The Integrated Energy and Communication Systems Architecture

Volume I:
User Guidelines and Recommendations

EPRI Project Manager

Joe Hughes

Cosponsor

Electricity Innovation Institute Consortium for Electric Infrastructure to Support a Digital Society (CEIDS)

EPRI • 3412 Hillview Avenue, Palo Alto, California 94304 • PO Box 10412, Palo Alto, California 94303 • USA
800.313.3774 • 650.855.2121 • askepri@epri.com • www.epri.com

DISCLAIMER OF WARRANTIES AND LIMITATION OF LIABILITIES

ORGANIZATIONS THAT PREPARED THIS DOCUMENT

General Electric Company led by GE Global Research (Prime Contractor)

Significant Contributions made by
- **EnerNex Corporation**
- **Hypertek**
- **Lucent Technologies (Partner)**
- **Systems Integration Specialists Company, Inc.**
- **Utility Consulting International (Partner)**

ORDERING INFORMATION

Requests for copies of this report should be directed to EPRI Orders and Conferences, 1355 Willow Way, Suite 278, Concord, CA 94520. Toll-free number: 800.313.3774, press 2, or internally x5379; voice: 925.609.9169; fax: 925.609.1310.

CITATIONS

This document describes research sponsored by EPRI and Electricity Innovation Institute.
The publication is a corporate document that should be cited in the literature in the following manner:
THE INTEGRATED ENERGY AND COMMUNICATION SYSTEMS ARCHITECTURE, EPRI, Palo Alto, CA and Electricity Innovation Institute, Palo Alto, CA: 2003 {Product ID Number.}

ACKNOWLEDGEMENTS

Although the IECSA project was massive in scope, the team tackling the project was unwavering in its resolve to deliver not only a useful product, but also a vision to the industry. Clearly, there were hundreds of individuals who listened to concepts and offered suggestions for IECSA. However, acknowledgment is due to the following individuals through whose sweat and labor, an architecture is born:

Project Management:
Joe Hughes – E2I – Project Manager, advisor, and project visionary
Peter Sanza – GE Global Research – Contract team project manager

Primary Contributors:
Mark Adamiak – GE Multilin – Principle Investigator and WAMAC Domain Leader
Raj Bharadwaj – GE Global Research – Architect, Domain Expert
James Bobyn – Independent Consultant – Domain Expert – Transmission Domain
Marty Burns – Hypertek – Project Advisor and architecture team member
Frances Cleveland – UCI – Architect, Domain Leader for Market Operations and ADA
Walt Dixon III – GE Global Research – Lead Architect
Herb Falk – SISCO – Architecture Team, Security Domain Leader
Grant Gilchrist – GE Network Reliability Products and Services – Architect, Domain Expert
John Gillerman – SISCO – Architect, and Technology leader
Erich Gunther – EnerNex – Architect and Consumer Domain Leader
Jack King – EnerNex Corporation – Stakeholder Engagement Team, Domain Expert – Consumer Domain
Mark Lachman – UCI – Domain Leader for Market Operations and Technology Architect
Jeff Lamoree – EnerNex – Stakeholder Engagement Team
Wing Cheong Lau – Lucent Technologies / Bell Labs – Architecture Team and Enterprise Management
Ellen Liu - GE Global Research – Domain Expert
Nokhum Markushevich – UCI – Domain Leader for Distribution Operations and Distributed Energy Resources
Louie Powell – GE PSEC – Domain Expert
William Premerlani – GE Global Research – Domain Expert – Synchro Phasor
Mike Reichard – GE PSEC – Domain Expert
Behrokh Samadi – Lucent Technologies/Bell Labs – Architecture Team and Enterprise Management
Jahshid Sharif-Askary – GE Network Reliability Products and Services – Domain Expert
Sandy Smith – EnerNex – Stakeholder Engagement Team and Domain Expert – Consumer Domain
Becca Voelker – GE Global Research – Financial Manager
Donna Withey – GE Global Research – Assisting Financial Manager
Rui Zhou – GE Global Research – Architect, Domain Expert

Special thanks go to:

- Jan Putman for her roll in educating and energizing the team to go forth and use the RM-ODP framework
- The CEIDS Project Advisory Group who listened to our work in progress and added guidance throughout the course of the project.
- The CEIDS companies and all other stakeholders (especially WE Energies, BPA, EdF, and PPGC) for their focused engagement efforts as well as their hospitality during the team's visit to their companies.
- Richard Schomberg, Don Von Dollen, and Marek Samotyj for their support during the course of the project
- The GE partners on this project (Utility Consulting International and Lucent Technologies) for their perseverance and team leadership throughout the process.

Lastly, we would like to acknowledge the staff and management at EPRI and E2I for having the vision to see the needs of the energy enterprise and for taking the steps to meet these needs.

This page is intentionally left blank.

EXECUTIVE SUMMARY

The Power Industry Meets the Digital Society

From the powering of the first commercial light bulb in 1882, the electric power industry has been on a journey of continual change and improvement. Over the course of this journey, advances in technology have led to revolutionary transformations in the way power is generated, delivered, and consumed.

Now, at the beginning of the 21st century, the electric power industry is once again on the verge of a revolutionary transformation as it endeavors to transition all aspects of the electrical enterprise to meet the needs of the 'Digital Society'. Television, radio, movies, telephony, audio, computing, books, and, of course, the Internet are all merging into an ocean of digital information. As members of this Digital Society, electricity consumers are surrounded by this ocean, where information is instantly accessible, easily searchable, rich in variety and texture, secure when needed, and (nearly) always available. The expectations brought about by the Digital Society are now driving similar changes in the power industry. Power customers are demanding higher reliability, more choice, and a constant flow of information–all at constant, or even lower, prices.

Without a unified vision, however, the issues facing the power system will be addressed individually by utilities, government agencies, and power system organizations. The net result of isolated development activities will be a power system plagued by 'islands of separation', where the power system of the future is only realized in limited areas or on a small scale. The Integrated Energy and Communications System Architecture–IECSA–overcomes this isolated development and is the first step to unite power system organizations on their journey to the future.

IECSA – The Power System Architecture of the Future

As with all journeys, having a vision of the ultimate destination is vital to find the best path to the next waypoint, avoid pitfalls, and minimize expenditures. The IECSA vision for the power system of the future is:

> *A power system made up of numerous automated transmission and distribution systems, all operating in a coordinated, efficient and reliable manner.*
>
> *A power system that handles emergency conditions with 'self-healing' actions and is responsive to energy-market and utility business-enterprise needs.*
>
> *A power system that serves millions of customers and has an intelligent communications infrastructure enabling the timely, secure and adaptable information flow needed to provide reliable and economic power to the evolving digital economy.*

To date, the paths leading to this vision have been rocky and diverse. Although portions of this vision do exist today within selected power utilities, there is a wide range of variation in the level of capability and compatibility across the overall power system. Generally, system integration and coordination are not performed on a wide enough scale to address the severity of the problems faced by the grid today, as clearly illustrated by analysis of previous blackouts.

IECSA Vision – The Information System Architecture of the Future

IECSA is intended to integrate two systems in the power industry: the *power and energy delivery system* and *the information system* (communication, networks, and intelligence equipment) that controls it. In the past, the power delivery system has been a primary focus of development efforts within the power industry. However, to effectively move the industry toward identified goals, the electric system must increasingly rely on the information system as well. These two systems must be developed in parallel and

will be comprised of advanced communications and networking technologies working with intelligent equipment and algorithms to execute increasingly sophisticated system functions.

Benefits of IECSA

The current information infrastructure of the energy industry is plagued with legacy systems, proprietary protocols, stranded applications and ad hoc interfaces. This jumble impedes the expansion and upgrading of computer systems, software applications, and new equipment. The IECSA Architecture, therefore, further identifies a recommended approach to add new applications that are readily integrated and replace the jumble of legacy interfaces with common ones; and thus provide lower cost solutions as the information infrastructure grows in extent and complexity.

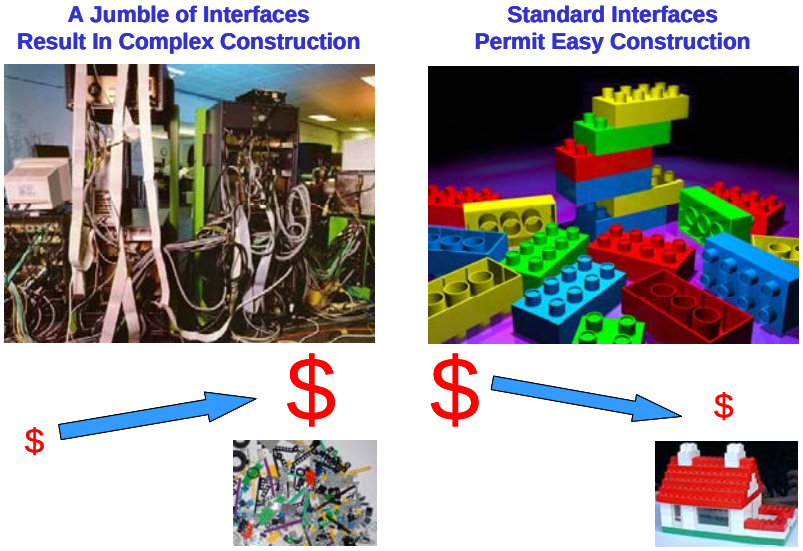

Figure 1: Benefits of Architecture

Reduced application costs from standardized 'building blocks'

The specific benefits of IECSA are:

- Enabling advanced applications that will require a ubiquitous infrastructure
- Capital savings from standardized components that can be competitively procured
- Life cycle savings from lower maintenance costs due to standardization
- Reduction in stranded assets from systems that can integrate
- Ability to incrementally build upon first steps; and then scale up massively
- Reduced development costs by building on components of IECSA systems engineering
- Robustness achieved from structured approaches to systems management
- And finally, an architecture is necessary to consistently and adequately secure the energy industry.

IECSA in Capsule

IECSA is a both plan for the integrated information infrastructure and a study of the requirements and principles required to make particular automation projects work. In basic terms, the IECSA architecture is a set of high level concepts that are used to design a technology independent architecture as well as identify and recommend standard technologies, and best practices. These high level concepts include:

- The use of object models and modeling services to give standardized names to data, and to describe their relationships, their formats, and their interactions in standardized ways
- The development of security policies and the implementation of security technologies where needed, not only to prevent security attacks and inadvertent mistakes, but also to handle recovery from the inevitable failures
- The inclusion of network and system management to monitor and control the information infrastructure in a manner similar to the monitoring and control of the power system
- The implementation of data management technologies and best practices to handle the exponential growth of data and the need to ensure data consistency across dispersed systems as more reliance is placed on automation
- The use of the tactical approach of 'technology independent components' to manage the diversity of systems and the migration from legacy systems to systems with standardized interfaces.

The energy industry encompasses many special types of information requirements, some unique to its operational needs, such as high-speed message exchange for protective relaying, and some very common to many industries, such as e-commerce. Therefore, the IECSA Architecture cannot recommend a single set of standard technologies for use everywhere in the industry, but rather it categorizes these special requirements as IECSA Environments, defining each Environment according to its common requirements, and identifying the standards that are appropriate for each of these environments.

The results of the IECSA project are contained in a series of printable documents, computer models, and web-browser navigable hypertext pages. It was early recognized that paper documents covering such a vast scope as the IECSA Architecture would be difficult to use. Therefore the key aspects of the IECSA Architecture, along with the IECSA Environments and their links to the standard technologies, were incorporated into a modeling tool.

To make these results more understandable and useful to a wider audience, information is extracted from the model and the printable documents – and presented combined in a web-navigable (hypertext) website. This website ties together key concepts contained within the model without sacrificing the rigor and standardized notation used to document the model. The results are presented in a human-friendly manner.

Recommendations to Executives for Adopting IECSA

The following recommendations are made to executives for adopting IECSA:

- Formally adopt the IECSA Architecture as the strategic vision for your information infrastructure.
- Ensure that the different users of the IECSA Architecture understand how to utilize the relevant parts of the IECSA products, including the power system functional descriptions and the IECSA high level concepts.
- Develop a plan for implementing technology independent architecture using the recommended standard technologies, based on your specific business needs and the timeframe appropriate for meeting those needs and your financial constraints.
- Develop a plan for migrating legacy systems and interfaces to the IECSA recommended standard technologies.
- Provide feedback so that the IECSA Architecture can evolve to meet future needs and to include standards that are created in the future.

PROJECT SUMMARY

Building the IECSA Architecture

In daily use, the term 'architecture' refers to the overall plan, style, and vision for a structure. It also refers to the general study of the principles of building. It is vital that any network architecture be based on the requirements for the use of the final structure, in the same way that the architecture of a building must be tailored to the needs of its inhabitants and the environment in which it is located.

Following this definition, IECSA is both a plan for the integrated power system infrastructure and a study of the requirements and principles required to make particular automation projects work. In basic terms, the IECSA architecture is a set of components and the rules to interconnect individual components. IECSA endeavors to define reusable architectural components and a common set of interfaces, or 'languages' that can be used to execute energy enterprise and industry-wide applications. To meet future use requirements, IECSA is based on the specific needs of the power industry in the same way a building's architecture is tailored to the needs of its owners.

To develop IECSA, a diverse team of industry experts was assembled with representation from utilities, vendors, consultants, researchers, and project managers. This team followed established steps of 'good system architecture design', specifically:

1. **Gathering requirements** from stakeholders across the industry.
2. **Analyzing** the requirements using modern methodologies and tools.
3. **Evaluating** the state-of-the-art in communications technology.
4. **Designing** the architecture by identifying common components and services.
5. **Capturing** the architecture design and recommendations using web technology.

Three key steps of system architecture design remain to be executed:

- **Testing** the principles of the architecture in prototypes and pilot projects.
- **Implementation** and validation of the design in real-world, large-scale systems.
- **Integration** of the lessons learned into further iterations of the process.

The Integrated Energy and Communication System Architecture – IECSA – is a first step in enabling this vision. As the title suggests, IECSA is intended to integrate two different systems: the physical energy delivery system, and the communications network of intelligent equipment that controls it.

As we look to the future of the power system, it will rely increasingly on this second infrastructure of information exchange. It must be developed in parallel to the power system infrastructure to effectively move the industry toward its identified and future goals. This second infrastructure will be comprised of advanced communications and networking technologies working with intelligent equipment and algorithms that can execute increasingly sophisticated operations functions.

As long as the two networks are dealt with separately by utilities and other power system organizations, the power industry will be plagued with 'islands of integration', in which the vision is realized only in selected areas and not on a scale large enough to ensure future visions of system operation.

1. Gathering Requirements – Past, Present and Future

When developing IECSA, it was vital that the architecture be based on a clear understanding of the needs of the power system network in five or ten years, not only based on today's requirements. If future needs are not considered, the resulting architecture would be obsolete by the time it was actually built. To this end, part of the requirements process involved interaction with more than 1,000 individuals during more than 100 engagements.

The information gathered during these engagements was captured in a 'template' format that formalized the type of information required from each stakeholder. The ideal goal would have been to capture both current and future communication system requirements from representatives in all functions and applications performed in the utility industry. This level of requirements gathering was, however, an enormous job and it was beyond the resources of the project to complete in time for the results to be useful.

Instead, the requirements gathering process did cover existing requirements lightly, but focused on the three primary growth areas that were determined by the IECSA team to most likely pose architectural challenges for the information infrastructure. These growth areas included:

- **Wide Area Measurement and Control** – in particular, those requirements for developing a self-healing, self-optimizing grid that can predict emergencies, rather than just react to them, and that automates many reliability functions currently performed manually, or not at all
- **Advanced Distribution Automation** – including the challenges raised by using Distributed Energy Resources, renewable energy sources, fault detection, fault location, sectionalization and automatic service restoration over large service territories and multiple organizational boundaries
- **Customer Interface** – including the challenges of real-time pricing, demand response, automatic metering, integrating the communications network with building automation, and the requirements for integrating real-time data gathered from the power network with business policies to enable secure trading in a deregulated environment

2. Analyzing Areas of Concern

After the requirement gathering process was complete, common themes quickly became apparent as the IECSA program team analyzed stakeholder requirements. It was clear that the architecture must provide common strategies in several areas that underlie nearly all requirements information gathered. The common themes uncovered during the information gathering process include:

- **Basic Networking and Connectivity Infrastructure.** In particular, how will the myriads of device and communications technologies connect? In general, IP-based networks presented an obvious solution to the project team because of their widespread use in general computing. However, utility requirements for reliability, wireless access, changing configurations, and quality of service dictate special guidelines for using IP, and for using other technologies in particular environments.
- **Security and Access Control.** Deregulation and other effects of the Digital Society are forcing utilities to rely on public networks provided by third parties, to communicate with competitors, cross organizational boundaries, and to expand their communication networks (both inward to their own organizations and outward to the customer). These requirements make the need for cyber-security ubiquitous in power system operations. Encryption and authentication technologies abound, but the focus of the IECSA security strategy is to tailor security solutions to particular problem domains, and link them together with shared security management services.
- **Data Management**. The sheer volume and variety of data required to operate a power system within the Digital Society poses a staggering challenge when standardizing interfaces for reading, writing, publishing, and subscribing to data. In this area, the key strategy will be to identify

standardized common object models that can serve as building blocks for common services and applications.

- **Network and System (Enterprise) Management**. For an area that is relatively mature in commercial networks, the science of monitoring and controlling the communications network is surprisingly primitive, or even unknown, in power system automation. The key here will be to harmonize network monitoring technologies and network object models with the functional equivalents in the power industry and then integrating both with security management.

The analysis was also guided by the following engineering principles:

- **Business Needs** of the power system industry, as captured in the power system operations functions, and categorized into the IECSA Environments
- **Strategic Vision** based on high level concepts of distributed information
- **Tactical Approach** based on technology independent techniques of common services, information models, and generic 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.

IECSA 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.

3. Evaluating the State-of-the-Art

Equipped with requirements gathered from the industry and general strategies for approaching key problem areas, the IECSA team next considered which communications technologies and best practices it could use to build the architecture. For the purposes of developing the architecture, the term ‘technology’ had a very wide definition and could include a protocol, a database format, an object model, or a policy, among other things. Toward this purpose, the team ‘cast its net’ as widely as possible. It evaluated technologies from:

- **Multiple organizations.** The team was committed to the creation of open systems, and preferred to use international standards whenever possible. However, some of the best technologies available have been created by government bodies, industry consortia, and even private organizations. Technologies from all of these bodies were considered.
- **Multiple applications.** It was likely that technologies developed for one part of the power industry would be useful in other parts. Therefore the team considered technologies from protection, control, monitoring, metering, consumer access, and all other parts of the power industry equally.
- **Multiple industries.** For the architecture to be truly integrated, it needed to incorporate the best innovations not just from the power industry, but also from desktop computing, telephony, industrial automation, other utilities, business-to-business and of course the Internet community, among other industries. These technologies were considered key to bringing the power industry into the digital society.
- **Multiple disciplines.** Not just ‘hard’ technologies, but also best practices and procedural improvements were considered, where they related to communications. This was vital in areas such as security management, which depend as much on the human factor as on electronics or software.

The team actually analyzed technologies ***twice***: once ***prior*** to designing the architecture, to determine what 'building blocks' were available, and again ***after*** designing the architecture, to determine the list of technologies and best practices that the team would recommend for use in the design. In both cases, technologies were grouped into the four 'problem areas' discussed earlier: basic networking, security, data management, and enterprise management. Data management and basic networking were subsequently reorganized into utility-specific and non-utility technologies for ease of reference.

Each technology was evaluated for its strengths and weaknesses. The team captured these in a brief paragraph for each technology, including web references where IECSA users could find more information, and keywords for searching for particular technologies.

The team quickly realized that unlike some previous attempts to 'unify' utility communications, IECSA could not recommend a single set of technologies for use everywhere in the industry. Therefore, the team developed the concept of **IECSA environments**. Based on the stakeholder input, they identified over twenty different logical areas having common communications requirements, and made technology recommendations in each of these 'environments'. The team captured these technology recommendations in text and as a system of interlinked web pages.

4. Designing the Architecture

The design step brought together all that had come before: requirements gathering, strategy, and technology analysis. The resulting architecture is based on the following principles:

- Using the science **data modeling** to capture and analyze requirements in 'use cases'.
- Using **layered technologies** to separate levels of abstraction and functionality.
- Creating **common information models** and identifying common services and generic interfaces to create a **technology-independent** representation of the architecture.
- Making use of **self-description** (plug-and-play) and '**meta-data'** (descriptive information about data) to reduce configuration effort and error, and to facilitate automatic translation between technologies.
- Defining a number of **utility-specific environments** having common sets of requirements, as discussed in the previous section
- **Identifying missing or overlapping technologies** as a tool for making **technology recommendations** in each of the identified environments.

IECSA's technology-independence can be summarized in Figure 2. It consists of a 'backbone' of common information models and services primarily based around the IEC 61850, IEC 61968 and IEC 61970 standards.

The common 'nouns' and 'verbs' of these exchange models are translated into a variety of different technologies for communicating in different environments. As discussed earlier, IECSA provides a tailored list of recommended technologies for each of the 'use case steps' and 'environments' that were identified through the requirements gathering and analysis processes.

It is important to note that the IECSA 'backbone' is a logical structure, not a physical one. Translation from one technology to another may take place at many different places in the network. The translation function *itself* may be implemented on a variety of devices and using a variety of technologies.

However, the core concept of IECSA is that all devices within the network will eventually be able to communicate with each other. The common information models and services make it possible to easily and economically convey information without loss of fidelity across ownership and functional boundaries. Basing these information models and translators on self-description permits the network to quickly adapt to new technologies, applications, and devices.

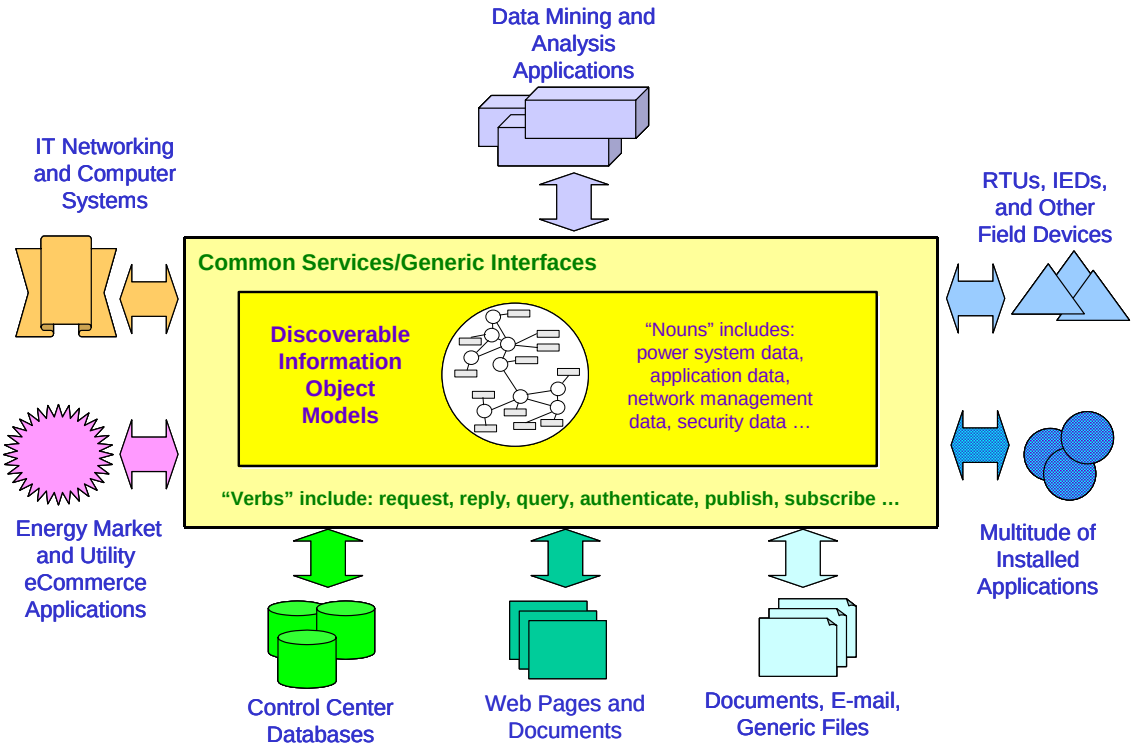

Figure 2:The Technology Independent IECSA Reference Architecture

The IECSA backbone consists of common information models, services, and interfaces that provide technology independence so the network can continue to grow and evolve.

5 . Capturing the results

IECSA is delivered in four volumes and a system of several hundred web pages. The deliverable components of IECSA answer the following questions:

- **The Value Story** – What are the drivers/benefits of an IECSA? What is the economic justification?
- **Requirements identification** – What types of data must be exchanged in an integrated power system? What functions must be performed? What knowledge will be needed in the 5 to 10 year horizon to build the supporting infrastructure *now?*
- **Analysis of the requirements** – What requirements do the messages exchanged within the power system have in common? Which requirements can be met by similar technologies? Which functions should be performed centrally and which should be distributed through the system?
- **Identification of future needs** – Not all the requirements that were identified can be implemented today. What technical areas need to be developed now in order to facilitate the integration of the power system in the future?
- **Terminology and Tools** – What tools exist for identifying, capturing and manipulating requirements? What language can we use to describe the power system of the future clearly enough to ensure interoperability?
- **Recommendations** – What practices need to be adopted universally in order to make an integrated power system a reality? What specific technologies should organizations use in their networks? What steps do standards organizations, governments, and consortia need to take?

- **Model of future operations** – How can we simulate the power system accurately enough to predict future needs? How can we describe new power system applications in a way that identifies their communications needs? IECSA provides industry-standard diagrams that graphically show the interactions among the various 'actors' and 'data items' in the functional areas explored.

These concepts are described in much greater detail within the body of Volumes I and IV. The organizational structure of the volumes is shown in the following table:

Table 1: IECSA volume organizational structure.

Volume	Title	Contents	Intended Reader
I	IECSA User Guidelines and Recommendations	▪ The executive summary ▪ The IECSA value story ▪ How to use and apply IECSA ▪ Basic terminology ▪ Detailed summary of the development process ▪ Summary of strategies, conclusions, and recommendations	▪ Executives ▪ Managers ▪ System architects ▪ Regulators ▪ Advisors who must decide how to use IECSA
II	IECSA Requirements	▪ A detailed description of the requirements gathering process and tools used ▪ Examples of particular 'use cases' capturing utility requirements ▪ Guide to the on-line website that express these requirements graphically	▪ Power system planners who must find new concepts and trends in automation ▪ Project engineers who must find solutions for particular problems.
III	IECSA Model of the Architecture	▪ A guide to the Universal Modeling Language (UML) database that captures the requirements and analysis of power system operations	▪ Vendors, IT specialists, Chief Information Officers who can use a model of power system operations to identify and build new solutions
IV	IECSA Technical Analysis	▪ A more technical guide to the development and results of the architecture	▪ System architects, power system engineers, and those interested in further analysis of the results

Recommendations for the Future

The first volume contains the IECSA team's recommendations for the future. These recommendations are divided into several categories:

- Encouraging power system organizations to design networks using an architecture approach
- Contributing to standards development organizations and consortia
- Sponsoring pilot projects and field trials
- Developing engineering tools and notation methods
- Integrating IECSA with other architectures
- Encouraging the adoption of IECSA concepts and recommendations
- Initiating work to continue systems analysis of the utility industry in more detail

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

- **Harmonize the existing common services, information models, and interfaces, as well as create new standards where they are needed,** so the power industry speaks a common communications language of 'nouns' and 'verbs' that can be translated into different

technologies. This is a key requirement for the higher levels of system integration now emerging across the energy industry

- **Integrate security, systems, network management, and technical development (i.e. new technologies)**, which have too often been considered separate tasks.
- **Unify technologies between power system automation networks, corporate networks, and inter-business networks**, again by linking them to common information models, services, and interfaces.
- **Remember that developing an industry-level architecture is a process** – not an end point. Requirements and enabling technologies are constantly changing. Although the guiding principles should remain constant, individual solutions *will* change over time.

