (capability of transforming an identity which exists in one identity domain into an identity within another identity domain)
- Provide Credential Conversion (provides credential conversion between one type of credential to another type or form of credential)
- Provide Credential Renewal (notify users prior to expiration of their credentials)
- Provide a Security Policy (concerned with the management of security policies)
- Provide for Policy Exchange (allow service requestors and providers to exchange dynamically security (among other) policy information to establish a negotiated security context between them)
- Provide Single Sign-On (relieve an entity having successfully completed the act of authentication once from the need to participate in re-authentications upon subsequent accesses to managed resources for some reasonable period of time)
- Provide Trust Establishment Security (security verification across multiple organizations)
- Provide Path and Routing Quality of Security (being able to determine a secure communication path)
- Provide Firewall Transversal
- Provide Privacy Service (the ability to ensure person information is not disclosed)
- Provide User Profile and User Management (combination of several other security services)
- Provide Security Protocol mapping (the ability to convert from one protocol to another)
- Provide Quality of Identity (the ability to determine the merit of converted credentials)
- Provide Security Discovery (the ability to determine what security services are available for use)
- Provide Delegation (delegation of access rights from requestors to services, as well as to allow for delegation policies to be specified)

Data Management Requirements

- Provide Network Management (management of media, transport, and communication nodes)
- Provide System Management (management of end devices and applications)
- Support the management of large volumes of data flows
- Support keeping the data up-to-date
- Support extensive data validation procedures
- Support keeping data consistent and synchronized across systems and/or databases
- Support timely access to data by multiple different users
- Support frequent changes in types of data exchanged
- Support management of data whose types can vary significantly in different implementations

- Support specific standardized or de facto object models of data
- Support the exchange of unstructured or special-format data (e.g. text, documents, and oscillographic data)
- Support transaction integrity (consistency and rollback capability)
- Provide for service discovery (discovering available services and their characteristics)
- Provide for spontaneously finding and joining a community
- Provide protocol conversion and mapping
- Support the management of data across organizational boundaries

Annex C CableHome Architecture and Reference Design

The following are lessons learned during the cable industries path to standardization and establishment of a reference architecture and design.

- Proprietary hardware and software solutions that extend between the back-office infrastructure and customer premise equipment always results in vendor lock-in
  - The Cable Industry's DOCSIS initiative has delivered standards-based broadband cable networking products & systems, resulting in heterogeneous data networks
  - Motorola and Scientific Atlanta still have an industry duopoly hold on analog & digital set-top boxes and their head-end devices & systems (OpenCable should change this in 2007)
- Cable networking standards need to be driven by cable operators, not the vendor community – reason for CableLabs (www.cablelabs.com)
- Standards are critical for allowing customers access to best-of-breed products and technologies at ever lowering price points, and prohibit vendor lock-in
- Vendor compliance testing & certification is critical to enabling retail market for customer in-premise cable networking products

Figure D.1 shows the timeline of this evolution and how it has impacted the prices of cable modem hardware.