Next Steps

The five steps discussed in this summary have captured an initial set of the power system's operational requirements and the proposed design for IECSA. However, three key steps of system architecture design remain to be executed:

- **Testing** the principles of the architecture in prototypes and pilot projects.
- **Implementing** and validating the design in real-world, large-scale systems.
- **Feeding back** the lessons learned back into another iteration of the process.

Designing IECSA is just a start. IECSA must now be built, proven, and continuously improved upon so that the vision of a power system integrated with its communication system can be realized.

CONTENTS

LIST OF FIGURES

LIST OF TABLES

1. INTRODUCTION

The Integrated Energy and Communications Systems Architecture (IECSA) project represents the initial steps on a journey toward a more capable, secure, and manageable energy provisioning and delivery system. The IECSA project envisions a variety of plausible futures for electric and energy service operations ranging from advanced automation to dynamic consumer response. The project results propose the next steps in the process of bringing this vision to fruition. These steps include using more rigorous systems engineering practices, application of IECSA principles, and implementing the project recommendations.

IECSA builds upon existing information industry infrastructure and standards development work and proposes a series of pathways by which the industry can more effectively integrate advanced automation and consumer systems over the long term. It should be noted that developing an industry-level architecture is a process, not an end in itself. The IECSA project represents only the initial steps in a longer journey toward more effective long term and intelligent use of advanced technology.

1.1 Historical Perspective

One can consider IECSA to be the third wave of focused efforts endeavoring to define reusable architectural components for energy enterprise and industry-wide applications. The first two waves of industry efforts were the Integrated Utility Communications Project and the UCA® 2 Effort.

Integrated Utility Communications Project

The first effort was performed through the efforts of the Integrated Utility Communications Project, which initiated by EPRI® in 1986. Through these initial efforts, a cadre of utility domain experts was consulted and their views combined into the first incarnation: UCA (Utility Communications Architecture). What was most impressive about this effort was the top-down, requirements-driven analysis performed by objective professionals in pursuit of a common communications denominator in the utility industry.

UCA 2 Effort

EPRI furthered the effort in a series of tailored collaborations that endeavored to apply the original UCA architecture. As UCA implementations efforts moved forward, improvements and clarifications were made to the document, which resulted in the issuance of enhanced architectural descriptions which became know as UCA 2.0. Crucial to the success of UCA was the involvement of domain experts and developers in the application of the concepts. At this time, EPRI took steps to submit the UCA documents to the International Electrotechnical Commission (IEC) Technical Committee 57, where the work was accepted into the IEC 61850 standards process.

These original EPRI efforts succeeded in establishing a direction for the industry and creating momentum toward abstract modeling and interoperability. The IEC 61850 standards are beginning to mature and major vendors are developing products from these standards. In addition, EPRI has worked to develop the Control Center API project into the Common Information Model through contributions to the IEC TC57 standards initiatives. Finally, EPRI has facilitated the formation of a users and vendors association, The UCA International Users Group[1].

More than a dozen years have elapsed since the first UCA effort. During this period two things have become apparent. First, an extraordinary evolution in communications and computing technology has occurred and will continue. Second, the scale and scope of advanced automation extends beyond the

[1] http://www.ucausersgroup.org/

standards that have developed for the energy industry. Standards and infrastructure development from a variety of industries must now be included in the design and enhancement of an industry-level architecture for the energy industry. The energy industry architecture must now include standards from information technology, building and home automation, and eCommerce, to name just a few. It is important to now advance the concepts originally conceived and laid down by the UCA into the modern age. The IECSA project represents this effort.

1.2 Industry Trends and Project Drivers

The IECSA project was initiated in response to several significant trends and drivers facing the energy services and power delivery industries. Of these trends, five main technical development and business drivers were key forces behind the conception of the IECSA Project. Each key driver, discussed individually below, carries important business and technical implications for the energy services industry as it moves ahead in the areas of advanced automation systems and consumer communications.

Driver 1: Cost effective use of emerging technology

The migration toward effective use of more capable open standards is crucial for a robust power marketplace where hundreds of companies supply products that enable future visions to become a reality. As such, the need for greater, and more effective, use of advanced communications and computing technologies is a key driver in the goal to improve the overall energy system.

The industry, as a whole, must strive to leverage investment in communications and advanced automation by more effectively using installed information automation equipment. Incremental investments in advanced automation and communication infrastructure must support multiple applications today and be extensible for future needs. The industry cannot afford to install single-purpose automation applications and equipment; this inevitably leads to layered, redundant infrastructures.

Designing the IECSA architecture to address this first driver will help overcome the limitations of proprietary systems and standards that are too narrowly defined. Large collections of disparate systems, sometimes with partially overlapping functionality, can quickly become confusing and unwieldy to manage. By comparison, a well-designed architecture enables initial designs and installations that take into account for future operating scenarios. Developing a cohesive architecture and intelligently using open systems will also assist in more effective life-cycle management of equipment. An overall architecture will help ensure that systems are initially built with a robust set of initial requirements so they are adequately specified and designed for both present and future needs. Architected systems will enable future integration and extensibility so that adding a new function does not require wholesale upgrades or replacement of systems.

Driver 2: Higher levels of integration across traditional boundaries

The need to better integrate advanced systems across traditional boundaries and barriers to create interoperable systems is the second key driver for the IECSA Project. Industry changes are driving tighter operational integration between a greater diversity of business entities - for example, integrating electric energy generation and delivery with consumer premises equipment. In response to this demand, the industry is attempting to dynamically integrate consumer operations through a collection of applications, under the phrase ‘demand response’. A myriad of technical and management issues must be addressed, however, to enable this vision to reach maturity.

Unfortunately, this emerging paradigm will require a massive level of interoperability previously unseen in the power industry. Connecting end consumers to power system operations will call for the integration of millions, or even billions, of devices. Furthermore, administration of such a system presents a huge burden for entities using the equipment.

Development of an industry architecture will result in migration to more uniform systems development, thus easing the burden on systems administrators. More powerful systems administration capabilities (including data management, security, monitoring, and diagnostics) can be designed and built directly into equipment, enabling systems management that can scale to the levels now envisioned for the energy industry.

Driver 3: Infrastructure development and standards coordination

The third IECSA driver responds to the need for greater coordination and integration of the myriad of standards and infrastructure development initiatives currently taking place across the industry. Standards are necessary for systems to interoperate. However, it is important to note that the *standards* developed by the industry must also work together or these very standards contribute to the greater problem of balkanized systems on large scales.

Development of an industry-level architecture is a necessary response to the need for greater integration within, and between, standards communities, as well as enterprises. The energy industry has had some painful examples of system installations that failed to scale to large numbers, or to interoperate effectively with systems from different vendors. An architecture will play a critical role in developing and integrating future standards by providing a context and a larger-scoped framework than is normally considered by a single standard. Only in this way can standards hope to interoperate today and scale to address the needs of tomorrow.

Driver 4: Response to new and emerging requirements

The fourth IECSA driver arises from emerging enterprise-level and industry-level requirements. Since new system requirements appear constantly, any proposed power system must be robust enough to both anticipate and adapt to changing requirements. Many systems that are installed today will eventually require upgrading to meet future requirements. Systems that are inadequately specified to meet future needs are effectively obsolete, even before they are installed.

The IECSA project has particularly emphasized system requirements to capture scenarios involving future operations. These requirements for future system functions originate from a variety of sources. Most requirements are *constructive* in nature and seek to add capabilities or integrate with more systems. Other requirement sources, however, can be bluntly described as ‘hostile’. While advances in new communication, embedded computing, and information technologies can provide significant benefits, they also bring with them a serious dark side that must be addressed. System architects designing future energy provisioning systems must be concerned with meeting plausible requirements from an expanding set of *hostile* sources. In addition to cross-industry integration, requirements are emerging in key areas of policy-based systems management and cyber security. That which was once deemed a reasonable level of protection is inadequate today and for the future.

It should be noted that the IECSA project emphasizes that it is not only important for the energy industry to use new and emerging technology, but also vitally important to address how the technology is implemented.

Driver 5: An industry vision to enable a robust future

Finally, the IECSA project is about creating a vision for the future and embarking on robust and strategic pathways to enable applications envisioned today, as well as those not yet imagined. To operate in a manner unimpeded by traditional thinking, an industry architecture must address the former and enable the latter.

The IECSA project has created plausible scenarios for future operations that extend beyond traditional energy service provisioning. IECSA’s reach extends from central generation systems and natural direct energy sources to operations within and between consumer end-use equipment. IECSA goes beyond the flow of electric energy into end-use equipment to encompass performance and functions both within and peripheral to this equipment. By definition, an architecture at this level

must be used for visioning with a scope broad enough to embrace the future effectively. This visioning is not exhaustive within IECSA, but rather *representative* of the types of interaction and integration that are both useful and possible within the energy services industry.

1.3 IECSA Project Scope

The scope of the IECSA project, by definition, must consider the entire energy enterprise: the *power engineering* and *information technology/distributed computing* elements. Since the distributed computing systems must support both power engineering applications and information systems, the requirements for the future distributed computing system are subordinate to the needs of the power engineering and business support systems and to the system management functions. IECSA is required to integrate customer interaction, power system monitoring and control, energy trading, and business information systems. It will reach across customers, feeders, substations, control centers and energy traders.

IECSA is a roadmap for 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 power system capable of handling emergency and disaster situations, while also able to accommodate current and future utility business environments, market requirements, and customer needs.

> *"We have a digital economy and we're still trying to provide power to it through a mechanical design system that was designed over 50 years ago. It is a marvelous system, but we've been effectively borrowing against the future to pay for the present, and the future has caught up with us, we need to build the system to serve the digital society of the 21st century.*
>
> *...And it's then the controllability of that system. Once we have those digital controls in, we can instantaneously manage the power system so it is self healing, that is it can detect instantaneously a difficulty and correct for it locally so that cascading effects can be eliminated and fundamentally improve the reliability of the system so that computers and other sensitive equipment that has come in over the last decade [are] not upset by power disturbances."*[2]

1.4 Adoption of Advanced Tools and Methods

In any vision of the future energy industry, operations will be substantially more complex than today. This complexity must be managed on a variety of levels, including business relationships, regulatory processes, and technology integration. An architecture must account for these relationships and complexity. To meet the challenges posed by this project, the IECSA team found it necessary to innovate tools and methods to capture the complexity of future energy industry operations. This required adopting both systems engineering methods and emerging standards for representing high-level architectures. As a result, the IECSA project introduces necessary terms and language emerging from architecture development and systems engineering communities.

IECSA is not an endorsement of specific methods, tools, or products

The tools and methods used within this project were selected for the purpose of developing the IECSA Framework. The project used systems-engineering-related standards and notations to document relationships and content specific to those relationships. While these standards and methods represent some of the best thinking in the industry, they also continue to mature as a technical discipline. While the specific tools and methods selected for the IECSA project are useful to define

[2] Kurt Yeager, EPRI CEO in an August 25, 2003 interview on the Lehrer News Hour about the August 14, 2003 East Coast Blackout.

architectural level issues, this generally does not constitute an endorsement of these specific tools. The team selected tools and methods on the basis of the best available approach for defining and evaluating large complex distributed computing systems. However, the underlying systems engineering discipline and the community developing the industry-level architectures will continue to mature. The team anticipates further refinement and improvement of the specific methods and notations used within this project and recognizes that there will be additional valid methods for representing industry level architectures.

Systems engineering methods are recommended

The energy service provisioning industries have reached the point where managing technical and business complexity is of paramount importance. The combination of information technology, advanced automation, and communications systems, (collectively referred to as 'distributed computing') does not yet have the technical rigor of traditional engineering disciplines, such as electrical, mechanical, or civil engineering. This requires greater discipline than traditionally used in development or implementation of many advanced automation and distributed computing systems. Systems engineering is the discipline of rigorously defining systems through a series of technical steps where design decisions are traceable back to requirements. The IECSA Project recommends that the next steps in the development of an integrated industry architecture follow the disciplines underlying systems engineering.

1.5 A shortage of integration and cooperation, not technology

An architecture is fundamentally about integrating a wide variety of components into a coherent and beneficial whole. While there is no apparent shortage of base technologies and components that may comprise the future energy system, there is a significant shortage of interoperability and integration between individual technologies and components. Examples of base technologies include computers, communications, and field devices. The free market does well developing these base technologies and stand-alone products but is not as successful when developing infrastructure. This is understandable since the principal goal for vendors of products is differentiation, not uniformity.

There is a particular need in the power industry for an organized infrastructure (standards and technology) that will enable valuable and cost effective interoperation between products developed by different vendors. Without substantial demand (or pull) from the user community, there is little incentive for vendor 'A' to facilitate interoperability with products from vendor 'B'. Instead, vendors must recognize that interoperation is the minimum common requirement and that differentiation will come from feature sets and service offerings.

1.6 Infrastructure required to move energy industry forward

For a century the electric industry has focused predominantly on developing the electric system that we know today. The system of power plants and power delivery system components comprise a significant energy infrastructure. This electric infrastructure has grown during a century of technical development and is the most capital-intensive of all the public service infrastructures described as utilities. As we look to the future of this system, it will increasingly rely on another infrastructure that must be developed in parallel to move the industry effectively toward the future.

This second infrastructure, the information infrastructure, will be made up of communications technologies, networking technologies, intelligent equipment, and algorithms that can execute increasingly sophisticated operations functions. This second infrastructure can be collectively described as 'distributed computing' since it comprises a variety of technologies that enable the sharing of data and controls within intelligent equipment.

1.7 Architecture Defined

An architecture is directed toward the development, integration, organization, and life-cycle management of information technologies and advanced automation systems. The architecture community has developed a few working definitions that can be applied to the IECSA project:

> *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.*[3]

Though there are several different definitions for architecture, all include the following recurring themes:

High-Level Perspective

The most common theme defining an architecture is that it must have a high-level perspective. This perspective enables an organization to view its operations in the context of how it integrates with multiple systems, both within the enterprise and outside of it. The IECSA Project is unique from this perspective as it views the operations of the future electric energy services industry from a high perspective level that cuts across traditional boundaries.

Need for Common Language on Different Levels

The high-level perspectives of an architecture often expose challenges when attempting to integrate business or operational entities that have not considered operations beyond their traditional domain. Bringing these systems together requires effort to develop a common language across all business and operating domains. A common language is required for both business discussions and technical 'computer to computer' communications.

Life Cycle Strategies

An architecture seeks to develop strategies by which new levels of integration can be achieved across the enterprise and across the industry. Additionally, an architecture examines the system from a long term perspective with an eye to how the system may evolve. A good architecture should require little change over time. Indeed, a strong architecture plans for change and includes a process to adapt and evolve, lest it become obsolete itself.

Integration of Standards and Technologies

The essence of an architecture is the use and integration of standards and technologies into an interoperable framework. In this project, the reader will see several references to standards, technologies and best practices as the building blocks of an industry architecture. However, an architecture is not simply about making better use of standards and associated technologies. Today's standards and infrastructure are often developed with narrow scopes or with specific groups of applications in mind. In comparison, architecture development implies working within the standards communities to develop methods and strategies through which the standards can work together more effectively. It also means that in some cases, those working on standards and their associated technologies will discover new capabilities and requirements.

Integrating standards strategies is, therefore, one outcome of architecture development. Several examples of standards and technology integration needs have surfaced within IECSA. The IECSA framework, if followed by those implementing technologies, will provide a strategic pathway by which systems that were once islands can become integrated.

Recognizing a Variety of Audiences

An architecture addresses technical issues that arise at an enterprise or industry level. The implications of these issues may be manifest at various levels within an enterprise. Architecture

[3] IEEE STD 1471, 2001

development carries implications for both business operations and technical operations within an enterprise. For this reason, architecture development has implications for the high level business process, as well as for lower level tasks, such as just getting two products to interoperate. As such, architectures must address a variety of audiences, ranging from business strategy planners to field engineers. The primary audience, however, is system architects who are concerned with enterprise level systems integration. These individuals are typically associated with either information technology systems or advanced automation systems.

Integration with other developing architectures

IECSA's enterprise and industry-wide scope necessarily means that other architectures undergoing development in parallel will become part of the implemented form of IECSA. For example, other key architectures in development at federal, state and even international levels will need to be integrated with IECSA to some degree.

Emerging federal and state information technology architectures are establishing policies to integrate information systems within government agencies. IECSA's reach will include the combination of information and advanced automation systems needed to integrate with developing federal and state level architectures. Examples of possible integration include business-to-business, electronic commerce, and basic consumer service functions. Policies, including system management and security, must be compatible across architectures to achieve the desired levels of system integration and interoperability. The energy provisioning industry must integrate strategically with other developing architectures to achieve the visions put forward by the industry.

Several emergent architectures that are predicted to be integrated with the energy services architecture are discussed below. It should be noted that these architectures are driven by federal legislation, Government Accounting Office (GAO) guidance, and other mandates that are key drivers:

Federal Enterprise Architecture

The Federal Enterprise Architecture (FEA) was developed as the result of federal legislation passed during the 1990s. The FEA's purpose is to integrate the information systems of all federal agencies. While it predominantly targets information systems environments, the policies that FEA presents, such as the development of e-commerce and e-government, have implications for integrating energy industry initiatives. The FEA has been undergoing development for the past several years and represents a serious effort to integrate federal agency systems. Information systems installed by federal agencies must show compliance or migration to the FEA in order to continue to receive funding to support these systems.

Department of Defense Architecture Framework

The Department of Defense Architecture Framework (DODAF) is the architecture intended to integrate the systems of the Pentagon and all branches of the U.S. military. This architecture prescribes policies for integrating information systems and advanced automation systems with military buildings and business systems. Energy systems seeking to interoperate with Federal DoD buildings (for example, building automation systems) will be subject to the policies within the DODAF.

State Level Architecture Development

Many states have begun developing architectures to integrate systems and services at the state level. These architectures are directed toward integrating state office functions and public services, including, but not limited to, state and local public services. Similarly, these architectures will address business and government electronic commerce systems. States, such as Arizona, Ohio and others, have begun establishing enterprise architectures and policies for information systems. In addition, organizations, such as the National Association of State Chief Information Officers, endorse the concept of architecture development. Policies emerging from state architecture development related to security policy management, systems integration, e-

commerce and e-government can be foreseen to impact the implementation of energy related functions with government buildings and information systems.

International Level Architectures

Architectural elements and rules of governance are under development by international communities to address issues such as models of governance and commerce across national lines.

1.8 The products of an architecture

An architecture is comprised of a variety of elements including requirements, models, analyses, terminology, and recommendations. All of these elements were addressed during the IECSA project.

Recommendations

It has been stated that an architecture is a journey and not a destination. One of the most important outputs from an architecture development effort is a clear view of what lies ahead, as well as the path to get there.

As such, the IECSA architecture provides a collection of recommendations for using and applying a variety of standards and technologies, which, in turn, can be used as the building blocks of integration. Also included are best practices for the energy industry to follow as the integrated architecture is implemented. In addition, the IECSA project has highlighted technical issues that must be addressed to 'complete' the standards, technologies, and best practices for the future energy services industry to operate effectively. An example of these issues can be seen in the variety of requirements now emerging for industry operations, which pose unique challenges to future advanced automation systems. Integrating the required technologies is an emerging technical need. These recommendations are presented in Volume IV of this series.

Analyses

The IECSA architecture also contains analyses that support the project team's recommendations. The analyses may utilize a variety of methods to understand future energy industry operations. This project used a variety of analysis methods that were based on the requirements gathered during the project, as well as on the team's experience within the industry and standards communities. However, all analyses, no matter how rigorous, are grounded in human, subjective terms. It is therefore imperative that all decision points are traceable back to requirements. Only in this way are the conclusions meaningful.

Requirements for future systems

For this project, a series of future operational scenarios and their associated requirements were developed. The requirements were developed through a combination of studies and interactions with some stakeholders of the future energy system. The set of requirements captured within this project do not exhaustively cover every possible application of advanced automation or information technology. A comprehensive list of applications could number in the thousands.

It should be noted that the requirements considered in this project were developed for a select set of applications that were believed to carry 'architectural significance' for the industry. These requirements and associated operations scenarios, known as 'use cases', form a framework of functions that encompasses most architecture challenges faced by the energy industry. Architecturally-significant issues addressed in the IECSA project included challenges arising from implementing systems on a large scale and over a wide diversity of businesses and technical operating environments. These issues include integration and interoperability issues, implementing consistent policies and developing the techniques to manage systems on large scales.

A Model of Future Operations

The IECSA project also developed a model of future operations using a combination of two sets of standards for architectural modeling. The complexity of the future energy system requires modeling to effectively capture relationships and integration between systems. Developing a model for an Integrated Energy and Communications Systems Architecture prior to its detailed design and implementation is as essential as having a blueprint for a large building. Good models assure the robustness of the design and are necessary for communicating among stakeholders.

Terminology

One of the largest challenges any architecture project faces is bringing forward a common set of terms that are useful for discussions across traditional operating boundaries. Just as a model is critical to communicating among stakeholders, so too is standardized terminology. It is impossible to have consensus on meaning and intent without first establishing definitions for the terminology. It is equally important to have definitions traceable back to standards bodies in order to maintain consistency in meaning across disciplines and industries.

To that end, terminology is presented and used in the model of future industry operations. Ideally, terminology is traceable to the standards that are adopting the terms. Within the IECSA project, priority is given to terminology being developed within key standards organizations.

1.9 Vision and process for a seamless, managed architecture

IECSA's vision for the architecture uses an integrated approach to describe the enterprise requirements. An approach focused solely on applications does not easily yield the type of interoperability needed or desired. Instead, a rigorous *systems engineering approach* was adopted for soliciting requirements from key stakeholders. Enterprise domains tell us what the top level requirements are, and analysis reveals key applications that could realize those requirements. Key applications with the promise of exposing common services to enable interoperability are further explored. Analysis of those common services can allow the team then to enumerate the communication requirements for interoperable systems.

When conducting analysis at different levels (enterprise, application, services, communication), it is important to understand the context of each requirement. A formal framework for capturing the full context of each requirement was adopted. The methodology used by the team separated the description of the systems and subsystems into five different viewpoints. Just as a building plan relies on differing views (plumbing, structural, electrical, etc.) to represent the whole, so too does a communication architecture rely on different descriptions. As seen in Figure 3, the model breaks down into five viewpoints that can be roughly portrayed as describing (1) **Who** participates, (2) **What** information is exchanged, (3) **How** is the data processed or interpreted, (4) **Where** are the interacting devices located and (5) **Which** technologies are used to facilitate or manage the exchange.

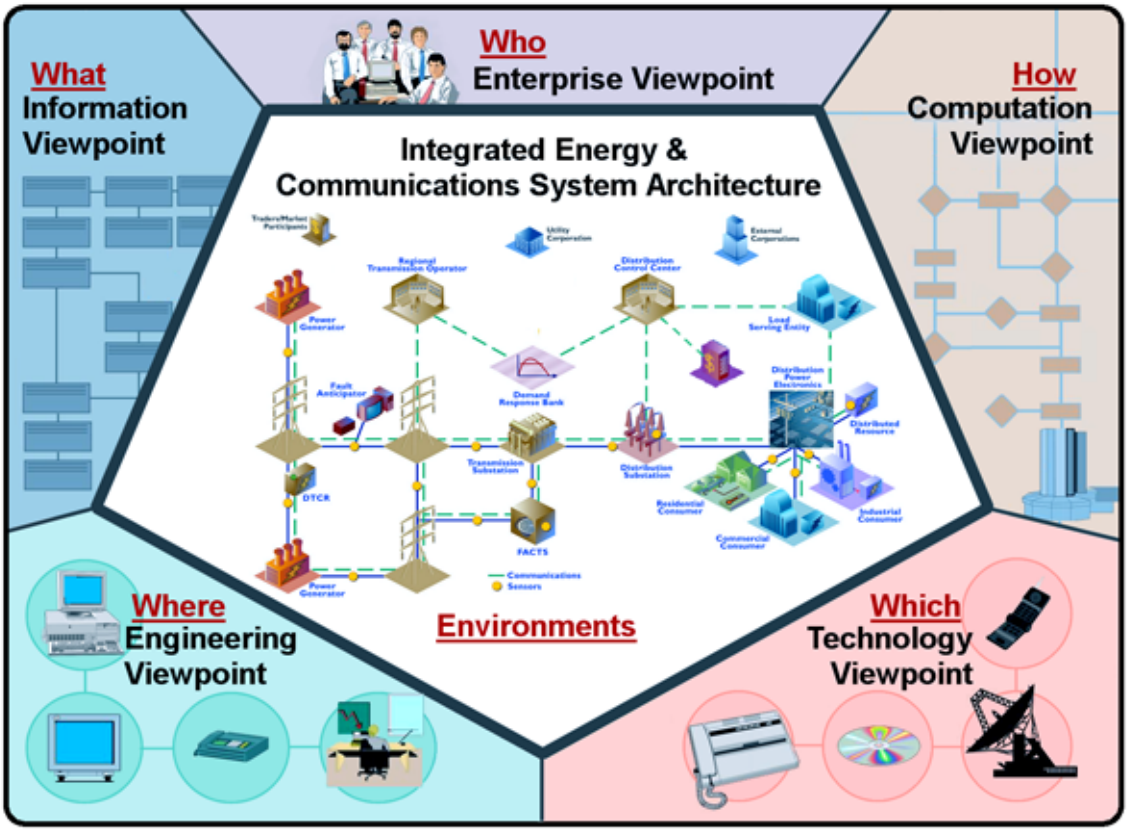

Figure 3: Introduction to IECSA

The Architecture must be understandable to architects and lay people alike to be useable.

2. THE NEED FOR AN INDUSTRY ARCHITECTURE

There is a two-part answer to the question, "Why it is necessary to develop an industry architecture?' First, it must be understood that the challenge facing utility executives is keeping the lights on while also enhancing the value of services to consumer. However, by itself, the need for increased reliability is not enough to mandate the development of an industry architecture. The second, and more powerful argument, is that the only way to address the challenge utility executives face is to go back to basics, understand why the current system doesn't perform as needed, and then to design interoperability into the system from the ground up.

2.1 The value of an industry-level architecture: baseline energy system integration versus status quo

In today's uncertain, vulnerable socioeconomic and geopolitical environment, utility executives are under increasing pressure from shareholders to efficiently manage the electricity supply chain, while maintaining a sustainable growth rate. At the same time, these executives must strive for more efficient, cost effective, reliable, environmentally friendly, stable and secure operation of the power system. Regulators, government, governing bodies, interest groups, and consumer advocate groups also require utilities to comply with numerous reliability, restructuring, and environmental mandates. Last, but far from least, consumers demand the utility ***to keep the lights on***.

To meet these expectations and the needs of our power-hungry society, utility executives must rely on the machine known as the 'electric power grid'. Over its hundred-year history, this grid has been expanded continuously. It has become quite complex and technologically fragmented, thus making it difficult to manage and predict its behavior. In recent years, the electric power grid has been asked to perform far beyond its originally designed capabilities, creating operational challenges for today's utilities. The threat of cyber attack and physical sabotage further complicates the challenge of keeping the system operational. To keep the lights on, the current system must be analyzed and deficiencies in the fundamentals of quality power delivery addressed. Current fundamental deficiencies in the grid include:

Stability of Supply

The network's age and complexity, along with the increased energy demand, challenge the stability and reliability of the grid. Moreover, the inadequacies of legacy distributed computing systems, dispersed heterogeneous data and legacy applications, and lack of reliable integrated energy and information infrastructure compound this problem. Reduced maintenance budgets, increasing life cycle cost, and a shortage of trained personnel add even more dimensions of complexity. Power systems operating near system capacity, managed by dispersed computing processing and information infrastructures, utilizing legacy applications without a unified view, and shortage of expert-trained staff are destined for cascading failures and the resulting widespread blackouts.

Quality of Service

Today's digital society is dependent on a reliable source of electric power. The loss of power is not only very inconvenient, but can also be very expensive. The costs associated with loss of power during the Aug 14, 2003 blackout have been estimated at $6 billion. Although the cost of making the electric power grid an impenetrable fortress is prohibitive, much can be done to significantly improve its overall reliability and availability. Moreover, the frequency of power outage also causes the loss of customer confidence in their electric supply, and consequently has resulted in corporate sector spending to install temporary power.

Security

The growing danger of cyber attack and physical sabotage pose fundamental challenges to the security and reliability of the power supply. Untenable and inconsistent system management and security policies resulting from a lack of an industry-wide integrated system architecture and inadequate key business/regulatory entities, exacerbate this problem.

Environment

Environmental concerns have made it difficult to augment the grid and add additional transmission capacity. Environmentally conscious consumers increasingly demand 'green energy' sources, including wind and photovoltaic energy. Adding these distributed energy resources to the grid will bring new opportunities and challenges to effective grid management.

Workforce Reduction and Talent Swap

Competition for the information technology talent base, reduction in power system trained engineers, voluntary force reduction, and loss of workers with legacy system knowledge has created a talent gap which directly affects critical day-to-day grid operations.

Satisfying All Stakeholders

Against the backdrop of deregulation, it is becoming increasingly difficult to satisfy the myriad of stakeholders with vested interests in the operation of the power grid.

Asset Swap/Capital Investment

Globalization, mergers, and acquisitions—combined with restructuring and economic uncertainty—have forced the deferral of critical asset procurement. One report[4] shows a $112 million per year decline in transmission system spending (Figure 4). This trend underscores the need to develop techniques channel more power through existing assets.

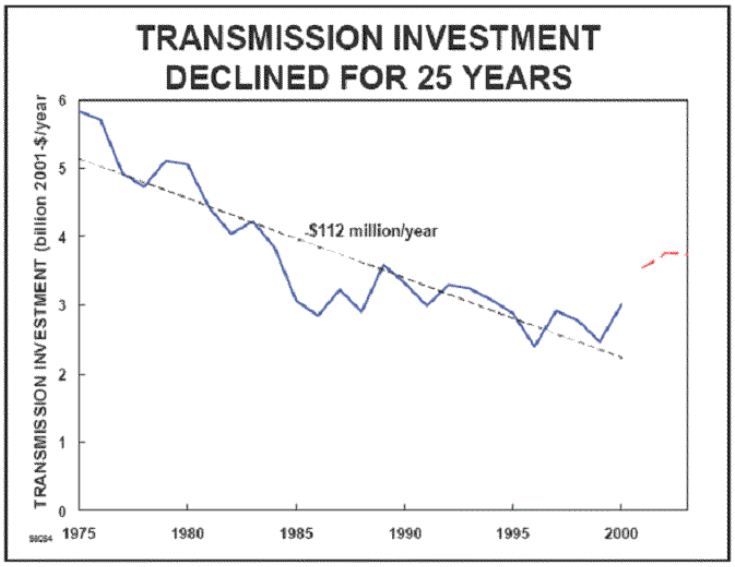

Figure 4: Transmission Investment Trend

There has been a decline in transmission investment for the past 25 years.

[4] Hirst, Eric; "Transmission Planning for a New Era"; 1/2004; http://www.ehirst.com/PDF/TXPlanning102.PDF

In this volatile and uncertain operating environment, it has become an unprecedented challenge to ***keep the lights on***. There is an urgent need to revitalize and modernize the electric power grid. Meeting these expectations requires the overlay of a robust high-performance information infrastructure. Put simply, to build a solid foundation, all the fundamental aspects of quality power must be reinforced.

2.2 Back to Basics…the need for a reliable customer centric operation

Growing pressure for customer-centric and highly reliable power systems mandates new integrated approaches to enhance power system robustness at the grid apparatus level. In addition, there must be new approaches to develop the underlying communication and information infrastructures. Only through this paradigm shift can utilities find an operational balance to increase reliability without sacrificing profitability. They must find a way to deliver measurable benefits to their customers and shareholders including:

Operation stability

Reduce outage frequency and duration b*y* identifying problem conditions and preventing difficulties (harmful conditions in transmission and distribution, power quality variations, interruptions, equipment failures) *before they occur*.

Asset management

Defer capital expenditure by increasing asset life and system throughput through continuous automated monitoring, thereby *resulting in reduced operating and maintenance cost.*

Responsiveness

Retain customers by providing consolidated and *competitive service and innovative product offerings.*

To achieve the new level of reliability and profitability mandated by customers and the new market dynamics, the fundamentals of quality power must be revitalized, redefined, and rebuilt with a new mindset. This mindset must employ a new set of disciplines and guidelines in accordance with the current geopolitical and geo-social reality.

In this new paradigm, the system is simple but intelligent; its behavior adaptive and proactive, not static and reactive. It is secure.

To achieve these objectives, the new paradigm must provide a clear set of useful, reality-based tools, procedures, and guidelines to facilitate:

- Integration of operational and business decisions
- Expandability, scalability, flexibility of applications and computing systems
- Information (distilled from data) to support the right decision
- Tools to communicate with customers
- Increased throughput and decreased congestion
- Adherence to stringent environmental requirements
- Competitiveness in response to profit pressure
- Disaster prevention and recovery
- Post disturbance monitoring and analysis
- Mergers and desegregation of assets
- Security

Adapting the fundamentals of quality power into this new paradigm will provide a solid foundation for a power system made up of automated transmission and distribution systems all operating in a coordinated, efficient and reliable manner. Such a system will handle emergencies, will be 'self-healing', and will be responsive to energy-market and utility business- enterprise needs. This system will involve millions of customers and have an intelligent information infrastructure enabling the timely, secure and adaptable information flow needed to provide reliable and economic power to the evolving digital economy.

Adoption of these principles will make the grid smart enough to monitor itself, predict problems, take corrective actions……***all while keeping the lights on.***

2.3 Consequences of the status quo

If the power industry continues with the 'baseline architecture' and the industry status quo, advanced energy automation and consumer communication systems will be significantly fragmented when viewed from an industry architecture level. Moreover, without concerted efforts to improve standards and technology integration, the status quo is likely to continue to be fragmented in several key areas. In some cases, there is duplication of standards development, while some needed standards are not being developed. It should be recognized that there are pockets of good standards work taking place, but the situation can be improved through improved coordination and harmonization between standards.

Further, the problem is not merely organizational: the technology gaps make the energy automation and applications integration tasks extremely difficult. Patchwork solutions applied to fix these gaps make the overall system unmanageable and difficult to maintain. Discovering how to develop standards, and their resulting technologies, comes strategically from efforts to develop an industry-level architecture.

The vision of a highly integrated, interactive, and self-healing system will not come about on its own. The integration and systems management needs suggested by this long-term vision demand the application of architectural principles in the design and development of advanced automation and consumer communication systems for the future. The system must be viewed from an architecture level, and strategies must be developed to bring about the necessary change and integration.

2.4 Why an architecture will solve this problem

Problems that surfaced in the August 2003 blackout touched on several architecture level concepts. Issues such as the need for sharing data over larger areas and the ability to view the system from high operational levels are architecture related issues that emerged. An architecture is required to survey the issues of integration from a high level. Ad hoc development work that focuses only on system components will not further the needs of the overall vision. An integrated power systems and communication architecture will enable the utilities to:

- increase the grid reliability–***keep the lights on***
- increase interoperability–***keep costs down***
- enable the next level of services for customers–***generate value for shareholders***

3. IECSA REFERENCE ARCHITECTURE FRAMEWORK

3.1 Objectives and Results of the IECSA Project

As seen in Figure 5, the development of IECSA focused on two primary project results, together called the IECSA Reference Architecture Framework. These results are described in more detail in the following sections.

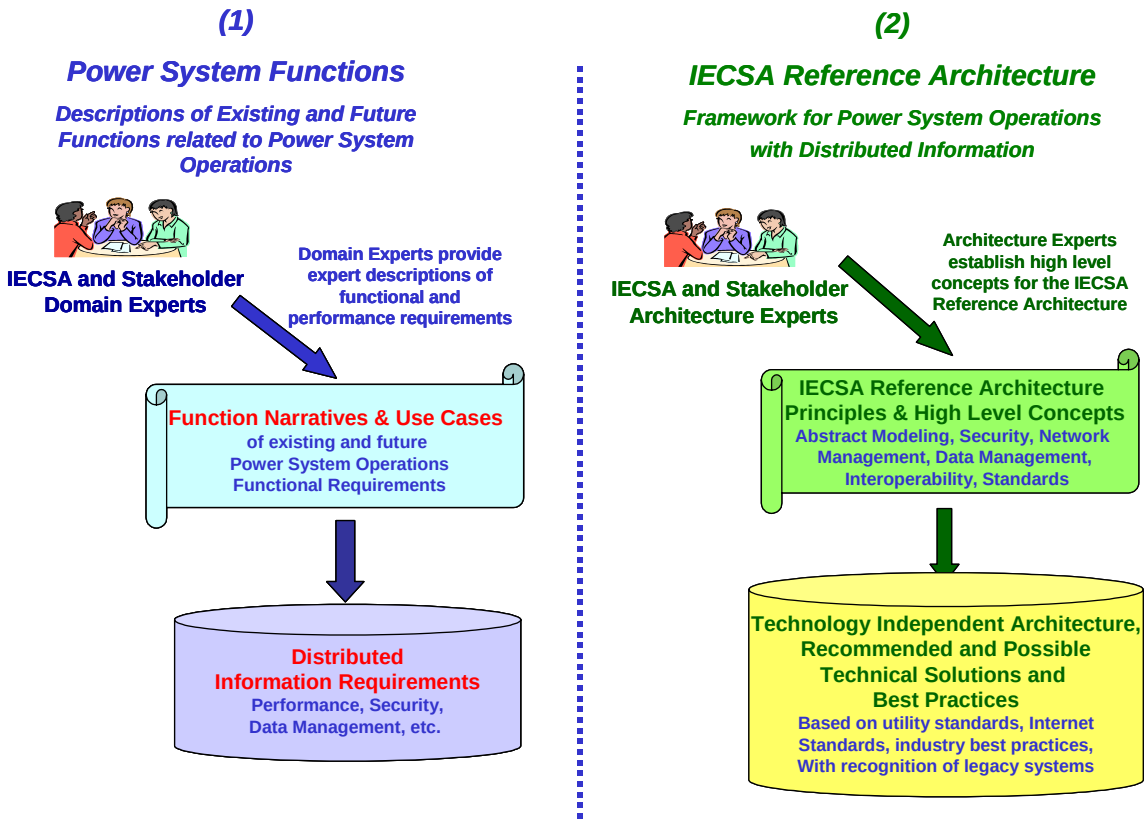

Figure 5: Two Primary Purposes of the IECSA Project
Collectively, this is the IECSA Reference Architecture Framework

3.2 The 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.

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.

3.2.1 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.[5]

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.

3.2.2 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 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

3.2.3 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 system out of the individual pieces.

3.2.4 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:

[5] IEEE STD 1471, 2001

- **Business Needs** of the power system industry, as captured in the power system operations functions, and categorized into the **IECSA Environments**
- **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. Figure 6 depicts the IECSA Reference Architecture Framework and clearly identifies how these concepts fit together. The individual concepts shown in the figure are discussed below.

Figure 6: IECSA Reference Architecture Framework

A top-down view of the IECSA Reference Architecture Framework

3.3 Business Needs – IECSA Environments Based on Industry Requirements

The energy industry's business needs were first captured as a set of power system functions, and then the steps of the functions were categorized by the type of information environment in which they were interacting.

3.3.1 Power System Functions

As part of the initial scoping activity of the IECSA project, over 400 power system functions were identified and briefly assessed for their information exchange needs and issues. After these 400 functions were reviewed, a few of them were selected as key functions for more in-depth analysis.

The power system experts within the IECSA team and a number of stakeholders outside the IECSA team developed detailed descriptions of these key existing and future power system operation functions, which were considered 'architecturally significant' in terms of having unique and/or complex information requirements. These functions were captured in narratives, diagrams, and detailed steps, using the concepts of the Unified Modeling Language™ (UML™[6]) which is the prevalent method for capturing and expressing the complex interactions of functions.

To achieve this first deliverable, the IECSA team created a list of all functions related to power system operations. This covered six 'Domain Areas' including: (1) Market Operations, (2) Transmission Operations, (3) Distribution Operations, (4) High Voltage Generation, (5) Distributed Energy Resources, and (6) Customer Services. Ultimately, more than 400 functions were identified at the very top levels. These functions were then assessed for key architectural issues, such as unique configuration requirements, stringent quality of service requirements, strong security requirements, and complex data management requirements. From these functions, a few key functions were selected, analyzed and evaluated in more depth, in order to understand the architecturally significant requirements in greater detail. Table 2 lists the power system operations functions that were analyzed in greater depth (see the Website and Volume II for more complete descriptions):

Table 2: List of Power System Applications analyzed in some detail

Some power system functions were thought to expose architecturally significant issues and were examined in more detail than others.

1. MARKET OPERATIONS
   a. Long Term Planning (Transmission and generation maintenance coordination, updating the power system model)
   b. Medium/Short Term Planning (Load forecast, outage scheduling, congestion management, long-term auction/sale of FTRs)
   c. Day Ahead Market (Auction/sale of FTRs, day ahead submittal of energy schedules, day ahead submittal of ancillary service bids, schedule adjustment of energy schedules, schedule adjustment of ancillary services)
   d. Real-Time (Operational calculations, real time submittal of schedules, real time submittal of ancillary services, normal dispatch re-dispatch/emergency dispatch)
   e. Post-Dispatch (Metering, market products schedule checkout, financial settlements, accounting and billing, market monitoring and auditing, transmission and generation maintenance coordination, updating the power system model, transmission operations)

[6] Unified Modeling Language and UML are registered trademarks of the Object Management Group, Inc.

2. TRANSMISSION OPERATIONS
    a. Automated Control Baseline
    b. Emergency Operations Baseline
    c. Wide Area Monitoring and Control Automated Control
    d. Wide Area Monitoring and Control Emergency Operations
    e. Wide Area Monitoring and Control Advanced Auto Restoration
    f. Advanced Auto Reclosing
    g. Synchrophasor
    h. Voltage Security
    i. Transmission System Contingency Analysis (Baseline)
    j. Transmission System Contingency Analysis (Future)
    k. Self-Healing Grid (across both transmission and distribution)

3. DISTRIBUTION OPERATIONS (INCLUDES SIGNIFICANT PENETRATION OF DER IN DISTRIBUTION SYSTEM)
    a. Data Acquisition and Control (DAC)
    b. Distribution Operation Modeling and Analysis (DOMA)
    c. Fault Location, Isolation and Service Restoration (FLIR)
    d. Distribution System Contingency Analysis (CA)
    e. Multi-level Feeder Reconfiguration (MFR)
    f. Relay Protection Re-coordination (RPR)
    g. Voltage and Var Control (VVC)
    h. Pre-arming of Remedial Action Schemes (RAS)
    i. Coordination of Emergency Actions
    j. Coordination of Restorative Actions
    k. Intelligent Alarm Processing

4. DISTRIBUTION OPERATIONS (INCLUDES SIGNIFICANT PENETRATION OF DER IN DISTRIBUTION SYSTEM)
    a. DER as Backup
    b. DER Operated by Aggregator

5. CONSUMER SERVICES)
    a. Real time pricing (RTP)
    b. Power quality monitoring (PQ)
    c. Customer communication portal (CCP)

3.3.2 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 7 and described in greater detail in Table 3.

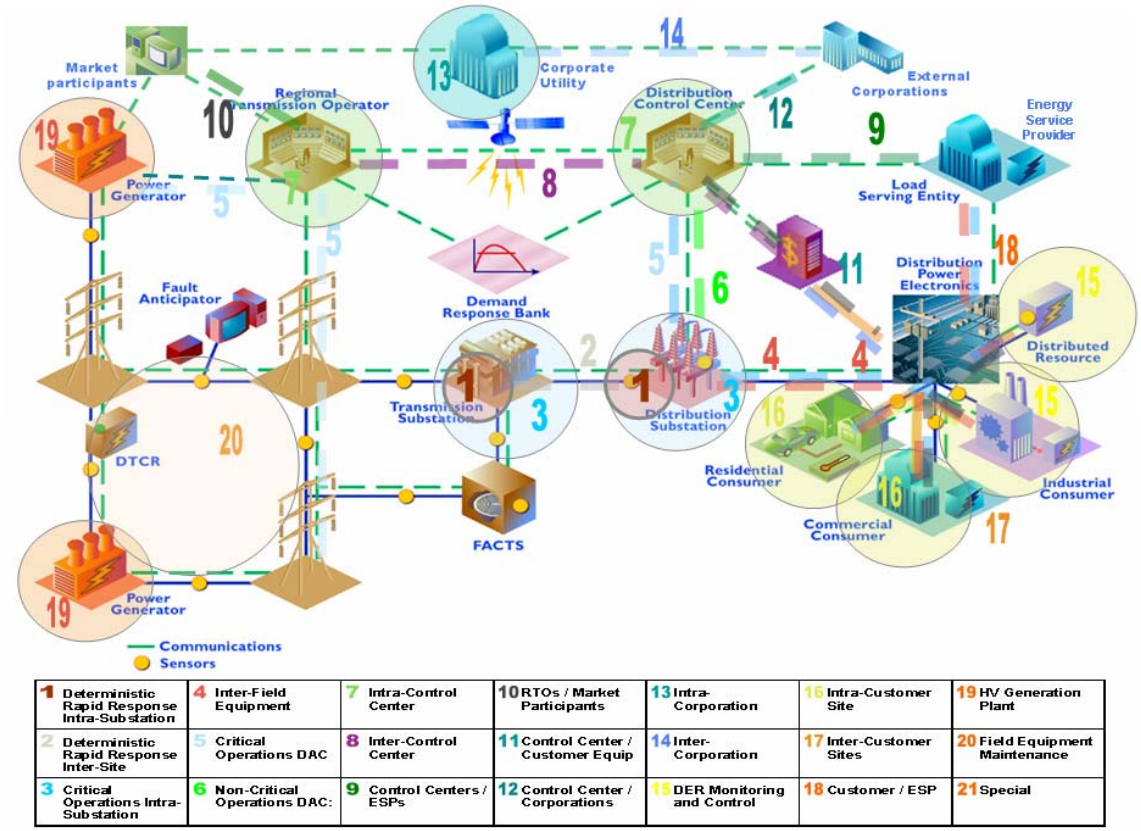

Figure 7: IECSA Environments in Power System Operations

The IECSA team observed 18 patterns of requirements that help distinguish the operational environments.

Table 3: Descriptions of each IECSA Environment.

Environment	Description
1. Deterministic Rapid Response Intra-Substation:	Deterministic, rapid response intra-substation environment (e.g. protective relaying, direct monitoring of power system parameters by current transducers (CTs) and PTs)
2. Deterministic Rapid Response Inter-Site	Deterministic, rapid response inter-substations and beyond substation (e.g. protective relaying, FSM)
3. Critical Operations-Related Intra-Substation	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)

Table 3: Descriptions of each IECSA Environment.	
Environment	Description
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 Plant	Within an HV Generation Plant site (e.g. within the electrical and physical 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.)

An example of a typical Substation Supervisory Control and Data Acquisition (SCADA) application spanning multiple IECSA environments is shown in Figure 8 below.

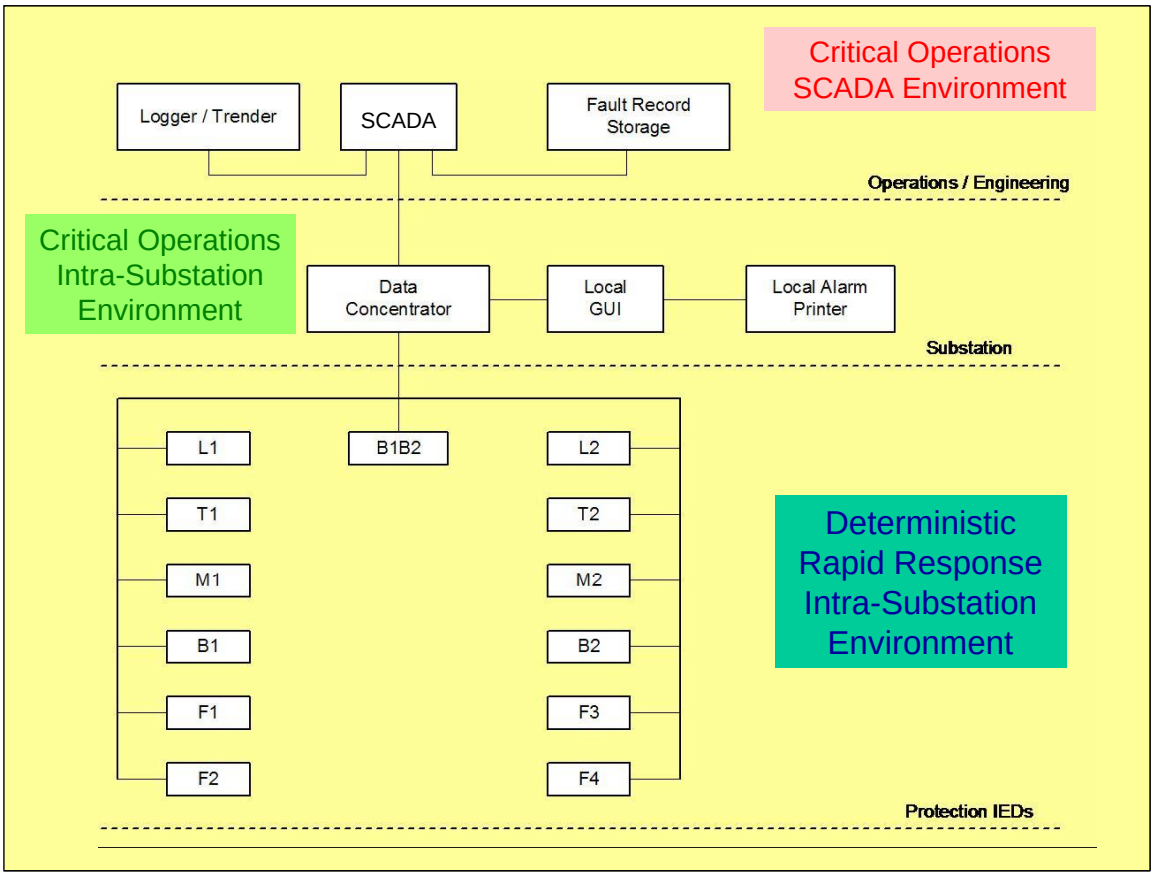

Figure 8: Typical Power System Substation Environments

A conceptual drawing of a typical substation SCADA environment helps articulate how typical power system operations span multiple IECSA environments.

3.3.3 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 were termed the 'aggregated requirements,' comprise the following:

1. 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

2. 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
3. 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)

4. 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

3.4 Strategic Vision Based on High Level Concepts

The strategic vision for the IECSA Reference Architecture reflects the ultimate objectives for a distributed computing infrastructure that can meet business needs, including configuration requirements, quality of service requirements, security requirements, and data management requirements. This strategic vision is based on:

- Abstract Modeling
- Security Management
- Network and System Management
- Data Management
- Integration and Interoperability

These strategic vision high level concepts are described in the following subsections.

3.4.1 Abstract Modeling

Modeling is one of the most powerful tools available for understanding, documenting, and managing the complexity of the infrastructures required to operate the energy system of the future. It is far less expensive to construct a model to test theories or techniques than to construct an actual entity only to find out that one crucial technique is wrong and the entire entity must be re-constructed.

Models have been used extensively by many industries as the basis to analyze and design complex systems. The telecommunications industries have made extensive use of modeling to develop the diverse communications infrastructure(s) in widespread use today. Physical models are used in many industries, ranging from airplanes and Mars Landers to circuit breakers and transformers. Building architects use paper models (blueprints) to capture all the complexity in a modern high-rise building. Virtual models are increasingly being used to model even more complex concepts, from weather patterns to cosmology and, of particular interest to the IECSA project, to information management. One can even make a simple abstract model of the IECSA Reference Architecture, see Figure 9 below.

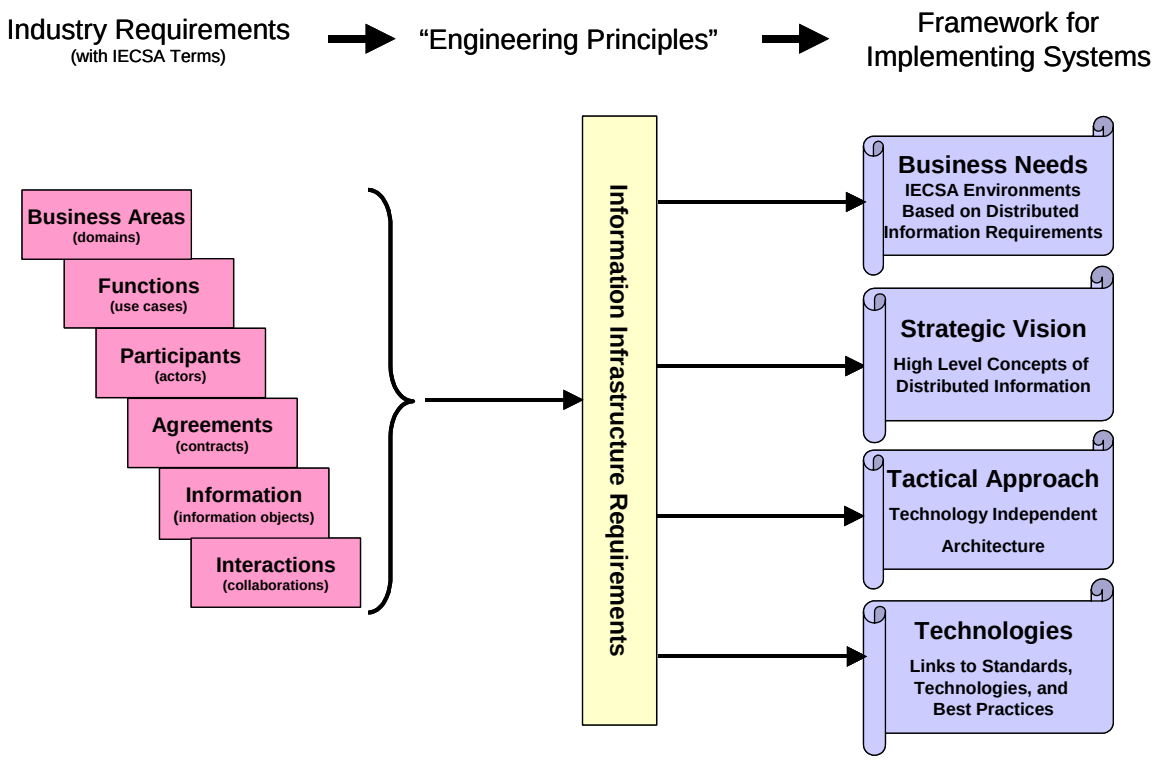

Figure 9: Abstract Model of the IECSA Reference Architecture

A simple abstract model of the IECSA Reference Architecture helps visualize what components and how they interact.