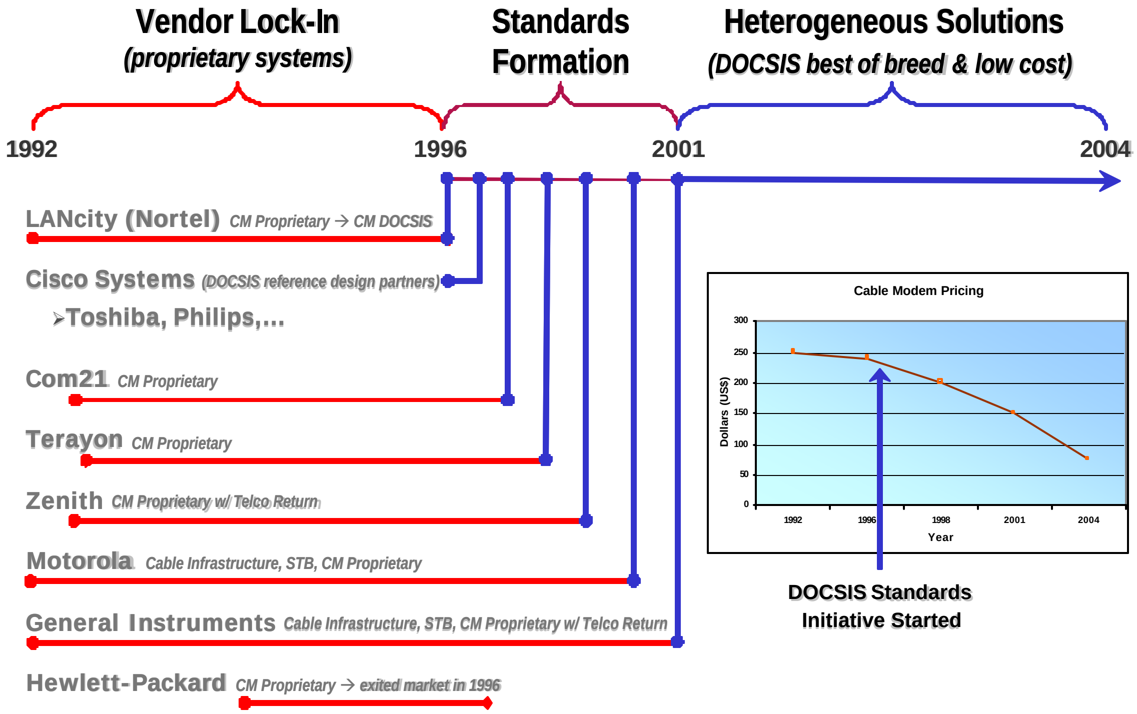

Vendor Lock-In
(proprietary systems)
Standards Formation
Heterogeneous Solutions
(DOCSIS best of breed & low cost)
1992
1996
2001
2004
LANcity (Nortel) CM Proprietary → CM DOCSIS
Cisco Systems (DOCSIS reference design partners)
➢Toshiba, Philips,...
Com21 CM Proprietary
Terayon CM Proprietary
Zenith CM Proprietary w/ Telco Return
Motorola Cable Infrastructure, STB, CM Proprietary
General Instruments Cable Infrastructure, STB, CM Proprietary w/ Telco Return
Hewlett-Packard CM Proprietary → exited market in 1996
Cable Modem Pricing
300
250
200
150
100
50
0
Dollars (US$)
1992
1996
1998
2001
2004
Year
DOCSIS Standards
Initiative Started

Figure C.1 – Cable Modem Standardization Timeline

The following standards initiatives were responsible for realizing true interoperability among cable modems and related systems and services:

Cable Modem/DOCSIS®

Defines interface requirements for cable modems involved in high-speed data distribution over cable television system networks.

OpenCable™

Defines and enables deployment of "plug-and-play" retail television receivers and other equipment compatible with advanced digital cable applications and services.

CableHome™

Developing the interface specifications necessary to extend high-quality cable-based services to network devices within the home.

Go2BroadbandSM

Creates an Internet-based electronic commerce tool to assist in selling cable services.

PacketCable™

An initiative aimed at developing interoperable interface specifications for delivering real-time multimedia services over two-way cable plant.

VOD Metadata

Investigating the distribution of content assets from multiple content providers sent over diverse networks to cable operators.

By adopting and enforcing standards, Cable has dramatically broadened its offerings, lowered costs and empowered the consumer with products & services. The following figures show the CableHome architecture and reference designs