The following abstract modeling methodologies and concepts were incorporated into the IECSA Reference Architecture:

Reference Model for Open Distributed Processing and the Unified Modeling Language– Years of engineering have been invested in defining how enterprise level architecture should be defined. RM-ODP is an international standard (ISO/IEC 10746) prescribing a methodology for architectural development. The methodology provides guidance on breaking the problem into understandable pieces and helps to ensure that important design details are not forgotten.

By design, RM-ODP provides the methodology, but does not include a recommended notation for documenting an architecture. The most popular standardized notation for system modeling is the Unified Modeling Language (UML), which provides a standardized way to graphically document the systems and components of an architecture. Together RM-ODP provides the architectural guidance and UML provides the standardized notation. It should be noted that as of this writing, the standards for applying UML to RM-ODP concepts are under development. As the energy industry moves forward in the development of advanced automation systems, the adoption of these sophisticated methods should be encouraged.

Object Modeling and Information models define data names and structures. These information models can be described informally as consisting of nouns. Nouns consist of data names and their structure. Examples include simple data points such as a point called 'State' that consists of one 8-bit integer, as well as more complex data points that include the value, the quality of the value, the description of the point, etc. These nouns can also range to complete descriptions of a utility's power system, for example 'ABCPowerSystem', which consists of thousands of components in some well-known structure. There can be millions of nouns in any system.

In the power industry, IEC61850 includes such a model, which is focused on field device characteristics. Another information model is IEC61970 Common Information Model (CIM), which is focused on modeling **what** information about the power system structure is to be exchanged among application programs. It has been expanded to model other types of information to be exchanged among application programs. As an information model specifies **what** information is exchanged, it is part of an RM ODP information view.

Abstract Service/Interface Models –A **service** model describes the functionality that a software application provides. IECSA's Common Services describe common functionality needed to operate a utility. For example, the common service of 'LogOn' specifies the common function of initiating a secure session with a software application.

An **interface models** define the mechanics of how data is passed to get the right information to the right destination at the right time. These interface models can be described informally as consisting of verbs. Verbs are the abstract services used to exchange the nouns, such as 'request', 'send', 'report if changed', 'add to log', etc. Although different verbs/services are used in different environments, the number of different types of abstract verbs/services is generally on the order of 10 to 20.

In the power industry, IEC61850 includes such a model, which is focused on field device operation. Another service model is IEC61970 Generic Interface Definition (GID), which is focused on **how** information about the power system structure is to be exchanged among application programs. An interface model specifies **how** information is exchanged; it is part of an RM ODP Computational View.

Naming and avoiding ambiguity (name collisions)–One aspect of information models is the need to uniquely identify all objects within the model. In addition, as the number of names being used proliferates, there is a need to avoid 'name' collisions. That is the same name used with two different meanings. This is handled by namespace allocation. Namespace allocation is a very simple concept: different groups can have the authority to give names their own objects so long as those names are unique within the group's domain; however, they do not need to be universally unique. This permits different groups, whether they are whole industries, or standards organizations, or types of products, or a department within a company, to define their own terminology and abstract model names and structure.

Namespace allocation for the electric power industry should be performed in a top-down manner that clearly captures the different arenas. Although some namespaces should be as broad as possible (i.e., valid across the entire electric power industry), additional namespaces should be allowed as part of a formal scheme to permit specific utilities, specific vendors, specific functions, and other groups to apply for and register their own namespaces.

An example of namespaces within the IEC TC 57 is the allocation substations to the IEC61850 namespace and the allocation of transmission power system applications to the IEC61970 namespace.

Self-Description and Discovery–Future advanced automation systems must have more capable methods for managing networks, connected equipment and the applications that run on this equipment. This will require more sophisticated systems to assist system administrators in managing large scale networks and massively distributed equipment. Concepts such as self-description and discovery will become a necessary part of future systems or maintenance could easily become unwieldy.

Self-description and discovery is a fancy name for what happens when you plug a new printer into a PC: For example:

- 1st message: “New hardware detected”
- 2nd message: “Driver xxx is being installed”
- 3rd message: “Printer is ready for use”

Now, imagine a SCADA/EMS system performing equivalent actions:

- 1st message: “New RTU detected”
- 2nd message: “SCADA database being updated”
- 3rd message: “Data acquisition commencing”
- 4th message: “Power System Model being updated”
- 5th message: “Contingency Analysis is ready to execute”

Self-description and discovery form the basis for ‘plug-and-play’ technologies. The concept behind self-description and discovery is that data models can be stored electronically in repositories, servers, and other distributed databases, using a language for describing data such as XML. These XML descriptions of the data models are ‘self-describing’: they contain the standardized name of the data along with the structure and formatting of the data. Thus, they can be browsed by users who can immediately understand what they are browsing.

In addition, ‘discovery’ of these data models can be implemented by special applications (which could be called intelligent agents or metadata browsers) that ‘read’ the name and format of the data in the remote server (e.g., ‘New RTU’), set up their own local database (SCADA database) to reflect this name and format, then establish links so that the actual information can be read from the remote server and stored in the local database (Data Acquisition commencing).

Technology Independent Design–Using a technology independent design is an important concept when developing interoperable systems and equipment today. A technology independent design must focus on the behavior and structure of the components within a system and abstract the implementation details of any particular technology. This key concept allows for different implementations and technologies to exist, yet still allow these components to be used interchangeably. Using technology independent design enables a coherent architecture to be created independently of deployment specifics. When implemented, the technologies are chosen to meet requirements but are implemented in a way that complies with the technology independent design.

Some of the concepts derived from technology independent design are developed in more detail in the Tactical Approaches section.

3.4.2 Security Issues

Security is the second concept under IECSA's strategic vision. Security is one of the strongest drivers for applying architecture principles across the industry (see Volume IV Appendix A for an in-depth discussion of Security-related issues and technologies). The cyber security of advanced automation and consumer communications systems is one of the most important and challenging technical issues of our time. Increasing demand for information technology and reliance on advanced automation has created substantial challenges for system administrators as they try to keep their cyber systems secure from attack. Higher levels of integration across the industry and using open systems combine to raise the challenges of securing systems. Security policy implementation, a recommended practice, requires many of the concepts that architectures bring forward including system documentation, and structure.

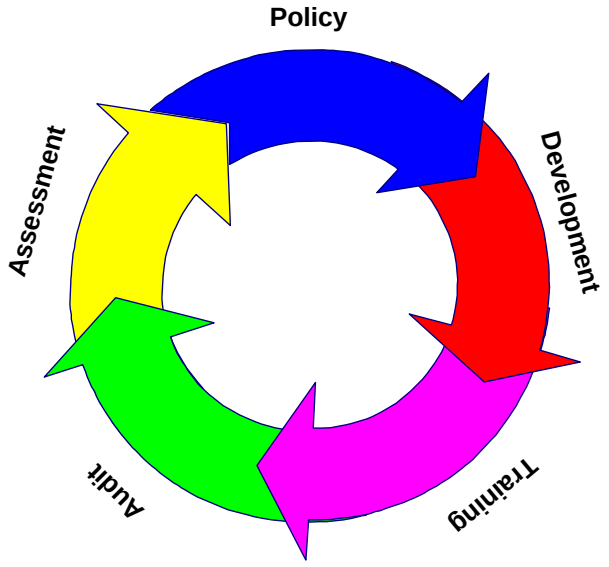

Figure 10: The Information Security Process

Security is one of the strongest drivers for applying architecture principles across the industry.

Cyber security encompasses a variety of functions for the next generation of distributed computing systems, including, but not limited to: developing and implementing security policies (for individual enterprises and the industry), threat and vulnerability assessments, system 'hardening' against intrusions, and managing the 'residual risk'.

The public electric power system is now characterized as among several critical infrastructures that must apply security practices more rigorously. This project has identified several stakeholder communities that are likely to increasingly put forward security requirements for energy system operations. Requirements from diverse sources are a part of the security approach taken by the IECSA project.

Security functions are also necessary to design into the architecture as well as the equipment that will comprise the next generation of advanced automation. Specifying security upfront is particularly important for small resource constrained devices that have limited computing resources. This is because security functions can drive minimum requirements for small equipment.

'Security by Obscurity' is no longer an acceptable solution in the electric power industry. Cyber-security has become a major issue for utilities due in part to the increased vulnerability of utilities as they network computer systems and power system equipment; this is also due in part to the competitive environment where crucial information (gathered legally or illegally) can translate into millions of dollars. Deregulation pressures and opportunities are encouraging the transfer of energy between increasingly distant business and operating entities, with energy flows varying dramatically as the price of energy fluctuates during the day and over the year. These market-driven fluctuations increase the complexity of congestion management, so that reliability requirements are demanding rapid and accurate information about the real-time state of the power system and the equipment that

monitors and controls it. In addition, the power system is increasingly required to respond as 'intelligently' as possible to abnormal or at-the-limit conditions.

Increasing numbers of customers are adding cogeneration and 'backup' distributed generation at their facilities, and selling back to the grid when the prices make it worthwhile. As the trend toward local generation increases, power systems will see increased and rapid fluctuations in power flows as marketers buy and sell energy and ancillary services from these local generators as well as from the larger generators. Only through rapid access to accurate and secure information from these diverse sources will the power systems continue to be operated reliably.

The public Internet is a very powerful, all-pervasive medium. It can provide very inexpensive means exchange information with a variety of other entities. The Internet is being used by some utilities for exchanging sensitive market information, retrieving power system data, and even issuing some control commands to generators. Although standard security measures, such as security certificates, are used, a number of vulnerabilities still exist. These vulnerabilities include inadequate security policies, inadequately enforced security policies, and lack of security countermeasures for different types of security threats (such as denial of service).

Not all data are equal when it comes to sensitivity to security threats. The key to assessing the sensitivity of data is to determine the impact, both financial and societal, on compromising its security, and to determine the risk of that compromise occurring. For instance, the financial and societal impact of eavesdropping on the meter readings of a single residential home is far less than the impact of issuing unauthorized breaker-trip commands to high voltage transmission lines. Therefore, the primary need is the assessment of financial and societal costs of different security vulnerabilities, along with the assessment of the financial and societal costs of implementing security measures. The IECSA security strategy is documented in Appendix A for those technologies that have identified the issues in their respective environments (e.g. IEC61850). The security strategy for other technologies/applications will have to be developed based on the requirements of the particular application and using the technologies and practices found in Appendix A.

3.4.3 System and Network Management Services

As can be seen in Figure 11 and Figure 12, two infrastructures must now be managed: the Power System Infrastructure and the Information Infrastructure. The management of the power system infrastructure is increasingly reliant on the information infrastructure as automation continues to replace manual operations, and is therefore affected by any problems that the information infrastructure might suffer.

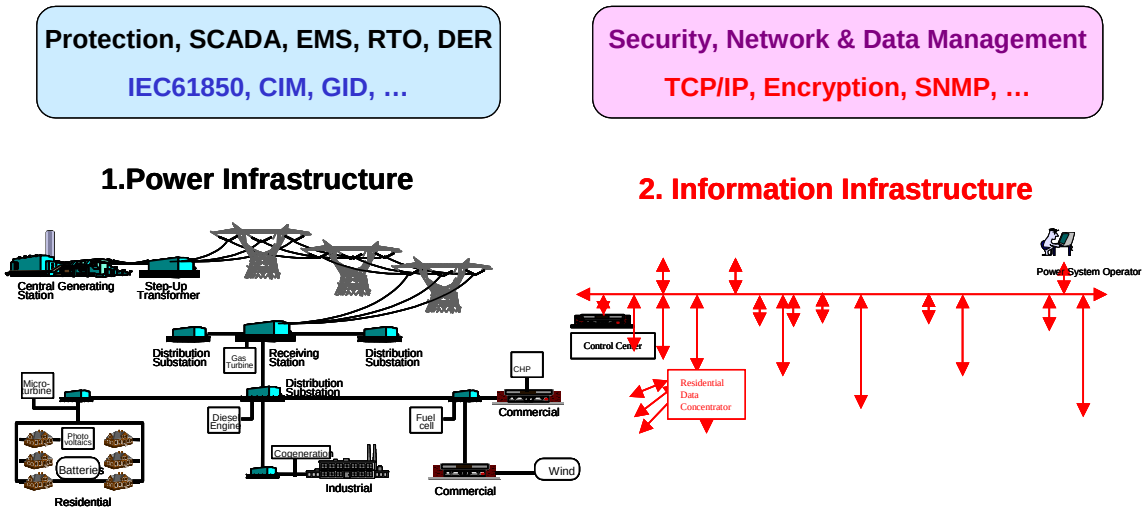

Figure 11: Two Infrastructures must be managed

Each of the two infrastructures has its own paradigms used for management.

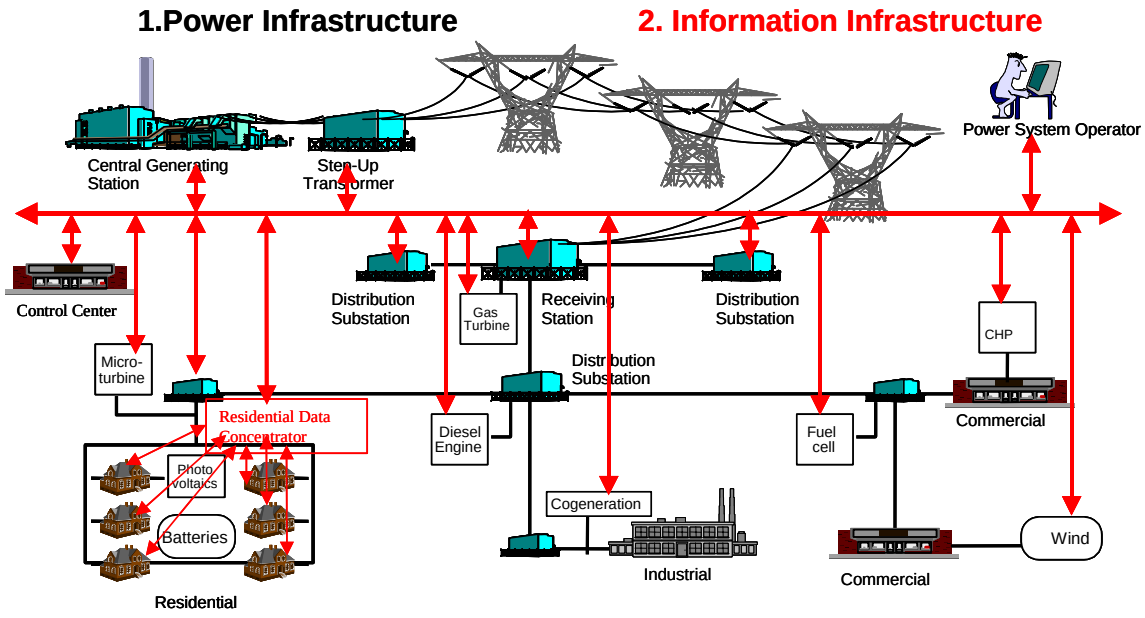

Figure 12: Power Infrastructure Relies on Information Infrastructure

Integrated Infrastructure Management

Both the Power System Infrastructure and the Information Infrastructure must be managed as an integrated whole.

Typical Simplistic Network Management by SCADA Systems–Electric power systems have been monitored and controlled by SCADA systems for many years. On the other hand, the information systems in the electric power industry have not been treated as a coherent infrastructure, but instead have been viewed as a collection of individual communication channels, separate databases, multiple systems, and different protocols.

Typically SCADA systems, in varying degrees, monitor whether communications are available with their (Remote Terminal Units (RTUs) and flag data as 'unavailable' if communications are lost. However, it is then up to maintenance personnel to track down the problem, which is a lengthy and ad hoc process. Every utility is different in the information available to its maintenance staff. Telecommunication technicians are generally responsible for tracking down any microwave or fiber cable problems; telecommunication service providers must track their networks; database administrators must determine if data is being retrieved correctly from substation automation systems or from GIS databases; protocol engineers must correct protocol errors; application engineers must determine if applications have crashed, have not converged, or are in an endless loop; and operators must filter through large amounts of data to determine if a possible 'power system problem' is really an 'information system problem'.

System and Network Management Vision–Network and systems management are those functions required to manage the communication networks and the connected communications equipment. Systems management includes managing remote equipment. These are functions a system administrator uses in managing the distributed computing infrastructure and connected equipment. The development of these functions is taking place both within and outside of the energy community.

In the future, the problem of network and systems management will become increasingly complex as a variety of systems are anticipated as well as greater demands on the capabilities of these systems to assist system administrators. Traditional SCADA systems will no longer have exclusive control over the communications to the field, which may be provided by telecommunication providers, or by the corporate networks, or by other utilities. Intelligent Electronic Devices (IEDs) will have applications executing within them whose proper functioning is critical to power system reliability. Field devices will be communicating with other field devices, using channels not monitored by any SCADA system. Information networks in substations will rely on local 'self-healing' procedures that will also not be explicitly monitored or controlled by today's SCADA systems.

The technology industry has developed two network management technologies: Simple Network Management Protocol (SNMP) for the Internet-based functions, and Common Management Information Protocol (CMIP) as an ISO standard. In each of these technologies, Management Information Base (MIB) objects must be specified representing the state of different equipment, applications, and systems. Although many MIB objects are generic enough to be used by electric power systems, some specialized MIB objects will need to be developed to represent some of the very specialized equipment used in power system operations.

Object Models for Network and System Management–Systems and network management functions are also supported by the application of object based communications. The IEC is currently working to develop network management objects for power system operations. In addition, the networking and telecommunications industries are working toward more sophisticated system administration infrastructures. Examples of possible types of network and systems management functions and objects for energy industry related IEDs are shown in Table 4 below.

Table 4: Possible types of networks and systems management functions.	
Possible types of network and system functions:	Possible responses or actions could include:
▪ Numbers and times of all stops and starts of systems, controllers, and applications ▪ Status of each application and/or software module: stopped, suspended, running, not responding, inadequate or inconsistent input, errors in outputs, error state, etc. ▪ Status of all network connections to an IED, including numbers and times of temporary and permanent failures ▪ Status of any 'keep-alive' heartbeats, including any missed heartbeats ▪ Status of backup or failover mechanisms, such as numbers and times these mechanisms were unavailable ▪ Status of data reporting: normal, not able to keep up with requests, missing data, etc. ▪ Status of access: numbers, times, and types of unauthorized attempts to access data or issue controls ▪ Anomalies in data access (e.g. individual request when normally reported periodically)	▪ Start or stop reporting ▪ Restart IED ▪ Kill and/or restart application ▪ Re-establish connection to another IED ▪ Shut down another IED ▪ Provide event log of information events ▪ Change password ▪ Change backup or failover options

3.4.4 Data Management Issues

Data management is one of the most difficult aspects of the information infrastructure. All too often a very carefully designed system that has been designed to provide excellent benefits to power system operations is ignored, or actually turned off, because the input data is just not accurate or available enough for the results of the function to be trusted – 'Garbage in; Garbage out'. Data management must address a complex set of issues, which include the following:

- Validating source data and data exchanges
- Ensuring data is up-to-date
- Managing time-sensitive data flows and timely access to data by multiple different users
- Managing data consistency and synchronization across systems
- Managing data formats in data exchanges
- Managing transaction integrity (backup and rollback capability)
- Managing the naming of data items (namespace allocation and naming rules)
- Maintaining database and data exchange
- Logging, reports, and audit trails

No single technology exists that can be globally applied to handle all of these data management issues, but increasing attention is being paid to develop 'best practices' and to promote various technologies that solve part of the data management problems. These efforts and technologies then form the vision for data management.

3.4.5 Interoperability and Integration Issues

Interoperability Goals–The ultimate goal of interoperability is to enable two independently developed devices to integrate their operations over a communications network. Interoperability has been defined as:

"The ability of two or more systems or components to exchange information and to use the information that has been exchanged"[7]

While the concept appears simple on the surface, the complexity of the systems or components requires a substantial amount of agreement in the way they interact. Even relatively simple levels of interoperability require not only adherence to standards and agreement on use of those standards, but technicians are also necessary to participate in setting up and configuring equipment. Higher levels of interoperability are a strategic goal for advanced automation systems and include capabilities to enable the equipment to participate in the management of the system. The concepts of 'Plug and Work' (or 'Plug and Play') require more sophisticated levels of interoperability. These capabilities enable you to plug in a new device, application, or system into an existing system, and the existing system automatically incorporates the new equipment. These levels of interoperability are strongly desired since it simplifies the human intervention required to manage systems. However, to achieve systems that are easier for humans to use requires a higher degree of internal sophistication. Interoperability and interworkability are terms that must be more tightly defined within the industry.

The goal of interoperable systems can be very hard to achieve in a diverse environment with many different requirements, many different vendors, and a wide variety of standards. Interoperability is particularly difficult where legacy systems prevent the use of more modern approaches. No one answer exists on how to integrate these older, less flexible systems, but the following technologies and best practices can help toward that interoperability.

- Using object and services modeling
- Using technology independent techniques
- Using 'Metadata'
- Using standards
- Using gateways and protocol converters

Key Points of Interoperability–An additional principlestates that while it is possible to standardize everything, it is also possible to end up with so many standards that ultimately there are no standards. Ultimately, there must be a balance between components of a communications system that are rigidly standardized, and, those that are fairly flexible to be pioneered by market participants -- vendors, customers, etc.

For example, the singular agreement on a 60Hz, 120 VAC electrical power system, and the physical shape of an AC wall outlet, made possible a diversity of products that use electricity in the United States. In the absence of such a well accepted standard, the growth of the appliance industry would have been hampered by the requirements of various power conversion adaptors and plug adaptors (as anyone knows who travels to other countries).

For IECSA, there will be an analogy between those key points of interoperability for power (60Hz, 120VAC, plug shape) that will be key to facilitating an explosion in goods and services that can interact using components referenced in the architecture. Some key points of interoperability are summarized below.

- **Manufacturing IDs**–Globally unique identifiers for the source of a component in a utility or other enterprise system.
- **Serial numbers**–Globally unique identifiers for instances of products.

[7] IEEE 610.12

- **Standardized object models**–Standardized object models with ‘well-known’ names and formats for exchanging data among disparate applications and systems.
- **Metadata representation**–Metadata is data that describes data. The term ‘Rose’ could be a persons name, a flower, a color or an acronym. Metadata is the term that describes what the word Rose refers to in a given application. Metadata is a powerful concept that can be used for embedded devices to exchange information and achieve higher levels of interoperability. . This ‘data’ that describes data permits users, applications, and systems to access or ‘browse’ the names and structures of object models in other systems as the key method for ‘data discovery’.
- **Internet and industry standards**–Using the Internet and other industry standards to take advantage of the effort used to develop them, the resulting decrease in prices, and the interoperability provided by them.
- **Time synchronization over a widespread geographic areas**–The ability to define a common mechanism to obtain a reliable global time synchronization for devices of any level of complexity

3.5 Tactical Approach Based on the Platform Independent Model

The Tactical Approach uses 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. To understand why this approach is important, consider the primary methods that have been used previously to achieve interoperability:

Islands of Automation - In the past, each system was developed by itself, with little or no thought given to interconnecting it with other systems. ‘Islands of Automation’ as they’ve been called, see Figure 13. With these islands of automation, if one system needed data from another, some programmer would develop an ad hoc protocol to link the two systems. This link was usually very simple but gave the programmer work for life, since only they could fix it whenever it crashed.

Database-Centric – A few years ago it became evident that this approach made these systems very difficult to maintain, and those vendors were finding it very expensive to expand and upgrade these systems. A new approach was needed. One tentative approach was to require all data to be exchanged through databases, see Figure 14. This simplified the problem of many different protocols by creating a single data exchange mechanism. Data could be stored in the database by one system, and other system could

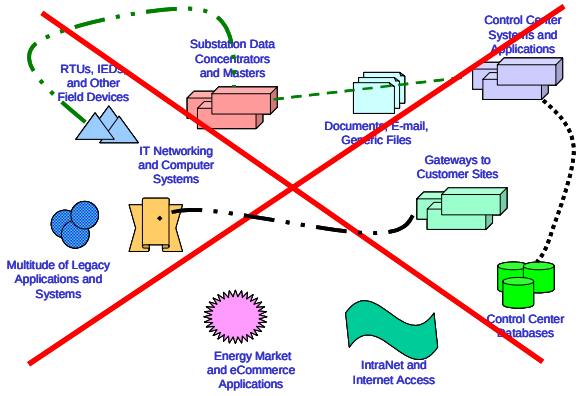

Figure 13: First Attempt:
Ad Hoc Proprietary Links as an After Thought.
This approach is too expensive.

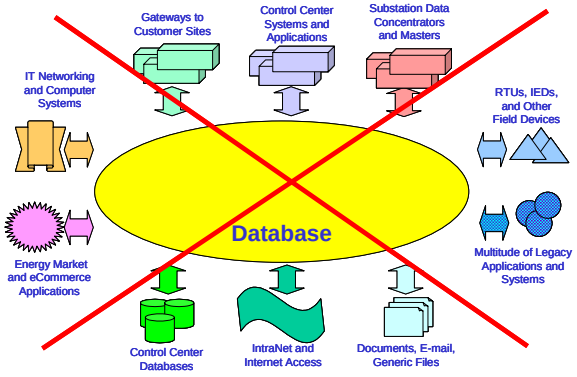

Figure 14: Next Attempt:
Database as Method to Exchange Data.
This approach is too inefficient.

retrieve the data at some different time. However, this architecture was recognized as being too brittle because changes to the database often necessitated changes in many related systems making maintenance very costly.

Platform Independent Model – More recently, more adaptable architectures have been developed. These architectures allow 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) is that former specification that is independent of any specific technology.

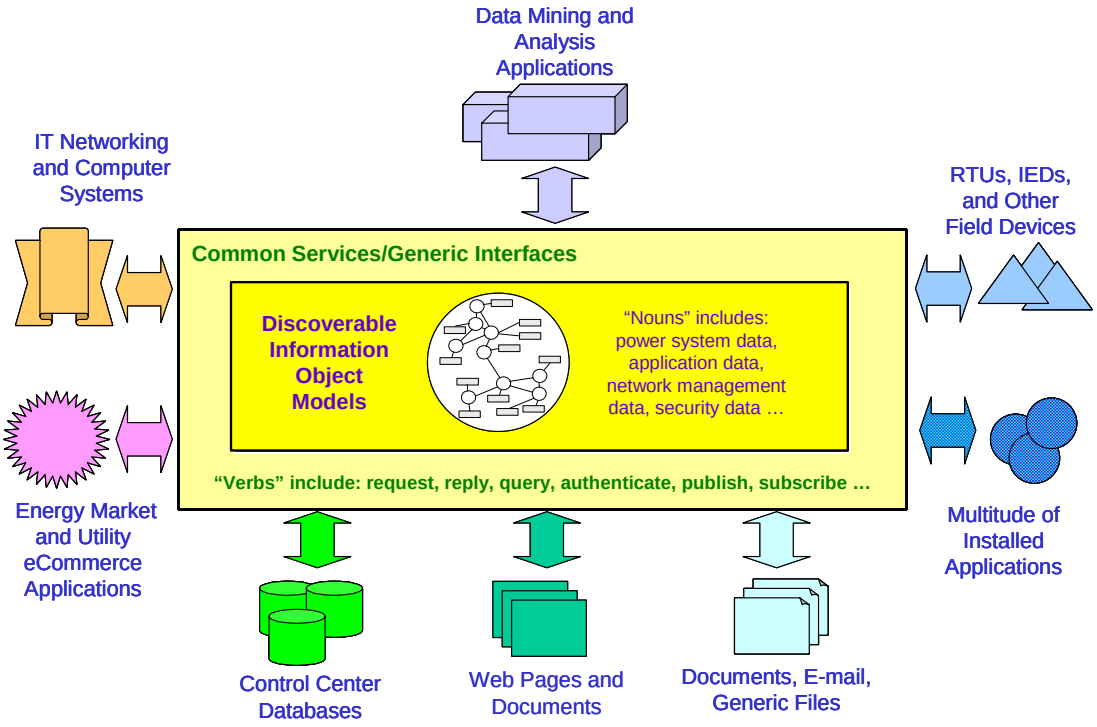

Figure 15: IECSA Platform Independent Model

Common Information Models, Common Services and Interfaces. This model manifests the desired technology independent features described in this section.

The IECSA tactical approach is based on these principles:

Development and Use of a Technology Independent Design for Communications–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.

Layered Technologies–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.

3.6 Standard Technologies and Best Practices

In the IECSA Reference Architecture Framework, standard, technologies and best practices are described, covering their basic capabilities, and, where relevant, their strengths and weaknesses with respect to specific requirements within specific environments. These standards, technologies, and best practices cover the industry-wide internet-based technologies, media-specific technologies, security countermeasures, network management solutions, system management practices, as well as existing power industry-specific standards and the many legacy technologies.

These standards, technologies, and best practices are categorized into the following groups. Detailed descriptions of each of these can be found on the IECSA website and in Volume IV, Appendix D. Additional information on Security is in Volume IV, Appendix A, and on Network Management, Volume IV, Appendix B and Volume IV, Appendix C.

3.6.1 Information Technologies

- Energy Industry Technologies. The electric power industry has developed standards and de facto technologies that meet their unique requirements. Although a few of these technologies may be replaced over time by more industry-wide technologies, most will continue to be used and evolved to meet specific needs. Many already utilize or plan to utilize the IECSA Reference Architecture Framework abstract object modeling, namespaces, and metadata repository concepts outline above. In some instances, standards do not exist, and only vendor-proprietary solutions are available at this time, particularly in the Automated Meter Reading arena.
- Information Industry Technologies. The ongoing development of the Internet has been a substantial source of advancement in networking and distributed systems development. It is important to distinguish, however, Internet-based technologies, such as TCP/IP and XML, from the use of the Internet itself. Using the existing Internet is an independent decision that should be consistent with system management and security policies from those organizations agreeing to use it. Internet technologies, and those emerging from the next generation Internet development work, can be used independently of existing Internet architecture. Internet-based technologies have become prevalent throughout most industries, and many, such as TCP/IP and HTML, are used almost to the exclusion of other equivalent technologies. Increasingly, web services are being seen as the wave of the future.
- Security Technologies. Security technologies have been primarily standardized through the ISO/IEC and the IETF for Internet-based security.
- Network and Enterprise Management. Network and enterprise management has matured in the corporate arena, but has not yet significantly penetrated the operations arena, where ad hoc solutions are more likely.

3.6.2 Best Practices

- Data Management Best Practices. Data management best practices describe techniques for handling data management issues that do not have any specific technology solutions, such as Data Validation, Management of Manual Data Entry.

- Security Best Practices. Security best practices identify the standards that specify methods or techniques that are important for security, such as Security Policies and Security Training.

3.7 Links between IECSA Environments and Technologies

The IECSA project team has taken project requirements input from a variety of sources and applied the tools and other analyses methods to arrive at project recommendations. Specifically, the team has identified relationships between stakeholder requirements and existing and emerging standards and associated technologies. The analyses and methods are described within the remaining three volumes and the associated appendices to the IECSA project. Most of the analyses are in Volume IV. Users of the IECSA Framework may judge the strength of the recommendations based on the team's analysis. It should be noted that while many of the existing and emerging standards and technologies address many of the requirements, there are none that comprise a complete standalone solution. Application complexity and the need for robust systems management and security means that the solution set will be comprised of necessary advancements to existing technologies or combinations of technologies.

Each of the IECSA Environments is linked to the appropriate standards, technologies, and best practices, based on the requirements of that Environment. In addition, these standards, technologies, and best practices are assessed as to how well they meet the IECSA High Level Concepts, as well as how appropriate they are for the specific requirements in each Environment. They are then labeled as:

- **Recommended**, if they meet most of the Principles, High Level Concepts, and the specific requirements of the Environment.
- **Alternative**, if they meet many of the Principles, High Level Concepts, and the specific requirements of the Environment.
- **Possible,** if they are less compliant with the Principles, High Level Concepts, and the specific requirements of the Environment, but are still feasible. Often these are legacy technologies.

In some cases, new technologies are incorporated into the IECSA Reference Architecture Framework not necessarily because they are better than what has been developed to date specifically for the electric power industry, but because the electric industry must follow technology trends from other industries where these are cost-beneficial and/or become part of industry-wide information technology strategies. In other cases, the electric power utility is just now getting into new areas, such as market operations, where the appropriate technologies are being defined elsewhere.

3.8 IECSA Website

The IECSA website (http://www.iecsa.org) contains all of the key information found in the four volumes, including:

- Overview and Guidelines, which consist of a set of pages that contain overview and guidelines information, taken predominantly from Volume I.
- IECSA Reference Architecture Framework, which contains the descriptions of the Business Needs, the Strategic Vision, the High Level Concepts, and the Tactical Approach, taken predominantly from Volume I.
- Power System Functions, which contains an organized set of descriptions and diagrams of the power system functions.
- IECSA Environments, which contains the 20 Environments, their defining requirements and their links to recommended technologies, services, and best practices.

- Technologies, Services, and Best Practices, which link to the descriptions of each of the technologies, services and best practices, taken predominantly from Volume IV, Appendix D.
- Detailed UML analysis of the Use Cases, which contains the results of the analysis of the Use Cases.
- Additional links such as to the Glossary

This page is intentionally left blank.

4. GUIDELINES TO UTILIZING THE IECSA REFERENCE ARCHITECTURE

This section describes how to use the IECSA Reference Architecture.

4.1 Audience

This section is designed for automation architects, power system planners, project engineers, information specialists, and system engineers who wish to understand how best to utilize the IECSA Reference Architecture, including the UML Model and the IECSA website. The specific objectives of this section are to:

- Describe how, and by whom, the IECSA Reference Architecture is expected to be used.
- Provide guidelines for using the electronic IECSA Reference Architecture UML Model and website.
- Provide an example of using the IECSA Reference Architecture website.

4.2 Using the IECSA Reference Architecture

The IECSA project has taken the first steps to frame an enterprise and industry architecture for future distributed computing systems. The framework includes both recommendations that can form the basis for system designs, as well as gaps and seams that were identified in existing infrastructure development. The IECSA Reference Architecture provides a documentation style and framework that is comprehensive for application development. IECSA includes a starting set of Use Cases for requirements, functionality, and nomenclature, and provides links from requirements to standards, technologies and best practices. In addition, IECSA includes in-depth discussions of the state-of-the-art of information engineering and technologies.

The IECSA Reference Architecture is a roadmap that can be used for many purposes by diverse groups of people. An industry and enterprise-level architecture primarily addresses issues related to enterprise integration, data and applications sharing across domains and the implementation of security and management policies. The issues addressed in IECSA are also concerned with integration with consumers and business entities outside of any given company. These issues are typically handled by systems architects, automation architects or systems engineers that may report to strategic corporate planners and chief information officers. The IECSA project results are also applicable to power system planners, power engineers and automation engineers to help define functional and information requirements for advanced automation systems and specific implementations in the near term. System engineers or system architects can utilize the IECSA models in the preparation of implementation specifications and in the systems engineering of actual applications.

IECSA provides several potential jumping off points for different types of users, for example, power system planners may work exclusively with the Use Cases, while project engineers and information specialists can select various environments to review. Specific uses include:

- **Power system planners and project engineers** will use IECSA to help define their functional and information requirements for specific, near term implementations
- **Automation architects and information specialists** - Chief Information Officers (CIOs),, vendors, and IT specialists will use IECSA to develop strategies and migration plans for long range objectives

- **System engineers or system architects** can utilize IECSA models to prepare implementation specifications and in the systems engineering of actual applications.

Individual user groups and their potential use of the IECSA Reference Architecture are depicted in Figure 16 and are discussed in more detail in the following sections.

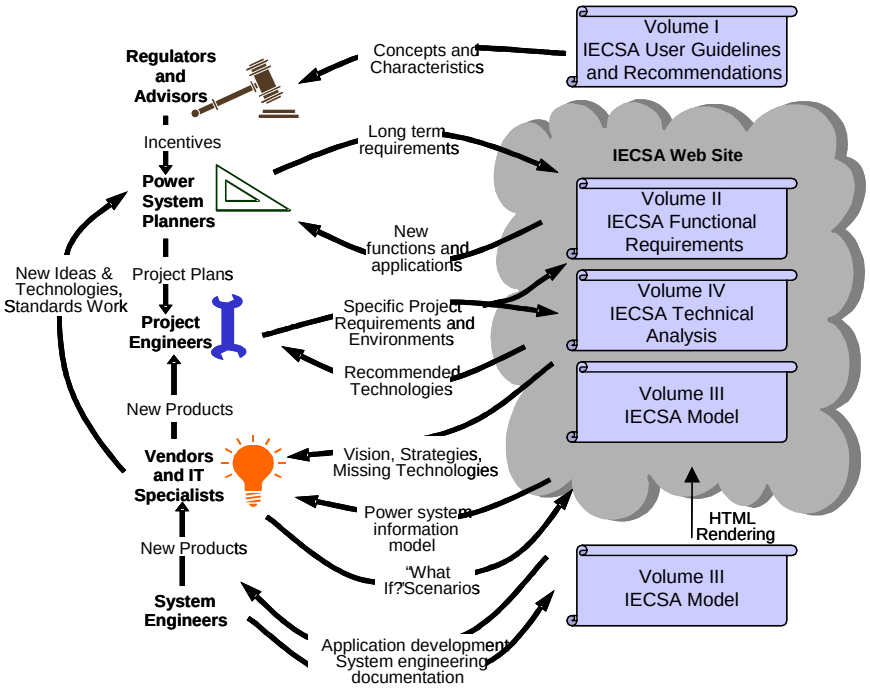

Figure 16: Ways the IECSA Reference Architecture can be used.

This drawing depicts the four major components of the deliverables set and suggests potential audiences for each along with suggested uses.

Note: It is obvious that the 2004 IECSA Reference Architecture will require continual expansion and upgrading to improve the set of Use Cases and to take into account new standards and technologies. It is therefore incumbent on all users of the IECSA Reference Architecture to indicate where expansion and upgrades need to be undertaken.

4.3 For Automation Architects: Using IECSA as Roadmap for Corporate Architectures

The actual UML model that represents the IECSA architectural components is a powerful tool for the industry to use in application development. This section illustrates how a system engineer might use the UML model directly in starting a project and generating initial concepts and documentation.

The IECSA Reference Architecture provides a set of 'standardized interface' blocks for rapid prototyping of potential Use Cases. Logical interfaces between components – devices, computers, networks, and operators – can be tried out using the integrated IECSA UML library. Logical inconsistencies in prospective applications can be quickly eliminated before lower level interfaces are planned. The IECSA UML library can also generate a maintainable set of documentation directly from the advanced tool set without additional authoring.

The most time consuming and expensive part of a project is starting it. IECSA gives a new development project a big step up by providing:

- A documentation style and framework that is comprehensive for application development
- A starting set of documentation for requirements, functionality, nomenclature
- Several potential jumping off points for the project. Based on IECSA functional elaborations, one may be selected that is close to the project at hand. This documentation can then simply be expanded and elaborated with additional or differing user requirements resulting in a rapid initial set.
- A set of standardized blocks for rapid prototyping of potential use cases. Logical interfaces between components – devices, computers, networks, and operators – can be tried out using the integrated IECSA UML library. Logical inconsistencies can be eliminated quickly before lower level interfaces are planned.
- The ability to generate a maintainable set of documentation directly from the advanced tool set without additional authoring.

4.4 For Power System Planners: Learning from Others' Experiences

Power system planners (transmission and distribution planners, protection engineers, substation engineers, control center engineers, etc.) are tasked with determining what new functionality is needed to improve power system operations for their utility or other companies. To undertake this task, planners must review their own needs, but can use the IECSA Power System Functions to get new ideas on how best to provide the functionality that they desire.

Power system planners can use the IECSA Power System Functions to investigate new power system functionality and can incorporate these power system requirements into functional requirements for near-term plans and longer term goals. These Power System Functions were intended to elicit architectural level issues within the domains so they do not have all the details necessary for system designs. However, the Power System Functions illustrate the extent of integration that is foreseen, as well as the sets of interrelated requirements that should be considered as future advanced automation and consumer communication systems are planned. These Power System Functions are presented in Volume II, and can also be accessed electronically through the IECSA website.

4.4.1 Review IECSA Power System Functions for Similar Functionality

Power system planners can review any IECSA Power System Functions that are similar to the power system functions in which they are interested. These Power System Functions can be found on ‘paper’ in Volume II, and ‘electronically’ in the IECSA website. In both the paper version and the web version, each Power System Function contains:

- A comprehensive narrative that describes the function in detail in plain language.
- A diagram of the interactions of the Power System Function.
- A sequence of detailed steps that analyzes each interaction of the function that involves the exchange of information.

  Each step indicates the event that caused the interaction, a description of the process triggered by the event, the source of the information, the recipient of the information, and a description of the information exchanged.

Each step also indicates in which IECSA Environment the interaction took place. These Environments provide the links to the standards, technologies, and best practices that are recommended, alternative, or possible.

In addition, the paper version and the detailed UML Use Case pages in the IECSA website contain:

- Contractual issues, regulatory issues, and other non-technical issues
- Abnormal sequences of steps if these are significantly different from the normal sequence
- Additional other Power System Function constructs, including Actors, Power System Function Diagrams, and Collaboration Diagrams

In the paper version, power system planners will use the table of contents to find the most appropriate Power System Functions. In the IECSA website, a power system planner can navigate from the IECSA website home page (see Figure 17) to the appropriate Power System Function using standard browser hyperlink techniques to jump from the IECSA home page to the Power System Functions overview page, and from there, using the lower left index frame, to the overview page of one of the six domains (Market Operations, Transmission Operations, etc.). From the overview page, the planner can select the desired Power System Function.

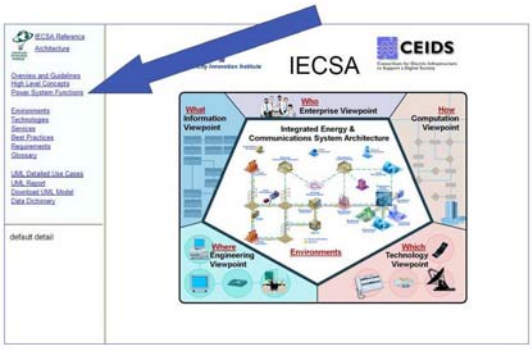

Figure 17: Jump to Power System Functions.

Each Power System Function Website contains the Narrative, along with pictures and diagrams, and followed by the Steps with links to the appropriate Environments. Some Power System Function websites contain multiple sub functions; some only contain one. A table of contents or sub-function links at the top of the page provide hyperlinks if more than one sub function is described.

4.4.2 Utilize Power System Functions to Expand Understanding and Provide New Ideas

Although no single Power System Function may completely reflect all requirements for a specific implementation, power system planners and architects can gain a significant understanding of the issues involved with implementing their function, can gain new ideas for improving this function either immediately or in the future, and can use this understanding to more succinctly define the power engineering requirements for the function that is to be implemented.

The power system planner should utilize the same Power System Function techniques to describe the function, as this provides the best method for ensuring the description is clear and complete. However, even without doing this, the power system planner can develop clearly defined functional requirements (which should normally not specify any specific technologies), and include a reference to one or more of the IECSA Power System Function as a means of clarifying these requirements.

Figure 18: Power System Function Narrative Table of Contents.

The power system planner then hands these functional requirements, along with the referenced Power System Function(s) to the project engineers, who may be 'in-house' or may be outsourced vendors who are

contracted to implement the function. (If the latter, the functional requirements would form part of a Technical Specification that would be used to contract with the selected vendor.)

4.5 For Project Engineers: Designing a System

Project engineers (project designers, implementers, project vendors, etc.) are responsible for implementing the information infrastructure that is needed to meet the functional requirements specified by the power system planners. Project engineers may be 'in-house' and work with the power system planners to define the information infrastructure requirements, and/or (more likely these days), they can be 'out-sourced' vendors and implementers who are contracted to implement the functional requirements described by the power system planners within a set of technical specifications. In either situation, the project engineers must be familiar with the specific requirements, not only for new functions, but also most importantly for all existing systems that the new functions must interact with.

Project engineers can use the IECSA Reference Architecture for a specific implementation project. These project engineers will utilize the Power System Functions identified by the power system planners to determine the detailed requirements associated with each step or 'environment' of the power system functions. These environments link to the appropriate IECSA website that describe the Platform Independent Architecture as well as recommended standards, technologies, and best practices for providing the information infrastructure needed by these power system functions. The IECSA website also identify alternatives and possible solutions for each type of interface, thus providing choices to the project engineers. Since different implementations will always have different constraints, existing legacy systems, and corporate policies, the project engineers will be able to review this range of solutions and select those solutions which best match the unique needs of their implementation.

A key thing to keep in mind is that project engineers cannot simply require vendors to 'comply with IECSA'. This is too broad a statement, since the IECSA Reference Architecture is a *reference*, not a specification. Instead, project engineers should include the IECSA Platform Independent Model as a template that they wish vendors to adhere to and may also select the appropriate standards, technologies, and best practices from this reference.

4.5.1 Review Power System Function 'Steps' and Associated Environments

Having received the technical specifications from the power system planners, the project engineers review the functional requirements and referenced Power System Function. They review either the paper or IECSA Website version of the Power System Function, identify the appropriate Power System Function steps that apply to the functions, and note the IECSA environments are associated with each of these steps.

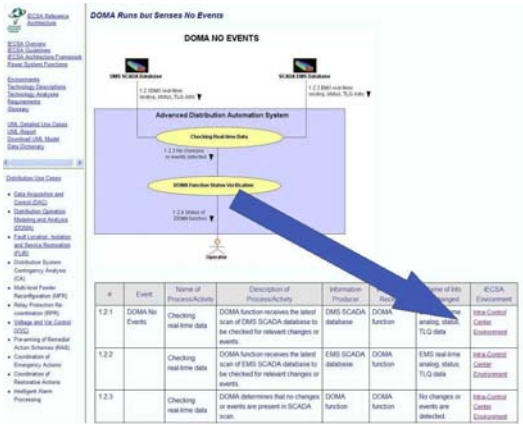

Figure 19: Power System Function Steps with links to IECSA Environments

These IECSA environments are the key methods by which project engineers can utilize the IECSA Reference Architecture. Each IECSA environment, which represents the information infrastructure requirements of the business needs, links to the three information infrastructure constructs of the IECSA Reference Architecture Framework (as shown in Figure 19). These constructs are:

- Strategic Vision and High Level Concepts
- Tactical Approaches
- Standards, Technologies, and Best Practices

4.5.2 Review IECSA Reference Architecture Framework

The IECSA Reference Architecture Framework, and the underlying Strategic Vision, High Level Concepts, and Platform Independent Architecture are relevant for all IECSA Environments. These concepts provide the goals toward which all project implementations should to head over the long term, and are therefore vital to understanding the recommendations made in the IECSA Reference Architecture.

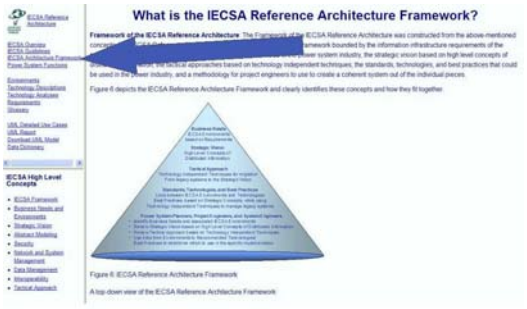

Figure 20: IECSA Strategic Vision

The overview of the Strategic Vision and Tactical Approaches are found in Volume I, Section 3 in the paper version, and can be jumped to from the IECSA website home page as seen in Figure 20. A more detailed discussion of the technical issues related to the architecture can be found in Volume 4.

4.5.3 Link to IECSA Environments

Project engineers can review key requirements associated with each relevant IECSA environment. These key requirements are discussed in Volume I, Section 3, or are available on the IECSA website through the IECSA Home Page as seen in Figure 21. Analysis of requirements appears in Volume 4 during the derivation of the IECSA Platform Independent Architecture. The description of the IECSA Environments contains:

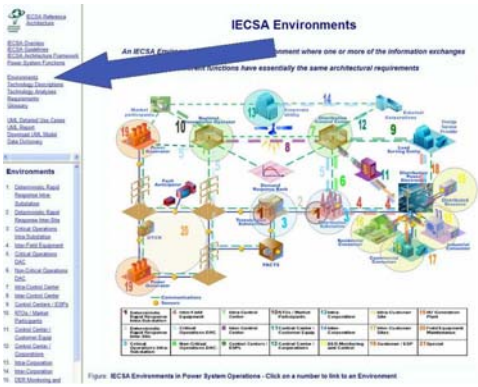

Figure 21: Environments

- Discussion of the characteristics of the environment
- The requirements that define the environment
- The recommended technologies, services, and best practices
- The alternative technologies, services, and best practices
- The possible technologies, services, and best practices

4.5.4 Requirements that Define Each Environment

Each IECSA environment description includes the list of requirements that defines it. This description can be found in Volume IV, Appendix D and on the IECSA website as can be seen in Figure 22. The Project Engineers should review these requirements to ascertain which may be the more important for the particular project they are working on. This prioritization can help them determine what decisions to make on the various standards, technologies, and best practices that are associated with the Environment.

Figure 22: Requirements for Defining Environments

4.5.5 Platform Independent Model

Project engineers can see the Platform Independent Model, either by browsing the IECSA Architecture website or by reading the IECSA Volume 4 document. Project Engineers need to promote a clear boundary between application requirements and the choice of specific technologies. Achieving a technology independent design for how to implement a system provides guidance to implementation engineers and achieves a level of interoperability, while still affording the flexibility that implementation engineers require to meet project goals and constraints.

4.5.6 Technologies, Services, and Best Practices for Each IECSA Environment

Project engineers can see the list of standards, technologies, and best practices associated with a particular environment, either by scrolling down the IECSA environment web page or by manually looking up the list in the paper version. From the IECSA website, this list links directly to brief descriptions of the standards, technologies, and best practices.

At the same time, project engineers will need the flexibility to use alternative technologies for specific implementations, due to existing legacy systems, existing vendor products, time constraints for implementation, financial constraints, company policies on technology choices, and a variety of other factors.

4.5.7 Recommended, Alternative, and Possible Solutions

It is for this reason that environments point not only to 'Recommended' standards, technologies, and best practices, but also include 'Alternative' and 'Possible' solutions as seen in Figure 23.

Recommended solutions are those that mostly meet the Strategic Vision High Level Concepts and are easily interfaced with using the Tactical Approaches.

Alternative solutions - those technologies that "mostly" meet the IECSA vision

Possible solutions - those technologies that don't adhere to the IECSA vision but functionally meet the requirements.

Figure 23: Recommended Standards, Technologies, and Best Practices

These distinctions are based on expert opinions and often fall into 'gray' areas where one alternative solution may be better than another alternative solution under different circumstances, and vice versa,

while a possible solution may still be the only available solution due to the availability of vendor products, legacy systems, or one-of-a-kind implementations.

Project engineers should review the recommended solutions and use those if feasible. Sometimes there may be more than one recommended solution for the same requirement. This stems from the fact that one solution cannot possibly meet all needs. For instance, specific implementations must take into account legacy systems, corporate policies, and financial situations. Given this, the recommended solution may not be acceptable for a specific implementation. Or one solution can partially meet a requirement, but requires another solution to meet the requirement completely. If no recommended solution is feasible for a particular requirement, then a migration plan should be included in the specifications to indicate how the recommended solutions could be achieved at a later date.

Project engineers can use alternative solutions that best meet the specific requirements. Possible solutions should be avoided unless no other solution is feasible.

4.6 For Information Specialists: Envisioning New Technologies

Information specialists are defined in this context as those vendor engineers, IT specialists, CIOs, and corporate strategists who are responsible for longer term goals, such as product planning, IT planning, development of future systems, research into new technologies, and future power system operations strategies. These information specialists are not responsible for a particular implementation, but instead envision the future systems and develop migration strategies to reach longer-term goals.

Information specialists would focus (in the context of this document) on developing strategies and migration plans for long range objectives. They can review the UML models, described in Volume III, and study the detailed engineering descriptions, in Volume IV, to better understand information engineering concepts and strategies, and thus plan the migration path to future systems and products along the common roadmap. Information specialists are also most likely to review the gaps in technologies identified in the IECSA projects, and then contribute actively to develop the standards or other solutions to close up these gaps.

4.6.1 How to Design Products Using the IECSA Reference Architecture

For vendors, the most time consuming and expensive part of developing future products is determining what objectives must be met and what future technologies are best to use. The IECSA Reference Architecture provides such a project a big step up by providing a roadmap to the future information infrastructure. In particular, information specialists can use the Strategic Vision and the High Level Concepts to plan long range objectives, and then review the Tactical Approaches, described in Volume 4, for determining the best paths for migration from older systems and to create interoperability between systems from different vendors.

Although the term ‘vendor’ is normally associated with external companies selling products to other companies, in reality any department or group that is developing products for any other internal or external clients can be seen as a vendor. Therefore, this product design strategy is as important to internal product developers as it is to external vendors.