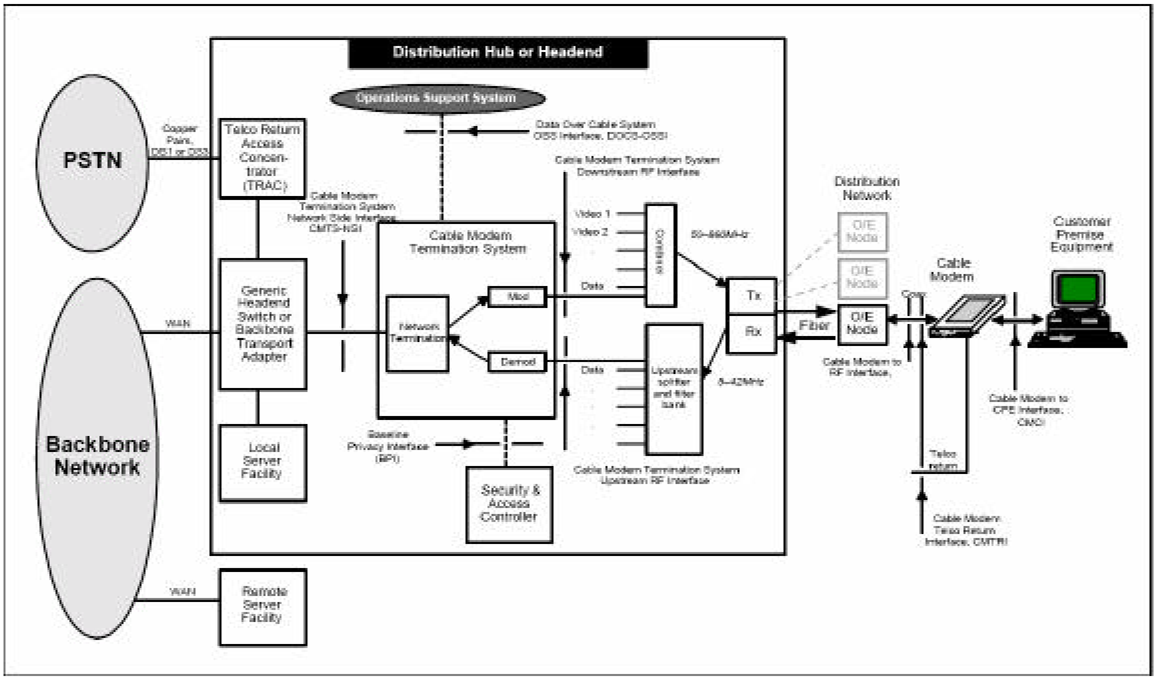

Distribution Hub or Headend
Operations Support System
PSTN
Copper Pairs, DS1 or DS3
Telco Return Access Concen-trator (TRAC)
Data Over Cable System OSS Interface, DOCS-OSSI
Cable Modem Termination System Downstream RF Interface
Cable Modem Termination System Network Side Interface CMTS-NSI
Cable Modem Termination System
Video 1
Video 2
Data
Combiner
50-860MHz
Mod
Network Termination
Demod
Data
Upstream splitter and filter bank
5-42MHz
Tx
Rx
Fiber
Distribution Network
O/E Node
O/E Node
O/E Node
Coax
Cable Modem
Customer Premise Equipment
Cable Modem to RF Interface,
Cable Modem to CPE Interface, CMCI
Telco return
Cable Modem Telco Return Interface, CMTRI
Backbone Network
WAN
Generic Headend Switch or Backbone Transport Adapter
Local Server Facility
Baseline Privacy Interface (BPI)
Security & Access Controller
Cable Modem Termination System Upstream RF Interface
WAN
Remote Server Facility