4.6.2 How to Develop a Corporate Long Term Strategy Using the IECSA Reference Architecture

CIOs corporate IT specialists, and other corporate planners involved in the flows of information can use the Strategic Vision of High Level Concepts from the IECSA Reference Architecture as a guide to develop long range goals. These specialists can also use the Tactical Approaches as key methods for developing migration plans for their corporations.

4.6.3 How to Contribute to the Evolution of the IECSA Reference Architecture

The IECSA Reference Architecture cannot be a static document. Instead, IECSA must be a living, expanding, and evolving Reference Architecture that takes into account new requirements and technologies as they appear. Information specialists will be particularly able to point out these new developments and recommend updates to the Reference Architecture.

Information specialists are also in an excellent position to review and understand the gaps in standards and technologies identified in the IECSA project. These specialists can then be active in developing standards, technologies, and other solutions to fill these gaps.

4.7 For Regulators and Advisors: Building the Grid

The next type of IECSA user includes people who influence the future of the power system through legislation and their advisors. Regulators can use IECSA as a tool to ensure that the power system develops as an integrated, reliable whole rather than a set of unstable, loosely connected islands. The project also brings to the surface R&D issues related to the technologies necessary to move the industry forward. These details are provided in Volume IV Appendix D of this series.

4.7.1 How to Regulate Using IECSA

It is important that legislators, regulators, and their technical consultants read and understand the concepts presented in the User's Guide (this volume, Volume I). The key items for a regulator to understand about IECSA include:

- IECSA encourages a vendor neutral approach for advancing automation and consumer communication systems. The approach taken within the IECSA project is one of developing and assisting the maturity of open systems as a viable approach to building a public infrastructure.
- IECSA encompasses emerging requirements that are important to the management and security of public infrastructure.
- IECSA is not a single technology. It starts with a 'backbone' common data model, common services and a set of generic interfaces, but the IECSA system will also include many other protocols and technologies that have gateways or 'wrappers' to connect them to the backbone.
- IECSA will be customized for each utility. Not all utilities perform the same services to their customers; therefore, not all utilities should implement every portion of IECSA.
- IECSA should be deployed gradually, with migration plans to ensure that connectivity and interoperability are maintained throughout the deployment process.
- IECSA will involve process changes for utilities. Especially in the area of enterprise management and security, deploying IECSA will require significant changes to the way utilities operate. Many of the 'technologies' recommended by IECSA are actually behaviors and best practices for organizations.
- IECSA addresses life-cycle system costs and encourages a systems engineering approach**.** In the medium to long term, the approach of moving to open systems and effective life-cycle management will pay for the investment in the initial efforts to implement such an approach.

Examining this list shows that using IECSA has much in common with the science of quality management. It may be that the way regulators can approach the implementation of IECSA is similar to that of the ISO 9001 quality standards: this set of documents defines a core 'reference architecture', but each utility will implement it in a different way.

4.7.2 How to Evaluate IECSA-Based Networks

It is anticipated that consultants and service organizations within the power industry will begin to offer IECSA audit or evaluation services. To accomplish this job, the evaluator must be familiar with the entire IECSA document set. The definition of a detailed evaluation process is beyond the scope of this project, but an important recommendation listed in Volume IV. The key questions an evaluator must ask in such a process are:

- Has the organization made use of a common object model, common services, and generic interfaces (i.e. the IECSA 'backbone')?
- Is the organization using technologies recommended by IECSA, in the environments recommended by IECSA?
- Are the architects of the organization familiar with IECSA strategies with respect to infrastructure, security, data management, and enterprise management?
- Are the technologies being used either the same as those of the organization's business partners, or being translated through gateways?
- If gateways are used, are the common object model and semantics preserved across organizational and technology boundaries?
- Is the architecture deployed in all areas of the organization?
- Has the organization made the process changes needed to support the architecture?
- Are migration plans established in areas where the answers to the previous questions are 'no'?
- Is the organization participating in the process to improve and implement missing technologies required to establish IECSA?
- Is the organization providing feedback to the IECSA database to improve the quality of the IECSA models?

4.7.3 How to Develop a Migration Plan

Regulators must recognize that organizations will not deploy IECSA all at once throughout their networks; therefore migration plans must be in place. A strong migration plan will be based on the recommendations presented in Volume IV, which can be accessed through the IECSA website. The steps required to develop such a plan are as follows:

1. Choose the IECSA environment that most closely matches the area of the organization that is the focus of the migration plan.
2. Examine the Platform Independent Model and determine where data from this environment should be mapped into the model. The goal here is to develop a migration plan that can achieve interoperability without necessarily requiring specific technologies. Separation of design decisions from implementation decisions such as technology provides maximum flexibility and extensibility in the face of varying business conditions.
3. Select appropriate technologies to implement the Platform Independent Model from the list of recommended technologies for that environment.

4. Examine the discussion on that technology to identify any areas that be lacking with respect to the IECSA Platform Independent Model. Deploy technology or processes to address these concerns.
5. Develop a migration strategy to implement the new technology. Typical strategies include:
   - Installing gateways to convert one technology to the other.
   - Simultaneously using both old and new technologies as older devices or links are phased out.
   - 'Forklifting' all links and devices in selected parts of the environment where cost and environment boundaries permit.
6. Establish links between the new technology and the IECSA based integration infrastructure.
7. Develop training plans to alter the organization's processes to make use of the system.

4.8 For Standards Developers: Responding to the IECSA Recommendations

The IECSA Project has identified a number of 'gaps' in existing standards and technologies. Members of standards bodies and other interested parties should therefore use the IECSA Reference Architecture to determine how best to close these gaps and develop linkages between technologies. These proposed solutions should be actively encouraged and discussed by the various users of the IECSA Reference Architecture to ensure a consistent and complete resolution.

At the same time, the IECSA Reference Architecture must be constantly updated to reflect changes in requirements and technologies.

IECSA provides a loose, but specific, framework illustrating the boundaries adjacent to individual standards efforts. By taking note of these boundaries, standards organizations can tailor their fit at these boundaries. This is possible without sacrificing or altering the requirements of the specific standard, while allowing the results to be easily integrated into a multi-application domain whole.

4.9 Example – Protection Engineer to Review and Modify Protection Settings

Among the many potential IECSA uses, this section presents but one example, in some detail, to illustrate how one can obtain benefits from IECSA.

4.9.1 Statement of the Problem – Protection Planning Engineer

A protection engineer wants to review fault recorder information and modify settings in a protection device in a substation. She currently uses a dial-up modem from her workstation (which is connected to a modem bank through the corporate network) to the substation to review the information, but then must physically travel (or send someone) to the substation to modify the settings. This system has been in place a number of years and has worked reasonably well. However, the engineer has been told that all dial-up modems must be eliminated due to security concerns. Also, as staffing has been reduced, traveling to the substation herself, or sending someone, must be minimized. What to do?

The protection engineer goes to the Power System Functions on the IECSA website (or the Use Cases narratives in Volume 2) and finds a function (Transmission Operations – Automated Control Baseline) that is similar to her situation. She does note some differences, however. First, the Automated Control function assumes that protection devices can be accessed through a 'substation master', but in her situation, each protection device must be accessed separately. She is also aware that most of the protection devices are not configured to allow remote updating of settings (for security reasons), while the function assumes remote updates can be made. While this function is therefore not a perfect solution for the engineer, it is a strong start.

4.9.2 Engineering the Solution – Project Engineer

The protection engineer goes to the project engineer for help in the next steps. She shows him the Automated Control function on his computer by linking to the IECSA website and quickly jumping to the appropriate page. She explains what she needs and now it is similar but still somewhat different from the description of the function.

The project engineer quickly scrolls down to the Steps section of the Automated Control function and starts reviewing the steps until he finds the step that is closest to the problem she has identified. Scanning over to the Environments column, he realizes that the closest IECSA Environment to what she needs is the Critical Operations Intra-Substation Environment. He clicks on the link in the step.

4.9.3 Requirements

The Automated Control function's requirements have identified the following as key requirements which links to the Critical Operations Intra-Substation Environment:

- Configuration Requirements
  - Provide point-to-point interactions between two entities
  - Support peer to peer interactions
  - Support interactions within a contained environment (e.g. substation or control center)
- Quality of Service Requirements
  - Provide high speed messaging of less than 1 second
  - Support very high availability of information flows of 99.99+ (~1 hour)
  - Support time synchronization of data for age and time-skew information
- Security Requirements
  - Provide Authorization Service for Access Control (resolving a policy-based access control decision to ensure authorized entities have appropriate access rights and authorized access is not denied)
  - Provide Information Integrity Service (data has not been subject to unauthorized changes or these unauthorized changes are detected)
  - Provide Audit Service (responsible for producing records, which track security relevant events)
  - Provide Credential Renewal Service (notify users prior to expiration of their credentials)
  - Provide Security Policy Service (concerned with the management of security policies)
  - Provide Single Sign-On Service (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 Security Discovery (the ability to determine what security services are available for use)
- Network and System Management Requirements
  - Provide Network Management (management of media, transport, and communication nodes)
  - Provide System Management (management of end devices and applications)
- Data Management Requirements
  - Support the management of large volumes of data flows

- Support keeping the data up-to-date
- Support extensive data validation procedures
- Support specific standardized or de facto object models of data
- Provide discovery service (discovering available services and their characteristics)
- Provide conversion and protocol mapping

4.9.4 IECSA Reference Architecture High Level Concepts

These requirements link to a number of recommended technologies, services, and best practices that are based on the IECSA Reference Architecture High Level Concepts. Therefore, the project engineer first reads through the IECSA Reference Architecture High Level Concepts by clicking on the different topics under 'IECSA Architecture Framework'. These topics include:

- Abstract modeling
- Security services, risk assessment, and policies
- System and network management services
- Data management issues
- Integration and interoperability

The project engineer notes that they have been advocating object-oriented approaches for a few years, but has run into 'legacy system' issues and lack of management support that have prevented him from moving forward in that direction.

4.9.5 Platform Independent Model

The project engineer should understand how the high level concepts are realized in a technology independent way. While the exact technology used to implement the architecture may vary from vendor to vendor or over time, the Platform Independent Model provides continuity to ensure that a unified approach is maintained. Additionally, the Platform Independent Model provides for a level of interoperability that cannot be achieved via just the specification of high-level concepts and technology.

4.9.6 Recommended Technologies, Services, and Best Practices

Next, he examines the technologies identified as recommended and alternative solutions for the Critical Operations Intra-Substation Environment. These recommended technologies and alternative solutions include the following (in part).

- Energy Industry-Specific Technologies
  - ISO 9506 MMS–Manufacturing Messaging Specification - Configuration, Quality of Service,
  - IEC61850–Substation Automation Communications - Configuration,
  - IEC61850 Part 7-2–GSE (GOOSE and GSSE - Configuration, Quality of Service,
  - IEC61850 Part 7-2–SMV (Sampled Measured Values) - Configuration,
  - IEC61850 Part 7-2–Abstract Common Services Interface (ACSI) - Configuration, Quality of Service, Data Management
  - IEC61850 Parts 7-3 and 7-4–Substation Object Modeling - Network Management, Data Management
  - IEC61850 Part 6–Substation Configuration Language - Network Management, Data Management

  - IEC61850 Power Quality Object Models - Data Management
- Security Functionality
  - FIPS 197 for Advanced Encryption Standard (AES) - Security,
  - Role-Based Access Control - Security,
  - FIPS 186 Digital Signatures Standard (DSS) - Security,
  - Intrusion Detection Technologies - Security, Network Management,
  - Intrusion Prevention Systems (IPS) - Security, Network Management,
  - Service Level Agreements (SLA) - Security,
- Network and System Management Functionality
  - Simple Network Management Protocol (SNMP) - Network Management,
  - IEC 62351-7 Objects for Network Management - Quality of Service, Network Management, Data Management

The project engineer has heard of AES but isn't really sure what it is and where it stands in terms of being implemented by vendors. IEC61850 is just a number and he hasn't a clue what it is. He is quite familiar with SNMP, but has never heard of it being used within a substation. This intrigues him, because he has been under increasing pressure from the IT department to implement Internet-based technologies. If it really pans out that SNMP could help him solve her problem, then he will have killed two birds with one stone.

4.9.7 Use of UML to Develop Specific Use Case

However, spurred by the IECSA Reference Architecture concept of using UML for abstract modeling of functions, and with the help of one of his IT colleagues, he reviews the UML diagrams of the Automated Control function by going to the detailed UML-based Use Case links on the IECSA website, and finding the detailed analysis of the Automated Control Use Case. He creates a similar one that reflects the situation in his utility and the specific needs of the protection engineer. He reviews this with the protection engineer who, after adding some more details, agrees that conceptually it meets her requirements. But the question of *how* has still not been resolved.

4.9.8 Use of Environments to Determine Solutions

The project engineer now delves into the technologies, services, and best practices that were associated with the IECSA Environment. Ultimately he decides to:

1. Recommend using VPNs between the corporate network and the substation router, along with very strict role-based access control, passwords, and a strongly worded and enforced security policy. This will allow protection engineers to have direct access to the substation equipment again, now that the modems have been taken out.
2. Recommend the time synchronization of all substation protection devices using GPS devices. However, other devices can be time synched using the SNTP protocol.
3. Recommend using IEC61850 for all new protection IEDs, but with dual ports so that the SCADA system can continue to receive its data from the protection IED via DNP. This approach will provide protection engineers with more information, more accurate timestamp information, and more easily maintained data management.
4. Recommend that all data, including IEC61850 objects and CIM-based objects, use XML schemas to represent their metadata. This approach would permit protection engineers to browse the XML-

structured metadata objects, pick the information of interest, and have this data automatically included in their access list (if permitted under the security access control).

5. Recommend the implementation of data 'brokers' using the publish/subscribe service to update databases. These brokers will manage data across multiple networks, thus ensuring that key data is consistent across all databases. This data management system would include backup systems, automatic update of databases if they were off-line, roll-back of data if warranted, and other tools for managing data.

4.9.9 Architecting for the Future – Automation Architect

After the project engineer completes his tasks in supporting the protection engineer, he sets up a meeting with the CIO of his company. He shows her the IECSA website and the web pages describing the IECSA high level concepts. She acknowledges that she has heard about the IECSA project and that it was making architectural recommendations, but that she had not quite gotten around to checking it out. She agrees it is time for her and her staff to do so.

She clicks on the Executive Summary and the Project Summary to get a very quick overview of the project, and then jumps to the Recommendations. She sees there the recommendations to:

- "Adopt the IECSA Architecture as the strategic vision for your information infrastructure"
- "Create systems architect positions"
- "Think in architectures, not projects"

After reviewing these recommendations in more detail, and discussing the concepts and possibilities with her staff, she develops a position paper using many of the arguments discussed in the IECSA recommendations. She presents this to the other executives, shows them the Executive Summary from the IECSA website, and gets their overall concurrence, with the understanding that although the IECSA concepts are indeed the strategic vision, individual decisions will need to be made on actually implementing specific technologies, based on financial and technical situations.

The CIO agrees with these provisos, appoints an 'Automation Architect', and requests that he develop a more detailed plan for implementing the IECSA recommendations.

This page is intentionally left blank.

5. PROJECT DESCRIPTION

The IECSA project has set forth the following high-level objectives for defining an Enterprise Architecture:

1. Develop a complete set of systems requirements and architecture documents to support an industry-wide enterprise architecture for the self-healing grid and integrated consumer communications interface.
2. Contribute project results, as appropriate to relevant Standards Development Organizations (SDOs) and industry consortia to effectively move the development of key open standards forward toward a robust industry infrastructure.
3. Apply systems engineering concepts to architecture development including, but not limited to, the elicitation and management of system requirements, analysis of requirements, development of proposed architectural designs, evaluation of architectural designs, and use of standardized industry notation for documentation of architectural views.
4. Identify the potential for infrastructure sharing and synergy between power engineering operations and other application domains.

5.1 Project Tasks and Analyses

A project of this magnitude has significant project management requirements. A very disciplined approach is required to elicit system requirements and resolve conflicts. The IECSA team applied Six Sigma® quality methodology, which encompasses and extends the traditional systems engineering process, to identify, design, optimize, and validate the IECSA framework architecture. In accordance with the Six Sigma methodology, IECSA development was broken down into seven tasks – each building on, in general, the previous task. The list and sequence of these tasks are described below.

Task 1: Define the Scope of Requirements

The initial step when developing IECSA was clearly defining the scope of the requirements of the energy generation, delivery, and system functions and identifying all stakeholder roles. There are many power system applications and a large number of potential stakeholders who participate in energy system operations. In the future, more stakeholders (including customers responding to real-time prices, distributed energy resource owners selling energy and ancillary services into the electricity marketplace, and consumers demanding high quality) will actively participate in energy system operations. At the same time, new and expanded applications will respond to increasing pressures to manage energy system reliability as market forces push the power system to its limits.

System security was also recognized as crucial in the increasingly digital economy. The key has been identifying and categorizing all of these elements so their requirements can be understood, their information needs could be identified, and synergies among these information needs could be determined.

The purpose of Task 1 was developing a deeper understanding of the project's scope and beginning to develop the rigorous methodologies the IECSA team used to determine and analyze functional and non-functional requirements for automating, managing, and planning electric energy operations. The scoping entailed identifying some 70 high-level activities and over 400 supporting activities. In addition to objectives stated above, Task 1 also included a rigorous tools selection for IECSA development. Analysis of the identified activities resulted in three areas of focus in Task 3.

Task 2: Assess the Industry and Technologies

Task 2 included a 'first pass' listing of the technologies that the IECSA team believes should be considered in developing a comprehensive utility communications architecture, and the reasons these technologies should be considered. This assessment formed a baseline solution for meeting the power system functional requirements that was developed in Task 3. In addition, the assessment identified potential problems where there were missing or weak infrastructure development efforts, duplication of efforts, overlapping standards, and ad hoc industry infrastructure initiatives that could lead to greater confusion and fragmentation in the industry.

Task 3: Perform a Formal Requirements Gathering Process

Task 3 defined the formal requirements gathering and development process. The process began with development of a 'Domain Template' that identified key pieces of information to be elicited from domain experts in the stakeholder interview process. The information to be solicited was driven by the IEC standard – Reference Model for Open Distributed Processing (RM-ODP). Part of the requirements gathering process involved identifying various stakeholder classes that would have input, at different levels, into the requirements development process. Captured information was input into the domain template, resulting in Use Cases for the selected applications.

Task 4: Analyze Requirements

Task 4 focused on 'commonality/normality' analysis of the various data items identified in Task 3. Commonalities were identified and abstracted into data objects, common services, and generic interfaces. Identification of common elements allowed for minimization of the data items, services and interfaces that the architecture must support.

The Task 4 objective was to begin the design process by building on the foundation established by the requirements gathering process. The first step was mapping the general requirements into a preliminary, abstract, high-level design, which consisted of general components and subsystems. The next step was identifying the interactions between these subsystems and components to produce requirements for the communication system between these entities. The third step was unifying the working requirements by identifying potential synergies and overlaps among requirements that could be exploited to streamline and simplify the requirements. The fourth step was describing the methodologies that support the building of the systems architecture, as well as subsequent activities to manage changes.

Task 5: Specify and Analyze Architecture

Task 5 included the distillation of the normalized Use Cases into standard notation and subsequent mapping into applicable technologies. In Task 5, the team took the high-level design and began the process of making it architecturally coherent and internally consistent. Abstractions were finalized, components and subsystems specified, and interfaces and protocols were formally specified where these have been clearly standardized or are in de facto use by the industry.

Task 6: Assess Existing Standards

The focus of Task 6 was identifying the *existing* technologies, identified in Task 2, against the requirements identified in Tasks 3 and 4 and the IECSA design that resulted from Task 5. It is important to distinguish between this task and the technology assessment performed in Task 2. Task 2 was concerned with identifying technology that might be useful in the new design, before any requirements were defined. Task 6 focused instead on how to build the new architecture on top of what exists now. In other words, the output of Task 6 describes 'how to get there from here', now that a 'there' had been defined.

Task 7: Formulate Recommendations

As Task 6 attempted to map existing technologies to the identified requirements, inevitably, there will be gaps and seams between existing technologies and the required functionality. Task 7 identified

new and/or technologies that will be required to meet future implementation needs. It is expected that the IECSA recommendations will be used as inputs to standards bodies to help formulate implementations to meet the identified needs. In addition, Task 7 identified industry trends from present implementation strategies, future functional requirements, and emerging technologies. The recommendations were laid out in a road map showing how the IECSA must migrate and evolve in the future.

5.2 Relationship to other CEIDS projects

As an overall architecture, IECSA can provide an architectural framework for work presently under development or under consideration. Some examples of applicability include:

Distributed Energy Resources/Advanced Distribution Automation (DER/ADA) Project: the IECSA recommendation to use a common language is being exploited as the DER/ADA project develops 'standard' objects for future DER/ADA devices and the DER/ADA project can advance the recommendation of using IEC 61850 as the communication protocol of choice.

Fast Simulation and Modeling (FSM): The hierarchical structure identified in the IECSA Self Healing Grid scenario is the parent of all FSM implementations. In addition, the captured requirements and identified technologies can all be fed directly into the total FSM solution.

Critical Infrastructure Security: As analysis of cyber security needs progress, the Federated Services in the area of security options can be taken as direct inputs into this project.

Consumer Portal: The numerous Use Cases describing Real Time Pricing, Direct Load Control, and Home Automation can be used to help lay out both physical and logical design criteria. Captured functional requirements can be directly fed into the project.

- Uses of IECSA: The Portal Project can use the methodology of domain template construction and the IECSA models to flesh out in greater detail the scenarios to be implemented. IECSA provides a documentation style and detail that can be used to seed the next stages of portal program development.
- Provided to IECSA: The Portal Project, Phase I provided domain templates illustrating use case scenarios to IECSA so that architectural requirements of consumer portals could be incorporated into the architecture.

5.3 Final Deliverables Roadmap

The final deliverables for the IECSA project are wholly contained within the framework of a four-volume set. The purpose for subdividing the work product into volumes is to organize related material together in a meaningful way and to focus specific target audiences on the review of appropriate materials.

All deliverable material is designed to be presented in a printable format, although it is anticipated that the more widely used portions of the material will be available in web-enabled formats allowing users to electronically search through and hyperlink among related materials.

Volume I: IECSA User Guidelines and Recommendations

Volume I is targeted toward managers and executives in the energy and information industries. It begins by painting an overall vision of the IECSA architecture and portrays the value story and market drivers for an integrated architecture. Volume I closes with a set of guidelines for using the project's results.

Volume II: IECSA Functional Requirements

Volume II is targeted toward domain experts and application engineers interested in reviewing the requirements and descriptions gathered by the IECSA team. It contains the raw data and descriptions of the materials gathered by the team, a description of the people and venues participating, and the processes used to gather the data. Also included in Volume II is a navigable description of the energy enterprise broken down into its constituent domains and linkages to the raw data.

Volume III: IECSA Model

Volume III is targeted toward application and information architects within the energy enterprise. It contains a description of the architecture in terms of a model. This volume includes a description of the modeling constructs used, a copy of the model itself, and a web-navigable snapshot of the model.

Volume IV: IECSA Technical Analysis

Volume IV is targeted toward application and information architects and implementers within the energy industry. It contains the analyses the team used to develop the architecture.

5.4 The IECSA Reference Architecture Development Process

Before discussing exactly how system architects, power system engineers, and system designers will use the IECSA Reference Architecture, the following subsections describe how the IECSA Reference Architecture was developed and what it contains.

Overview of the IECSA Reference Architecture Development Process

The development of the IECSA Reference Architecture and the process for using it are illustrated in and are described in more detail below:

1. **Use Cases**, developed by the IECSA team and stakeholder domain experts, were developed both to describe current and future power system operational functions, as well as to illustrate the range of functional requirements for power system operations that involve distributed information. These Use Case descriptions contained three major components:
   - Narratives that describe the function in plain language so readers can fully understand the functions themselves
   - The sequences of communications that need to occur between the various ‘actors’ that are either producing or consuming information as well as identification of the information being communicated
   - Identification of the requirements for each communication sequence such as the Quality of Service required, security needs, configuration issues, and data management needs.

   Examples of Use Cases include wide area measurement and control of transmission systems, real-time pricing, and advanced distribution automation.
2. Both **domain and architecture experts** extracted the distributed information requirements from the Use Cases and stored these requirements in a database consisting of the distributed information requirements, organized by the four issue areas
   - Configuration issues
   - Quality of Service issues
   - Security issues
   - Data Management issues
3. **The IECSA Reference Architecture High Level Concepts** for all distributed information technologies were developed by IECSA and Stakeholder Architecture Experts through the

analysis of current information technology concepts and trends. These architectural constructs form the basis for the detailed recommendations for the different technology solutions.

4. **The IECSA Environments** were extracted by reviewing the architecture requirements of all Use Cases and identifying patterns of similar distributed information requirements. These environment-linked requirements were analyzed to determine the appropriate technical solutions and best practices that would be needed to provide solutions to the requirements. Examples of environments include deterministic rapid response interactions within a substation; secure interactions between field devices and control centers; interactions among systems within a control center; and interactions between market participants and Regional Transmission Organizations/Independent System Operators (RTOs/ISOs).
5. **IECSA Abstract Services and Generic Interfaces** were identified as the abstract representation of the architectural requirements, in which each requirement was assumed to have some abstract service able to meet it. Thus, the confidentiality requirement became the Common Service 'Provide Confidentiality'. Common services are abstract because they do not represent any specific technology for actually providing this confidentiality. Common Services connect to one another via a set of Generic Interfaces.
6. **Recommended, Alternative, and Possible Technology Solutions and Best Practices** were analyzed by the IECSA team and stakeholder technology experts to link them to the technology independent architecture for each IECSA Architecture Framework environment. Most of the recommended solutions met the systems engineering principles and the high level concepts, while alternative and possible solutions include legacy technologies as well. The capabilities of the technology independent architecture, as well as the technology solutions and best practices, are described briefly. In addition, their specific advantages/strengths and disadvantages/weaknesses are also described.

Development of the IECSA Environments

Use Cases described their architectural requirement in the domain template spreadsheet. The IECSA Reference Architecture environments were extracted from these Use Case spreadsheets, such that each environment was made up of similar architectural requirements. These environments appeared as patterns of 'x's' in the spreadsheets.

Iterations on these environments allowed one environment to be split into multiple environments if distinctions appeared in patterns, or, vice versa, multiple environments to be merged into one environment, if it turned out that no significant differences were found.

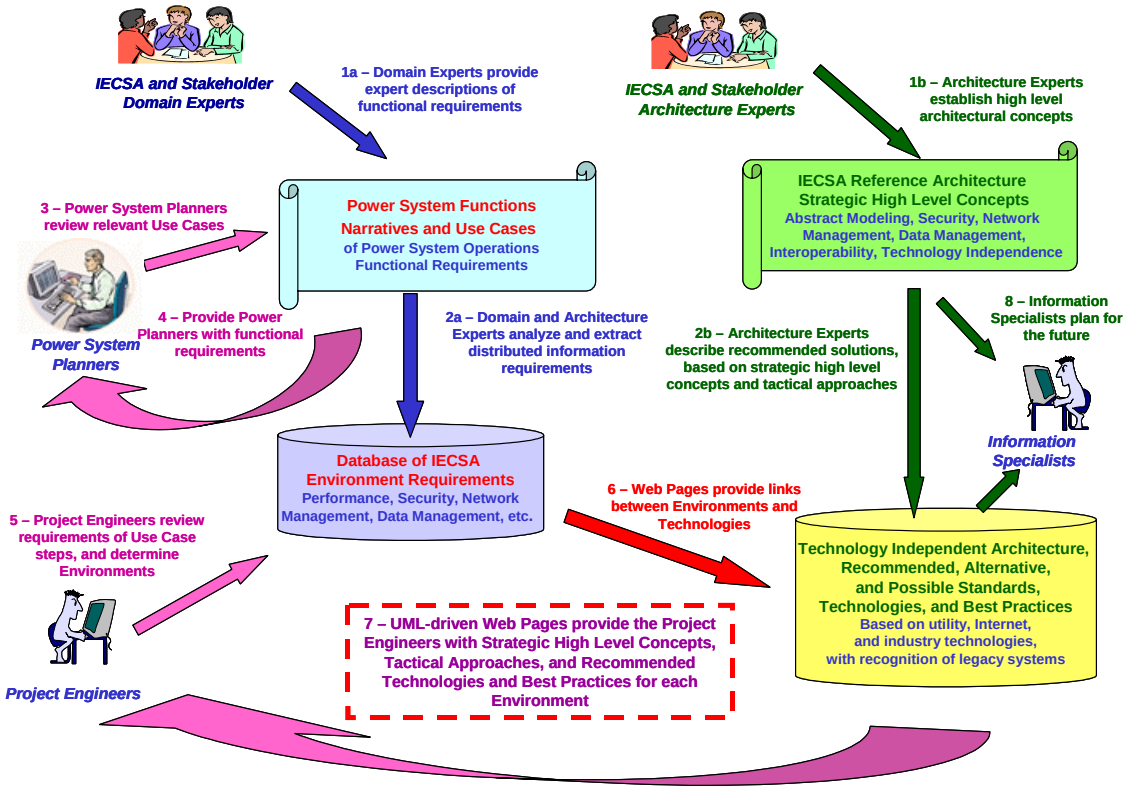

Figure 24: Development and Use of the Reference Architecture for Power System Operations with Distributed Information (the IECSA Reference Architecture)

The figure depicts the process the team used to develop the IECSA as well as the process by which it gets used.

6. RECOMMENDATIONS

The recommendations are organized into the following sections:

- Recommendations to Executives: Adopting IECSA as the Strategic Vision
- Recommendations to Chief Information Officers: Implementing IECSA in the Organization
- Recommendations to Energy Industry Engineers: Key Recommended Strategies, Technologies, and Practices
- Recommendations to the Energy Industry: Roadmap to a Deployed Industry Architecture
- Recommendations to System Engineers: Follow Best Practices in Systems Engineering
- Recommendations to E2I and EPRI: Future Efforts to Achieve IECSA's Long-Term Goals

6.1 Recommendations to Executives – Adopting IECSA as the Strategic Vision

- **Adopt the IECSA Architecture** as the strategic vision for your information infrastructure
- **Ensure that the different users of the IECSA Architecture understand** how to utilize the relevant parts of the IECSA products, including the power system functional descriptions and the IECSA high level concepts.
- **Develop a plan** for implementing the recommended architecture and standards-based technologies, based on your specific business needs and the timeframe appropriate for meeting those needs and your financial constraints.
- **Provide feedback** so that the IECSA Architecture can evolve to meet future needs and recommend standards that are created in the future.

6.2 Recommendations to Chief Information Officers - Implementing IECSA in the Organization

These recommendations are for Chief Information Offices to encourage the development of systems architecture as a philosophy for ensuring reliability and safety throughout the power network and efficient, cost-effective operations within the organization.

- **Use open system standards.** Despite the best efforts of many within the industry, there is still a tendency in some power system organizations to use proprietary technologies in their networks. Standards are the building blocks of a common architecture, and if they are not used, the benefits of an integrated network will never be realized.
- **Use emerging standards.** The power system has traditionally resisted adopting new technologies because of the cost of deployment and the strict environmental requirements of the industry. However, to meet the needs of the digital society, the power industry must learn to become first adopters and share the cost across the industry if necessary.
- **Create systems architect positions.** All organizations within the power industry should have at least one person whose is a designated 'Automation Systems Architect'. This staff position should be responsible for ensuring that protection, monitoring, control, and maintenance of the power system are integrated with the information technology, network security, and enterprise management of the organization. This architect will also encourage integration with external organizations.

- **Develop common ways of doing things.** The power industry must learn to think of itself as a single shared infrastructure. Industry participants must develop common policies on security, common object models, common reference designs, and use common technologies. Only then will the power system be able to heal, optimize, and protect itself.
- **Think in architectures, not projects.** Too often, power system automation development is based around the 'project'. Someone champions a project, builds a business case, convinces management, and builds the project. Whether the project succeeds or fails, another project later takes its place at the focus of the organization's efforts. Too often, no one ensures continuity between one project and the next, interoperability between the project and the outside world, or even integration of the project with what came before. Utilities and other industry organizations must learn to think in terms of common components and interfaces that can be re-used.
- **Use architecture tools.** In the past few decades, whole separate industries have sprung up to develop tools for requirements analysis, network design, risk assessment, and data management. With a few exceptions, these tools are rarely used in the power industry. Once organizations have created architects, they must deploy the tools to make them reducers of cost and risk within the organization.
- **Encourage new standards.** Unfortunately, cost pressures have reduced the participation of power industry organizations in the development of new standards. It is vital that the people who are deploying technology have a say in the requirements for its development. Ways must be found to encourage participation. For example, some countries provide subsidies to organizations that participate in standards development; this model should be considered in the United States.
- **Integrate the standards that exist.** This document makes specific recommendations for harmonizing standards and technologies that currently exist in the power industry. A more general culture must be developed, however, around the concept that fewer standards are better. There should not be so much truth in the old industry joke, *"The great thing about common standards is that there are so many of them to choose from"*.
- **Keep the work going.** IECSA is a start in defining the concepts and models that will be needed to integrate the industry. However, cross-industry organizations must support the idea of a common architecture, and continue to feed input back into the IECSA structure so it can grow richer and more powerful.

6.3 Recommendations to Energy Industry Engineers - Key Technologies and Practices

This section summarizes the major recommendations made in Volume IV regarding the use of a common architecture, technologies, and best practices. It is not intended to be comprehensive, but to give the flavor of the important items. This does not rule out the use of other practices and technologies depending on the working environment.

6.3.1 Architecture Definition

It is important that the energy industry begin to develop networks using systems architecture concepts and tools. In particular, the engineers within the energy industry should:

- Use **UML methodologies** for documenting and analyzing systems. UML is a mature technology with a variety of available tools.
- Join with other organizations to create **reference designs** for power system operations. The concept of the reference design has been used with great success in other industries such as telecommunications.

- **Adopt common language(s) and harmonize standards focused on language development.** The common language elements adopted and or recommended by IECSA must be continually developed. Developing and using a common language for intelligent equipment operations is a key IECSA recommendation. Language development and harmonization is one of the key strategic pathways to systems integration. IECSA calls out prominently language development taking place within key energy industry standards communities, however, common language development and harmonization is also needed for interoperation with industries outside of traditional energy industry standards. These include, but are not limited to, residential, commercial and industrial in-building communications, as well as systems and enterprise management oriented communications with telecommunications industries.

6.3.2 Object Modeling

The core of interface interoperability is the shared definition of nouns and verbs to create a common language that can be unambiguously understood and acted upon by intelligent equipment. A substantial body of work is available for communications with advanced field equipment and this work is now emerging as an International Standard under IEC TC 57 committees. Product vendors and energy industry engineers should:

- Use **IEC 61850 object models** and services for automation of substations, including the additions currently being developed for distributed energy resources, wind power, and other applications.
- Use **BACnet™** for consumer communications within commercial and industrial in-building networks automation. Recommended by ASHRAE, it is a leader in its field and provides common object models. This recommendation also includes continuation of work to integrate objects for energy related communications developed within the IEC with the development of the BACnet protocol. This integration enables two industries to interoperate through using a common language. This not only leverages development work but also can reduce the need for 'gateways' to translate messages between energy and building automation industries. This recommendation can also be considered for residential network standards that use object based communications. As noted later in the Recommendations section, however, this is a volatile field with a multitude of worthwhile technologies available. The immediate future of consumer access will likely focus around common gateways or portals.
- Use **ANSI C12.19** for metering data. Its XML representation of data will be a part of the 2004 release of the updated standard.
- Use IEC 61970 and IEC 61968 **Common Information Model (CIM), Generic Interface Definitions (GID), and System Interfaces for Distribution Management (SIDM)** as common interfaces for energy management and distribution management systems. Once these have been harmonized with other information models, such as IEC 61850, they should be used throughout the power system.
- Use the **self-description** capabilities of these technologies to enable **electronic access to metadata**. Metadata is information about the source, format, and meaning of data. Once this is available online, much of the cost of power systems integration will be reduced because this information will be freely available, instead of being either filed in multiple formats or kept in the heads of systems engineers. Intelligent 'agents' or other special applications can then use the metadata to help create cooperating plug-and-play systems, even when these systems are developed by multiple vendors with different implementation constraints over many years of evolving technologies.

6.3.3 Security

The power industry is only starting to become awake to security concerns. In order to implement security in an architectural fashion, organizations should follow a set of effective practices and implement security technology standards to ensure the cyber security of their systems. These practices and standards include:

- Perform similar levels of **formal risk assessment** on the vulnerabilities of the communications network and information systems as are currently performed on the power system itself. Implement a regular risk re-assessment process.
- After analyzing security requirements based upon risk assessment, **define security policies** based on those requirements, and implement new policies. Note that the security implementation can sometimes decrease availability of information from, and control of, the power system. Take this into account when designing the combined network. It should also be noted that security policy related requirements are being formed in key organizations, such as North American Electric Reliability Council (NERC) and government agencies with the charter to protect critical infrastructures.
- Security should be approached as part of your organizations overall security policy implementation. Security includes a **portfolio of strategies and technologies** that are combined to meet the security policies of an organization. The technologies included and recommended in the IECSA analyses represent individual elements and components of an overall security strategy.
- Consider **open systems standard security technologies,** such as TLS, IPSec, PKI and Kerberos, throughout the power system automation network, along with some specific IEC security standards for protection relaying.
- Focus on **security management** such as the deployment of keys and certificates and how this affects the organization's processes.
- Use **XML-based security technologies** that integrate data management with security, such as Security Access Markup Language (SAML) and XML Key Exchange.

6.3.4 Network and System Management

Today's automation systems are often characterized as a collection of pilots that are limited by their existing infrastructure. This limitation is often traceable to a lack of robust systems administration capabilities including network and systems management. As the industry seeks to scale up automation equipment to large numbers of field devices. Systems administration must become more capable to enable systems that can be effectively managed on large scales. IECSA emphasis on network and systems management reflects the challenges that come from massive deployments. These topics must be rigorously addressed or the field deployments can quickly become unwieldy to manage. Network and system management are functions commonly performed in business computing and telecommunications, but not yet deployed extensively or completely in power system automation. The following are a few of the recommendations that have emerged from project analyses. :

- **Expand network management into the power system communications network** beyond the simple status reporting that SCADA systems often perform. Begin deploying **the Simple Network Management Protocol (SNMP)** functions (IETF RFC 1351, 3411, and 3414) or equivalent, i.e. the ability to gather statistics, receive alerts, enable and disable devices from any location in the network.
- **Develop network and systems management, security management, and power system applications in parallel**. As systems are specified it is important to develop requirements for network and systems management and security at the same time as the applications. This is

important for small resource constrained devices since the management and security functions may drive minimum hardware requirements. Currently, almost all focus is on the development of power system applications only. The portfolio approach to system designs will help to ensure adequate capability for managing the field equipment including the ability to run diagnostics in remote equipment as well as managing application execution.

6.3.5 Data Management Practices

Energy industry engineers are recommended to employ the IECSA Architecture to develop data management methodologies particularly for intra-control center functions The IECSA Reference Architecture provides a common data management approach and also recommends and discusses the merits of different technologies and services that will help integrate a variety of operationally focused applications such as EMS, DMS, GIS, AMS/WMS, OMS, CIS, and engineering applications. At the same time, IEC TC57 WG14 is developing CIM object models for exchanging data within the control center environment, while other standards groups are developing additional types of data objects (e.g. graphical object models).

However, this work is only the first step toward managing data and data exchanges within the control center environment. Different applications from different vendors in different control centers include many variations in data models and data exchanges, covering many different requirements. Energy industry engineers should therefore develop tools and practices focused on:

- Implementation of **IECSA-based metadata management practices** for object models used within the control centers so that the metadata is "browsable" and available for manual data mapping procedures, as well as for use by automated data mapping tools.
- Utilization of the results of the **harmonization efforts for IEC61850 device models and CIM power system models** for both IEC61968 (distribution) and IEC61970 (transmission)
- Handling of **data mapping** for different applications
- Handling of **IECSA-based data validation and synchronization** across functions
- Development of **role-based 'Client views' views' based on IECSA namespaces**: the establishment of what data is available and permissible for being accessed by different 'clients', such as applications, systems, and human users
- Use the **IEC61970 Part 403 – Generic Data Access (GDA)** as the common application interface for accessing metadata and data in a backend technology neutral way.

6.3.6 High-Speed Measurement

The self-healing grid will not be possible unless data is exchanged securely and consistently in real time across much wider areas. A number of technologies are vital to making this possible. The following are a few recommendations for time synchronization and event communications.

- Use **ISO/IEC 18014-1** timestamp format, permitting the creation and correlation of secure ***audit*** trails of power system events.
- Use **IEEE 1588** for sub-millisecond time synchronization across multiple networks.
- Use **IEC 61850-8-1** Generic Object Oriented Substation Event (**GOOSE**) protocol for real-time exchange of power system protection and interlocking information over LANs and WANs.
- Use either the **IEEE 37.118** or **IEC 61850-9-2** standards for exchanging real-time samples of synchrophasor information across LANs and WANs. This will move the power system from 'state estimation' to simply 'state measurement'.

- Use the **IEC61970 Part 404 – High Speed Data Access** - HSDA as the common application interface for Wide Area Measurement and Control. Note that OPC Data Access (OPC-DA) is an appropriate COM implementation of the HSDA as the client-server architecture fits well with the need for multiple applications having access to real-time data as well as for multiple applications being able to effect real-time control.

6.4 Recommendations to the Energy Industry - Roadmap to a Deployed Industry Architecture

The following recommendation sections are a blend of methods and content development. The recommendations on methods are necessary to appreciate and use some of the key project content. The future energy delivery and services industries will provide more function and value to the industry and consumers, but this will require much more complexity than today's systems provide. Managing the complexity of these systems as they are designed and developed is important to determine how far reaching and effective they will be. Emphasizing systems engineering methods represents an important direction for the energy industry to effectively migrate towards advanced automation.

Achieving an economy of scale and shared infrastructure sounds great, but how will those lofty goals be realized? IECSA provides the next step on the road to deployment of an industry architecture. IECSA follows successful strategies of earlier industry standards work, which have illustrated the benefits of common communications profiles, and well-defined industry standard object models. IECSA takes the next step toward fostering a deployable common infrastructure that can be constructed a small step at a time.

- **Codify the IECSA project work by developing real world designs and implementations** that are used to validate and refine the architecture. It is only by developing real world designs and implementations that the recommendations from this project can be validated, more fully developed, refined, and codified. The architecture and technology recommendations presented here are a roadmap and guideline for future development, but real equipment designs are necessary to determine how to bring the necessary technologies together. Further work to develop the architecture is necessary, but this work should be now specifically tied to projects directly addressing specific needs.
- **Incremental approach: Start small and learn lessons**. IECSA architecture and technologies must to be immediately employed in designing systems and products. Projects may be small in scope but should encompass the full vision of how they may ultimately become scaled and managed in large numbers. The architecture level recommendations within this project can be used to help define the technologies that should be considered for any small device that is likely to become part of a larger infrastructure. This concept is particularly important for small resource constrained field equipment such as meters, distribution automation equipment, and consumer portals.
- **Build small projects with IECSA that can be integrated across traditional boundaries**. Projects that particularly achieve integration across traditional boundaries are important to validate, test and develop the architecture principles put forward within IECSA. Examples include phasor measurement integrated across multiple companies, consumer portals that integrate energy industry and consumer in-building networks and equipment, and projects that integrate distribution operations with transmission operations. These types of projects will bring to the surface detailed design issues that still remain to fully specify an industry-wide architecture. Particular attention should be given to managing these cross domain implementations including security integration.

6.5 Recommendations for System Engineers - Follow Best Practices in Systems Engineering

Systems engineering is a multidisciplinary approach for developing, specifying and managing automation and information systems. Systems engineering is a maturing discipline and several standards are emerging as recommended practices. The following sections only touch on some systems engineering highlights. Readers should refer to organizations, such as INCOSE and other standards organizations within the IEEE and ISO/IEC, for a more complete treatment of systems engineering as an emerging technical discipline.

- Drive Systems with Stakeholder Requirements. Systems engineering emphasizes the need to effectively capture and develop requirements that are driven by stakeholders. It is important to incorporate a variety of perspectives in the requirements elicitation process, including individuals managing systems as well as those considered as end users. Requirements specifications are an important part of any system development process. It should be noted that robust approaches to requirements include provision for services and functions that may not be initially foreseen.
- Apply Architecture Development Concepts. The energy industry must apply architecture development and design principles when developing automation and information systems. The disciplines for developing architecture are beginning to mature and are a necessary step in the scale of integration and advancements now foreseen for the energy industry. Architecture concepts seek to understand and document systems from an enterprise and industry-wide integration perspective. This perspective is required to overcome the limitations of component or systems development carried out without a sufficiently broad vision.
- Migrate toward Standard Terminology. The energy industry must migrate toward using standardized terms for both business and technical domains. The IECSA project has adopted terms within the context of the project to enable appropriate linkages within the model and in documents. However, it is clear that many terms are overburdened and suffer from multiple definitions. The industry needs to take steps to define terms and their context for consistent usage. Standardization of terminology within technical and business domains remains an industry issue that can be addressed by contributions to key standards organizations and appropriately referenced. The IECSA project seeks to integrate and reference key definitions from IEC, IEEE, ANSI and other organizations.
- Use Standardized Notation for System Description. Using standardized notation, such as the Unified Modeling Language (**UML),** for documenting and designing advanced automation systems helps reduce the ambiguities inherent in natural language. While UML is currently supported with a variety of available tools, UML for describing architectures is a maturing technology. The industry should continue to follow the development of UML and UML for ODP now under development in the International Organization for Standardization
- Develop System Designs with Complete Specifications Sets. Baseline automation systems are often underspecified from several perspectives: the applications are single or narrow in purpose; the overall architecture as well as network and systems management are not adequately specified; and security; if present at all, is not robustly specified. These inadequacies lead to pilot projects that are limited in scalability and integration. Systems designs must be specified, as fully as possible, from project conception including robustness in the design
- Use IECSA Requirements as a Starting Point for Systems Development. IECSA requirements can be a starting place for most advanced automation systems that will confront enterprise or industry-level architectural issues. IECSA requirements, which are captured in the Use Cases templates, represent a sampling of advanced automation and communication systems. These use cases were developed at an architecture level and are useful for understanding the strategic

breadth and reach of future applications to understand how systems will need to interoperate at higher levels. These use cases are not exhaustive, nor are they at the detail of design level requirements for specific equipment. They can, however, be used as a useful project starting point.

- Use IECSA Architecture as a Basis for Understanding a Unified Approach. The IECSA Technology Independent Architecture provides a platform for off the shelf interoperability. This architecture can be used as the unifying construct for new system deployments.
- Use IECSA Analyses as a Basis for Understanding Capabilities and Limitations of Available and Emerging Technologies. The IECSA team analyses included an assessment of existing and emerging technologies against the requirements gathered for specific applications. These analyses can be used to understand the capabilities and limitations of technologies today as well as identifying where more work is needed to develop more capabilities in new standards.

6.6 Recommendations to E2I and EPRI - Achieve IECSA's Long-Term Goals

The recommendations to E2I and EPRI include a specific action plan to ensure that IECSA is successfully implemented. This plan proposes specific steps be taken in the following areas:

- Contributing to standards development organizations and consortia
- Sponsoring pilot projects and field trials
- Developing engineering tools and notation methods
- Encouraging the adoption of IECSA
- Initiating work to continue systems analysis of the utility industry in more detail
- Integrating IECSA with other architectures

6.6.1 Continually Evolve Specifications

Do not wait for standards…develop and drive them to completion!

This section contains recommendations for actions that can be taken by consortia and other industry groups. These groups are vital to create consensus on interoperability issues so that formal standards can be written. For many of these groups, they *are* the de facto standards organization in their area. Work on some of these items is already underway. In those cases, EPRI, CEIDS and other industry organizations must try to provide resources to encourage the work.

This section recommends an action plan for ensuring that an industry-level architecture can be successfully implemented. Adopting IECSA will require educating the general utility populace, implementing IECSA principles, developing and standardizing new needed technologies, and harmonizing those technologies that exist and presently overlap.

This section provides recommendations for contributing to standards development organizations and consortia in order to:

- Develop missing IECSA technologies
- Harmonize overlapping technologies
- Integrate existing technologies into IECSA
- Ensure the IECSA recommended technologies are all standardized

Develop Contributions to Standards Organizations and Consortia to Progress key Infrastructure Elements

Standards organizations and consortia make progress through contributions that refine the standard as a result of analysis or actual implementation. This important aspect of standards development is often overlooked in most projects that seek to implement them. As part of the IECSA Project, Table 5 represents steps in this direction. These recommendations must be further developed and new recommendations added as follow-on work continues. These are some of the necessary steps to build the components of an industry-wide architecture.

In Table 5, TC is defined as Technical Committee and WG is defined as Working Group. Unless otherwise noted, all working groups cited belong to the IEC TC 57 on Power Systems. Some of this work is already underway, in which case CEIDS' and EPRI's roles should support the work.

Table 5: Recommendations for Standards Organizations and Consortia

Recommended Action	Possible Group	Description
Harmonize CIM and IEC 61850	Ad Hoc WG07	The IEC 61968 and 61970 Common Information Model addresses the overall power system, while the IEC 61850-7 object models address devices and functions within substations. The IEC should either merge the two object models or define a standardized mapping defined between the two. This will enable the exchange of data between systems implementing the different models, and permit the creation of configuration tools shared between EMS and SCADA systems.
Harmonized 61970 GID and 61850 ACSI and 61968 Messaging Model	Ad Hoc WG07	The 61970 GID provides a way to access operational information once it has been transmitted by field communication networks. However, how to exactly integrate 61970 with 61968 and 61850 has not been standardized. The IEC should standardize the mechanics for HOW off the shelf components can be made interoperable.
Add missing Security for Legacy Protocols	WG3, WG15, DNP TC	The most popular serial protocols between and inside substations (DNP3, IEC 60870-5, ModBus®, Profibus) need standardized security solutions for authentication and encryption, both on LAN/WANs and serial links. The IEC should create these solutions. Adding such measures will permit utilities to continue to deploy these protocols where they are most effective without security concerns.
Endorse AGA 12-1 Retrofit Security	WG3, WG15	The IEC should endorse the AGA 12-1 security standard for serial links currently being developed by the American Gas Association and Gas Technology Association. This standard defines a protocol and device requirements for 'bump in the wire' encryption of serial links. Endorsing this technology in the power system can reduce costs because security can be added to legacy systems without 'forklift' upgrades.
Endorse IEEE 1588 LAN Time Synchronization	WG10	The IEC should endorse the IEEE 1588 standard for Precision Time Protocol (PTP) time synchronization over local area networks. IEEE 1588 allows synchronization down to the microsecond level which is required in applications such as SunchroPhasor Implementation of IEEE 1588 will reduce substation integration costs by eliminating the need for a separate LAN to distribute high-resolution time synchronization throughout each substation.
Create Security Risk Assessment and Deployment policies, procedures and metrics.	WG15, NERC, other?	The industry needs to develop process, procedures, and target metrics in regards to how security risk assessments should be applied to utilities and other power system organizations. NERC guidelines will help to set requirements, but the procedures and policies necessary to allow the development of policies based upon risk assessment need to be developed.
Integrate Legacy Protocol Mapping Rules.	WG10, WG3	The industry needs standards on how to map data from legacy protocols (such as DNP3, IEC 60870-5, ModBus, Profibus) onto IEC 61580 and CIM information models. Providing such mappings may encourage automation of substation and field equipment configuration, reducing errors and cost.

Table 5: Recommendations for Standards Organizations and Consortia		
Recommended Action	Possible Group	Description
Support Multicast IP.	WG10	The IEC should expand on the Generic Object-Oriented Substation Event (GOOSE) and Sampled Measured Value (SMV) protocols to permit their use in wide-area networks using multicast IP addresses. This will permit the centralization of protection algorithms over wide areas and the distribution of phasor information in real-time to control centers. Application on VLANs should also be considered
Secure GOOSE and SMV	WG15, WG10	The IEC should develop a standard mechanism for securing the high-speed GOOSE and SMV protocols between sites so they can be carried over organizational boundaries. This work is in the proposal stage.
Unify Utility Enterprise Management	WG12, WG13, DMTF	The IEC 61968 and IEC 61970 Common Information Models are missing information on enterprise (i.e. network or system) management. In addition, the IEC CIM should be integrated with work outside the power industry, in the Data Modeling Task Force (DMTF). The DMTF also has a CIM, which does not contain power system information yet. Harmonizing these two models will help to harmonize utility control network and corporate IT operations.
Harmonize Utility Security Management	WG10, WG15, WG13, WG14	There are currently no power system object models for managing security, i.e. detecting intrusions, logging user accesses, enabling or disabling security associations. The IEC should add these models and harmonize them with those of enterprise management (separate item). Creation of standard models will enable standardized tools for security management and smooth integration of security systems across the industry. They could lead to a nationwide 'utility security dashboard', as envisioned by the Department of Homeland Security.
Extend Power System Configuration Language	WG10	The existing Substation Configuration Language (SCL) defined by IEC 61850-6 addresses only substation devices. The IEC should expand the scope of this schema to include all types of power system equipment and concepts from the Common Information Model (CIM). Such an expanded configuration language would enable shared simultaneous configuration of various levels of masters and data concentrators within the power system. This would reduce cost and improve reliability of system upgrades, especially across organizational boundaries.
Create standards for Data Warehousing		The IEC should develop standards for a set of interfaces for gathering data from multiple data warehouses (data integration) containing metering data, asset information, etc. The groundwork for this capability has been laid in the IEC CIM, but it needs to be clarified. This work can enable the creation of 'CEO Portals' that can display real-time summaries of the working state of a utility, enabling better reliability, safety, and customer response.
Harmonize and Integrate OpenGIS® for Utility Industry	Expand scope of WG14?	The IEC should endorse and integrate the work of the OpenGIS Consortium (OGC) into the utility industry, especially distribution automation. This will standardize the power industry information models with Geographical Information Systems developed for other industries, notably the telecommunications industry and other utilities. Eventually, this will enable multi-utility displays that can be shared across organizational boundaries, encouraging cooperation between organizations in emergency situations.
Standardize Device Documentation		The IEC should standardize formats for providing documentation on intelligent power system devices. This type of standardization will reduce costs and errors in making equipment changes by encouraging the development of advanced management and administration capabilities.
Harmonize Power Industry eCommerce	WG16	The IEC should standardize the means by which existing eCommerce initiatives can be integrated into the power industry. Both wholesale and retail markets need to be addressed; they will likely involve different procedures and possibly different technologies. Guidelines should be provided on when wholesale or retail rules apply.