Figure C.2 – DOCSIS Reference Architecture

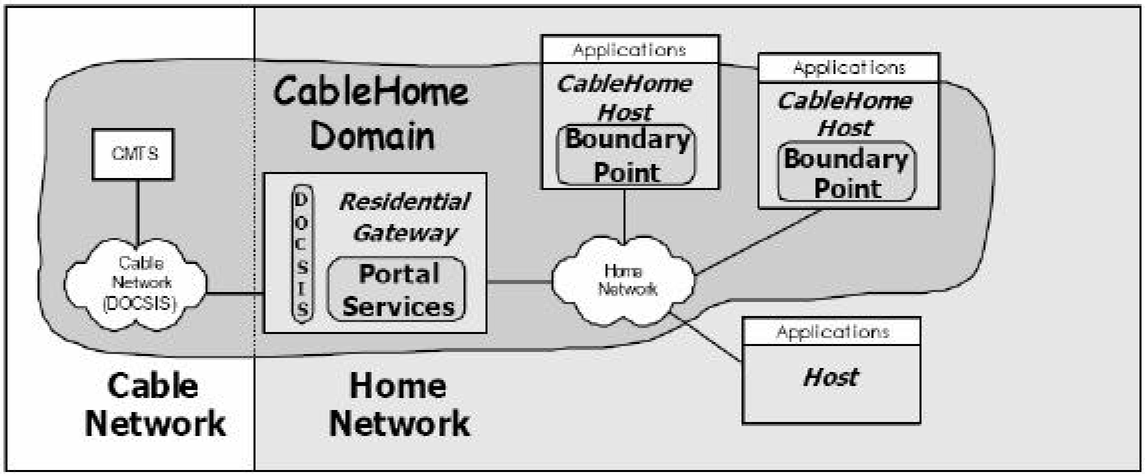


Figure C.3 – CableHome Portal Reference Architecture

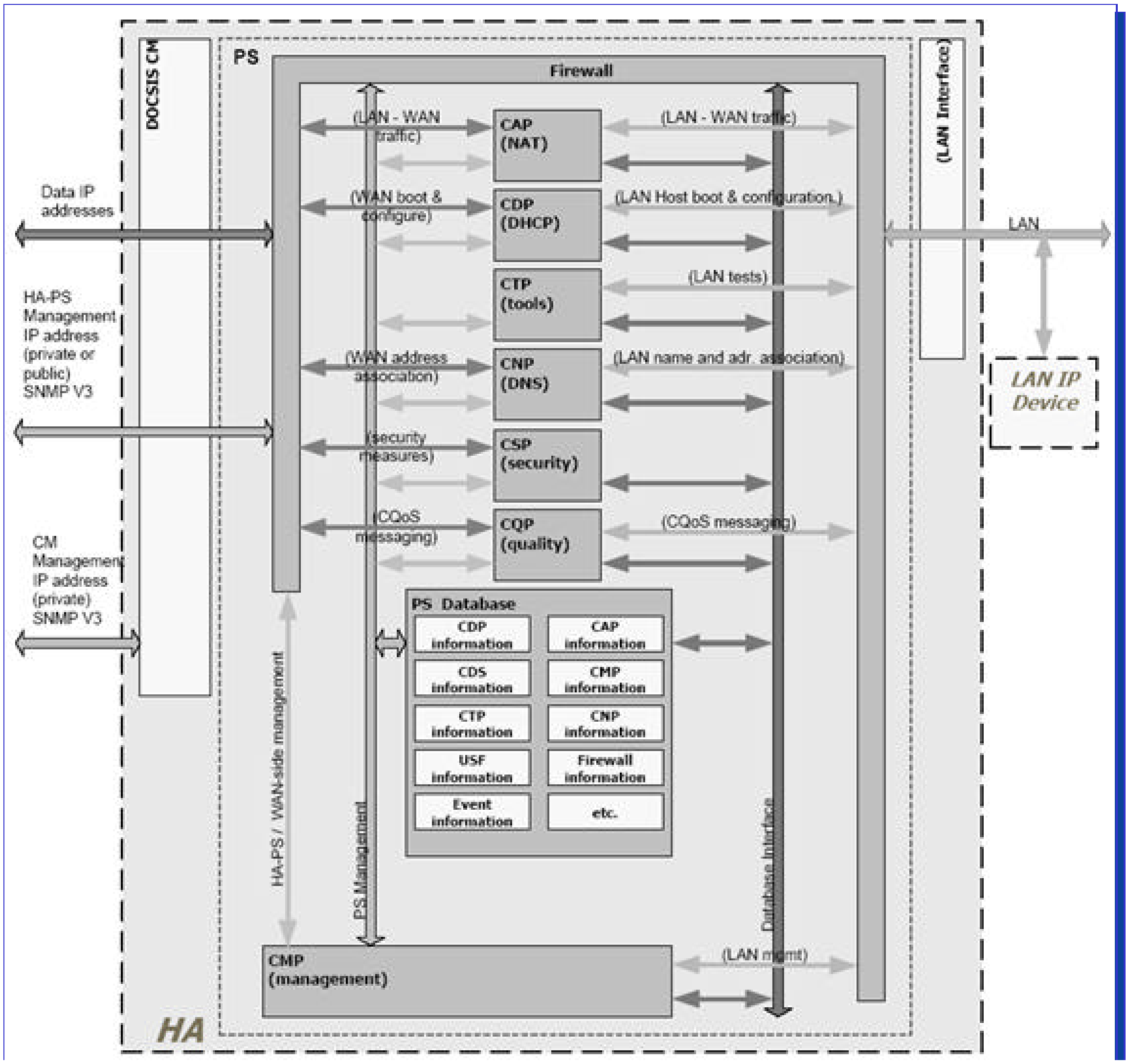


Figure C.3 – CableHome Portal Reference Design

Annex D Presentations

The following presentations were developed during the course of the project and are available from the CIEE and/or CEC:

First presentation to the technical advisory group
Meeting03172004.ppt

First presentation of concept to Art Rosenfeld and other CEC representatives
A Reference Design for Implementing Demand Response Systems 3.ppt

Business case presentation from Joe Desmond
Reference Design_Business Case.ppt

Business case presentation to the technical advisory group
Reference Design_Business Case_PIER4.ppt

Final presentation to Art Rosenfeld and other CEC representatives
ReferenceDesignPresentationrev2.3.ppt