Table 5: Recommendations for Standards Organizations and Consortia		
Recommended Action	Possible Group	Description
Standardize Broadband over PowerLine	IEEE	EPRI and CEIDS should encourage the work that is beginning on standardizing broadband communications over power lines. This will simplify the choice of multiple existing technologies and facilitate many of the future consumer use cases predicted by IECSA.
Standardize Security Revocation Server	IETF	The current CRL and OCSP technologies are polling (e.g. request/response) based. There are performance and timeliness issues that are caused by the size of CRLs and the polling intervals. The power industry needs a server that can be deployed within a security domain that has a knowledge of the certificates that are in use and which applications/entities use those certificates. The revocation server would then alert those entities if the certificate were revoked.
Create Security Audit Record Format	W3C®	There is currently no standard that defines the contents of an Audit Record. There needs to be a standard developed whose semantic content is extensible.
Create Security Audit Record Retrieval	W3C, OASIS	There is currently no standard mechanism for retrieving audit records. An abstract service needs to be defined to provide this capability. This service then needs to be mapped to various technologies (e.g. Web Services, IEC 61850, etc.).
Add Security: SAML Extensions	OASIS	There is no mechanism for an entity to determine how many credential conversions have occurred to provide the credential that is being provided. The SAML attributes need to be extended so that the chain of identity/credential mappings can be determined in order to facilitate the security Quality of Identity service. As part of this work, there needs to be a mechanism to determine the actual chain of credentials. SAML also needs to be extended to support other credential types (e.g. address and username/password).
Add Security: Password Renewal	IETF	There is no standardized mechanism, similar to PKI renewal, to allow password renewal and management.
Create Security: Quality of Security Service	IETF	The Quality of Service concept (e.g. to facilitate routing based upon cost/performance) needs to be extended to allow security to be used as part of the routing path determination. As part of this work, security metrics need to be defined in a standardized manner.
Add Security: Communication Path definition	IETF	The source routing option in IPv4 and IPv6 allows the packet recipient to know the hops/routes that the packet has taken. However, there is no mechanism for the sender of the packet to specify a particular path. This capability is needed in order to allow 'secure' and specific communication paths to be defined via software configuration.
Create Security: Service Discovery	OASIS	Currently there is no mechanism for determining what security services are available for use. A standardized abstract API/service needs to be developed to allow peers to determine the security services available by their peer. WS-Policy should be extended to allow this.
Extend Self-Description for existing protocols	DNP User's Group, ModBus IDA, Profibus Trade Org.	Develop and adopt additions to existing protocols that will enable self-description and other services similar to that found in IEC 61850. This may include developing XML schemas for configuration that are compatible or integrated with IEC 61850-6 Substation Configuration Language. This will reduce installation costs improve reliability and safety due to easier integration with IECSA systems.
Extend Security for existing protocols	DNP User's Group, ModBus IDA, Profibus Trade Org.	Develop a security scheme for securing DNP3, preferably one in common with IEC 60870-5, as discussed in the previous section. Develop security schemes for other common protocols. This covers security 'holes' in the communications networks that are currently addressed by specific existing protocols.
Create Reference Designs	Various	Create 'reference designs' for particular domain areas, such as a Consumer Interface, Demand Response, See discussion in Section 6.6.4for explanation. This will speed implementation of new utility applications and technologies.

Table 5: Recommendations for Standards Organizations and Consortia		
Recommended Action	Possible Group	Description
Develop Consumer Portal	ASHRAE®, BACNet®, CEIDS, UPnPTM,Home Plug Alliance, other vendors	Develop common object models, a reference design, and pilot projects for connecting consumer devices to the power system communications network. This will resolve overlap and confusion in consumer device protocols by designing a common point of connection to the power industry.
Create Demand Response Object Model	UCA International User's Group	Develop common object models for performing Demand Response. The UCA International User's Group can serve as a clearinghouse for this effort, which involves many consortia and standards bodies, including W3C, IETF, OASIS, IEC, IEEE, industry vendors. This will reduce industry 'churn' in developing access points for this application.
Develop Security Policies	IEC, NIST, ISA, NEMA®, DHS, AGA	Develop a security policy best practice document that includes processes and metrics to be evaluated. This document would also contain information in regards to how to perform risk assessment. This allows entities to follow similar steps ensure key assets are secured properly.
Improve Security Education	IEC, NIST, ISA, NEMA, DHS, AGA	A cohesive and coordinated set of educational seminars should be created to discuss the various aspects of security and its implementation. One of the prevalent issues is that often seminars offer opposing and conflicting ideas. This will facilitate ongoing, non-conflicting education/training.
Extend Revocation Server	IETF	The IETF should develop a specification for a central Security Domain revocation server (not a CRL server) with the following attributes: ▪ Allows certificate users to register that certificates are in the user certificate cache. ▪ The Revocation Server would query the CAs CRL servers and process the revocation list(s). ▪ Based upon the CRL processing, the Revocation Server would notify the certificate user that the particular certificate has been revoked. ▪ Optionally, such a Revocation Server could alert Security Domain management that a certificate of a particular user is about to expire so that corrective action could be taken. ▪ Optionally, such a Revocation Server could respond to OCSP requests so that newly configured certificates could be validated as still being valid. It is believed that work on such an entity is needed to allow more timely delivery of revocation information and to allow automation of such tasks.

6.6.2 Bring Forward Object Based Communications Models

Several of the recommendations listed involve the development and standardization of object models. EPRI, E2I, and CEIDS should take the lead in encouraging and providing resources for the development of these object models, using the excellent methodology pioneered in the current E2I DER/ADA project. This methodology covers:

- Initial drafts of object models (using the appropriate IEC61850 and/or CIM templates) using vendor information
- Analysis of the current and future data requirements, based on analytical studies and critical Use Cases
- Use of these data requirements to update the draft object models
- Mapping updated object models into software tools which conform to appropriate standards, in order to validate the object model conformance

- Developmental laboratory tests to verify that the analytical studies have determined the sufficient set of data, which includes all necessary data items, but does not include extra or unnecessary data items
- Field tests to verify the laboratory tests under actual conditions
- Submittal of these vetted object models to the appropriate standards body
- Follow through with the standards bodies to support adoption of the object models as standards
- Support to stakeholders to ensure implementation and deployment of the standard object models

6.6.3 Recommendations for Continuing IECSA Architecture Research

Recommendations for Smart Toolset to Maintain IECSA Over Time

The previously discussed systems engineering approach has been rigorously used during the development of IECSA. To deal with such an overarching architecture development, the team has adopted the Reference Model of Open Distributed Processing, ITU-T Rec. X.901 | ISO/IEC 10746-1 to ITU-T Rec. X.904 | ISO/IEC 10746-4, commonly referred to as RM-ODP standard framework as a conceptual guideline. RM-ODP provides an excellent conceptual framework that has been accepted by the Object Management Group (OMG) and others for providing a complete characterization of the enterprise.

By design, RM-ODP does not provide any notation and method; the IECSA team has not been able to identify suitable commercial tools that directly support its concepts. Rendering and representing architectures remains the subject of significant debate; there is no widespread consensus on how it should be approached. Therefore, a discussion on tool selection is central to architecture development.

The tools used for developing the IECSA framework can also be used to expand it and develop applications based on it. However, developing a *smart toolset*, such that it correlates, discovers, and recovers architecturally relevant solutions when provided with a new set of requirements will greatly enhance the usability of IECSA. This can be based on on-going research in language processing, artificial intelligence and knowledge discovery[8]. The team recommends development of *smart toolset* to increase the usability and applicability of IECSA.

Construction of such a toolset would encompass:

- Absorbing the contents of the ISO2004[9] for mapping RM-ODP to UML. This would allow accommodating a deeper and emerging standard mapping to RM-ODP.
- Revising the UML model of all import data to this extended mapping
- Migrating IECSA import and analysis tools to XML and adding some consistency validation to the word editing process (text sections and spreadsheet) -- this can include what has been done as a manual normalization process today.
- Producing a cookbook and necessary toolset to allow the IECSA process of Domain Template => UML import and normalization process to be replicated by interested and independent groups.

Research the Impact of Communication Failures on Power System Design

Determine how failures in the communications system itself can impact the stability and reliability of a next generation power system that depends upon it. What are the types of failures,

[8] NIST, "Automated Knowledge Discovery System (AKDS)", ATP, 2002
[9] ISO/IEC 19793 Open Distributed Processing-Reference Model-Use of UML for ODP viewpoints specifications – Working Draft.

including equipment failures, operational failures, errors, deliberate attacks, etc.? What are the communication failure mechanisms and mitigation strategies when such failures occur? What are the impacts of the initial communication failures on power system operations? What are the impacts of the failure management strategies, such as alternate paths, failover of equipment, etc on power system operations?

Study Strategies on Managing Disparate Technology Life Cycles

Communication technologies, with life cycles varying from months to years, change far more rapidly than the power system equipment with life cycles of years to decades. Communication technologies often involve continuous version updates and software patches that may or may not be thoroughly tested – especially considering that software gets better with age. What strategies are needed to manage these disparities? How can users be sure of the degree of testing that has been performed? What degree of assurance is needed for different functions?

Research on Distributed Control Strategies

Research should be undertaken to measure the stability and effectiveness of distributed control strategies in real-time and over larger periods of time. Distributed control strategies include closed-loop local and wide area, distributed and central control concepts. No matter what the underlying communications architecture and specific technological implementation, it needs to be demonstrated that use of the IECSA architecture to achieve a variety of local and globally optimized control strategies is possible. Research must be done to identify those implementations that are feasible, stable, cost effective, and enhance rather than diminish the power system reliability – a danger if the architecture and strategies are too complex. For example, control theory needs to be extended to deal with distributed, probabilistic response functions and the relative improvement in performance based on wide-area vs. local feedback measurements. Wide-area control strategies need to be simulated and perfected off-line before they are applied on a 'live' power system.

Development of High-Speed Authentication/Encryption Technologies

It was suggested in Table 5 above that standards bodies consider development of encryption technologies for high-speed device to multi-device communications (as will be required for sending phasor data from one measurement site to multiple subscribing hosts). It is to be noted that although this is a goal, the required level of technology is not available today. Specifically, an encryption technology is required on a point to multi-point message that will not slow down the delivery of the message.

Migration and Maintenance of the IECSA Website

For IECSA to have visibility, the information captured and developed during this project must be readily available to all interested parties. In addition, as the final deliverable is primarily being presented in electronic format, the IECSA.org website must be migrated to a final server and maintained on a consistent basis. It is a strong recommendation that this task be undertaken as soon as possible. The site should be designed for ease of navigation with links to the primary functionality of IECSA being visible on the home page. Also to be included are constructs to solicit comments and easy access to the various tools that were developed during the course of the project (including a link to the Magic Draw™ Viewer).

Develop an IECSA Users Guide

Although the IECSA Report provides a general guideline to assist different users in utilizing the IECSA results (discussed earlier in this volume), a complete Users Guide could provide more details and more examples. In addition, an accompanying IECSA seminar would provide individual support for different groups of users.

The IECSA Users Guide would provide detailed procedures for using IECSA for each of the different types of users: power system planners, project engineers, information specialists,

regulators and advisors, and standards developers. It would also include extensive examples of how the main IECSA deliverable could be utilized to develop concrete equipment and systems design specifications for implementations of the IECSA. This document would foster the necessary peer review of the IECSA deliverable and its implications on the design of the power system of the future. The results of such stakeholder review and comment would be used to focus and direct IECSA follow on R&D that takes the next step and works to recommend a concrete set of design specifications and test implementations.

The IECSA User's Guide would be a key part of the IECSA workshops discussed in section 6.6.5 below.

Develop Reference Design for Advanced Distribution Automation (ADA)

Multiple projects within and outside of E2I are underway, which involve advanced distribution automation (ADA) and other automated distribution operations (ADO). This area of utility operations, as indicated in the IECSA project, has become increasingly critical for future power system operations, as distributed generation becomes more widespread, market forces call for demand response capabilities, energy is becoming less easily available and therefore more expensive, and financial pressures are requiring more efficient energy transmittal operations.

At the present time, a few isolated implementations of portions of ADA are being undertaken by utilities. However, a full reference design including implementation procedures toward the distribution system of the future has not been developed. Presently, there is no consortium to address ADA; this could be resourced through EPRI, E2I, or CEIDS.

The following steps are recommended to develop and build on a reference design for ADA.

- Develop roadmap for ADA studies and projects toward the distribution system of the future, using expert opinion and stakeholder inputs
- Develop the actual reference design, coordinating across groups which are involved with different aspects of ADA to work toward common goals, including utilities, vendors, integrators, regulators, etc.
- Support ongoing studies, pilot projects, and system-wide projects involving ADA to ensure compliance with the roadmap. Some are discussed in section 6.6.4 below.
- Support periodic updating of the ADA reference design.

Applying the IECSA Reference Architecture to Legacy Systems

The need to integrate legacy systems is far more common than building systems from scratch, and the legacy system integration process is by far more complex. The IECSA Reference Architecture discusses these integration issues, but additional Use Cases, specific application of the IECSA recommendations to these Use Cases, and benefit-cost analysis of these recommended technologies in different legacy systems situations are needed to provide the supplemental information for information specialists to address the problems of their own legacy systems.

Since different types of legacy systems usually present unique problems, seminar material could be developed to cover different types of legacy systems, with experts presenting these seminars to different groups.

Develop Metadata User's Guide

One of the most challenging issues with data management is the fact that different data is needed by different applications. In addition, these needs vary from implementation to implementation, and in the same implementation over time. Using common information models and common interfaces is a major contribution to solving this problem. The technologies recommended in IECSA, such as CIM, GID, and the IEC 61850 object models, provide mechanisms for self-discovery of the metadata describing the data that is available in the network. However, a User's

Guide is necessary to explain to implementers how best to make use of the metadata and self-description concepts, both to publish data and to find the data that is needed. Such a User's Guide should explain:

- Methodologies for categorizing data within servers
- Techniques for making use of multiple hierarchies of data in order to determine the meaning of data that is not yet part of a common information model.

Research must be done to identify what analysis and decision support applications are required to facilitate the creation of a self-healing grid. For example, real time analysis and decision support applications that fuse data from power system security analysis with asset management applications.

These data management methodologies should be used as the basis for the intra-control center testbed project described below.

6.6.4 Recommendations for deployments and construction of reference implementations

Key reference designs

A *reference design* is a document describing the design of a system in generic terms. Multiple vendors can use this single generic design to create their own particular implementations that have value-added features but that are nevertheless compatible with each other. For instance, cell-phone vendors have produced reference designs for the next generation of phones.

The benefit of a reference design is that it reduces the time to develop and deploy a technology within an industry because the common elements of the system are only designed *once*. A vendor using a cell-phone reference design need not research the components necessary to make a new phone compatible with the network, but can focus on meeting specific market needs.

The IECSA team recommends that power industry consortia develop reference designs in the following areas that represent new power utility applications:

- Consumer interface, and in particular a Consumer Portal device (see next section)
- Control and monitoring of Demand Response (Real-Time Pricing)
- Control and monitoring of Distributed Energy Resources
- Organization of Micro-grids
- Energy marketing and trading

The IECSA use cases captured in these areas can be used as starting points for the reference designs.

Consumer Portal

The consumer interface and the home automation portion of the power industry are in significant flux at the moment. There are a huge number of different 'standards' being promoted by different organizations and vendors, with the result that there is very little interoperability.

This lack of standards (or surplus of standards, depending on your point of view) is a barrier to the development of important industry applications such as real-time pricing, demand response, micro-grids, and centralized building automation.

The IECSA team recommends that resolution to this problem focus around the concept of a 'consumer portal', also known as a gateway or aggregator. This portal would be able to convert from various technologies that are used on a customer site, to a common object model and a

smaller set of technologies (or a standard link between new technologies and the internal workings of the consumer portal) that would be used to connect the portal to the utility network.

The steps in this development should be:

1. Develop common object models for various consumer devices. These models would include objects for meters, sensors, controls, appliances, and so on, as well as an object model for the consumer portal itself.
2. Identify and prioritize requirements for the portal itself, starting with the capability to implement the object models for a variety of devices.
3. Work with industry consortia to select a technology subset to enable connecting the consumer side to the energy infrastructure (e.g. power line carrier technologies, XML based transactions and object models, financial transaction models, etc.)
4. Create a *reference design* (see the previous section) for the portal that vendors can use as a starting point for building one. A key part of this design should be that a portal could be embodied on a number of different platforms, such as an appliance, a meter, or as a separate stand-alone device.
5. Work with appliance vendors to develop IECSA-enabled appliances, either directly or through a portal.
6. Encourage pilot projects to demonstrate the technology.
7. Create application notes based on the pilot projects so that subsequent projects can deploy the technology better and faster.

Recommended Field Trials and Pilot Projects

This section provides recommendations for sponsoring pilot projects and field trials in order to:

- Illustrate key IECSA architectural principles.
- Demonstrate interoperability between IECSA devices and systems.
- Develop missing IECSA technologies.
- Develop wrappers, gateways or translators important to the success of IECSA.
- Validate the IECSA work in real-world environments, and provide feedback to CEIDS on the IECSA process.

In general, the IECSA team recommends that CEIDS, E2I, EPRI and other cross-industry organizations monitor projects that are being initiated by utilities, governments, and regulators, and try to introduce IECSA architectural concepts and technologies into these projects. A wide variety of such projects are being initiated in response to the September 11, 2001 terrorist attacks and large-scale blackouts. Initiators include:

- U.S. Department of Homeland Security
- U.S. Department of Defense
- Independent system operators
- State research and development agencies

This section provides a summary of proposed trials and projects. Subsequent sections provide more description of the projects.

Table 6: Recommended IECSA Field Trials and Pilot Projects		
Project Name	Purpose	Highlighted Concept(s)
Eastern Interconnect Phasor Project(	Develop a system of Phasor Measurement Units and associated communications that span the eastern grid	Selection of recommended communication technologies; view of future closed loop control needs
Utility Operations Test Bed	Establish a facility that can be used to test IECSA concepts, and demonstrate several new applications that cross environment boundaries.	Prioritize and implement relevant IECSA environments. Provide the needed test/certification process required. Previous test beds have focused only on a few environments.
DER/ADA Field Trials	Demonstrate specialized advanced distribution automation and Distributed Energy Resources devices/ functions using standardized object models in a real utility/industrial environment.	Implementation and acceleration of object model technologies and ADA algorithms. Highlights the IECSA major conclusion of need for a 'common language'. Links, expands and accelerates the work already in progress.
Harmonized Common Object Models	Demonstrate the benefits of a harmonized 61850, 61968, and 61970 object model.	Highlight the IECSA recommendation for the use of Object Modeling and enable the IECSA 'backbone' common information model.
IECSA-based GIS/DMS Integration	Demonstrate linkage of IECSA architecture with commercially available Geographical Information Systems (GIS) and DMS applications.	Integration of applications to provide the new integrated services of real-time asset management and equipment monitoring.
CEO Portal	Demonstrate that one can use commercially available tools with an IECSA-based architecture to quickly create a website that displays summarized real-time data from an IECSA network.	Use of IECSA concepts; Application of recommended architecture and technologies to provide a centralized, integrated data retrieval service.
Object-Oriented Risk Management	Demonstrate the benefits of performing Risk Management using IECSA-based data integration.	Demonstrate ability to integrate data models; demonstrate ease of implementation using standard tools; provide a vital but missing power system function in risk management.
Phasor Assisted State Estimation/ State Measurement	Demonstrate that synchrophasor information can be gathered from a variety of devices to augment and/or measure system state data from all desired portions of a network. Demonstrate that this leads to improved reliability in simulated emergency situations.	Meet advanced functional requirements identified by IECSA, especially in the Contingency Analysis realm; Apply architectural solutions.
Wide-Area Protection and Control	Apply IECSA vision to the architecture for a Wide-Area protection scheme / liaison with Fast Simulation and Modeling.	Apply the requirements gathering process identified in IECSA; apply existing requirements; apply architectural recommendations
Cross-Organizational Trust Management	Develop a demonstration of security technologies to permit cross-organizational control of power equipment.	Highlight and test the security technologies defined in IECSA
Security Challenge	Demonstrate the use of IECSA security technologies to secure a particular communication link. Identify areas requiring improvement.	Highlight and test the security technologies defined in IECSA.
Independent System Operators Architecture Board Liaison	Develop a close liaison with the national ISO Architecture Board	Promulgation of IECSA vision and architecture concepts
Real Time Pricing Architecture Development	Develop a standard 'model' of a Real Time Pricing architecture	Create IECSA recommendations into a document that can be a model for utilities and regulatory bodies across the country
GridWise™ Coordination	Provide technology transfer into the DOE sponsored GridWise Alliance architecture project	Enable re-use of the IECSA tools, processes, observations, and recommendations
Meta-Data	Test the use of the IECSA-based Meta-Data User's Guide to demonstrate new information models.	Use of self-description and common information models
Inter-Control Center Data Management	Implementing common object models and IECSA-based metadata access methods between control centers.	Further testing of the common IECSA Architecture and access to information models discussed in the Harmonized Object Models project.

Eastern Interconnect Phasor Project EIPP

The Eastern Interconnect Phasor Project (EIPP) has as its objective the establishment of a network of Phasor Measurement Units (PMUs) throughout the eastern US power grid that are networked via Phasor Data Concentrators. Present implementations are based on a communication protocol developed in 1988, which was designed to enable the necessary phasor data to be exchanged on existing 4800 bps communication lines. The proposal is to work with the Standards task force of the EIPP and to recommend architecture solutions based on IECSA

Utility Operations Test Bed

As the utility grid is required to be 'highly available', it is necessary to thoroughly test new technologies in environments that closely resemble the actual operating conditions found in the utility enterprise. To meet this requirement, the recommendation is made to create a Utility Test Bed that can simulate these environments. The test bed would be configurable and adaptable to the environment/technology under test, and to be able to simulate as many of the IECSA environments as possible. This recommendation should be coordinated with NERC and the U.S. Department of Energy.

DER/ADA Field Trials

In parallel with IECSA, work sponsored by CEIDS and E2I is ongoing to develop standard object models for Distributed Energy Resources (DER) in existing and future scenarios using Advanced Distribution Automation. It is recommended that the field trials be covered by the IECSA umbrella, - that is, that all aspects of the field trials be viewed with regard to the overall architecture concept – and that these trials expand their scope to focus on the actual ADA functions and algorithms as well as object models. As such, consideration of interconnection with the various utility control and monitoring centers be considered.

Before executing these field trials, it is necessary to develop an Advanced Distribution Automation reference design, as discussed above in this section.

Harmonized Common Object Models

In as much as one of the primary recommendations of IECSA is the use of Object Models as the common denominator in the IECSA profile, the harmonization of the models described in IEC 61850, 61968, and 61970 is required. To achieve this goal, coordination of this effort is suggested as a follow-on activity. This activity would entail identifying the commonalities and defining the linkages (such as the linkage between a current transformer and the measurement of a current)

IECSA-based GIS/DMS Integration

Demonstrate the benefits of an IECSA based architecture to perform real-time equipment monitoring when displayed in a user-friendly manner. Use a commercial GIS and existing EMS or DMS applications and connect the two based on IECSA architectural principles in a demonstration of how 'off the shelf' applications can communicate in a standard manner, to perform asset management of primary equipment over a large geographical area. The demonstration would compare real-time equipment monitoring data with nameplate specifications, location, and network location to visually display asset status.

CEO Portal

Using the IECSA architecture and 'recommended technologies' list, demonstrate that one can use commercially available tools to quickly create a website that displays summarized real-time data from an IECSA (object based) network, tailored to different users with different interests. Ideally display data from a number of different database technologies, historians and/or data warehouses as well as demonstrating the ease of migrating object based data into data warehouses and historians.

Standards Based Power System Risk Management

Demonstrate the benefits of performing Risk Management using in IECSA based integration infrastructure. As some of the needed financial data objects do not yet exist, part of the task would be to demonstrate how new financial objects could be developed and test the process for submitting them for standardization as part of CIM or 61850.

Phasor Assisted State Estimation/State Measurement

Room for improvement exists in solving the state estimation problem. Present implementations suffer from poor solutions under lost data scenarios and 'loosely coupled' system topologies. Phasor assisted augmentation of State estimators has been undertaken, however, further work/migration to State Measurement is needed. A demonstration is proposed to show that synchrophasor information can be gathered from a variety of devices to augment and/or measure system state data from all desired portions of a network. Show that this leads to improved reliability in simulated emergency situations. This work would most likely require upgrading an existing utility communication network (using IECSA recommended technologies) to accept higher volumes and speeds of data.

Wide Area Protection/Control (FSM Collaboration)

A major component of the Self-healing grid is the ability to dynamically protect and control the electric grid. In a follow-on effort, CEIDS is sponsoring work in a Fast Simulation and Modeling (FSM) project. It is recommended that a liaison be established with the FSM project to enable assimilation of the IECSA concepts into the FSM work. It should be noted that IECSA provides a sound starting point for requirements for the FSM function. It is expected that as FSM migrates into the demonstration phase, the improved reliability benefits from wide area protection and control will become obvious.

Cross-Organizational Trust Management

As more of the electron enterprise is incorporated into the utility communication network, the need increases to demonstrate how IECSA application and security technologies can be used to permit cross-organizational control of power equipment. The proposed task would be to develop an emergency scenario requiring participation and control of the power system by multiple energy organizations, including authentication and establishing a 'chain of trust'. Implement the scenario using IECSA technologies.

Security Challenge Demonstration

Demonstrate the use of IECSA security technologies to secure a particular communication link or set of environments. Identify areas requiring improvement. Build a secure system on the Utility Operations Test bed, issue a 'hacker challenge' and invite a NERC red team evaluation of the network.

ISO Architecture Board Liaison

During the stakeholder engagement process, it was discovered that the Independent System Operators throughout the country have established a national 'architecture' group that looks at communication issues throughout the ISO locations around the country. It is proposed that a liaison be established with this architecture group to provide education on the results of IECSA and to provide guidance as to the application of the results. Input would be made through involvement in teleconferences as well as attendance at group meetings.

RTP Architecture Development

Many utilities, public utility commissions, and energy commissions are working toward developing a Real Time Pricing (RTP) system architectures in order to better manage the supply and demand of electricity. It is desirably that nationally, if not internationally, that a common architecture be applied to this solution. It is recommended that a 'model' of an RTP architecture be developed and be made generally available to the industry. In addition, there is much

opportunity to bring the cross-domain concepts of IECSA to bear on the creation of the 'big picture'.

GridWise Coordination

The GridWise Alliance is a DOE sponsored effort to further the development of an architecture, similar to IECSA, which provides a reference model and guidelines for stakeholder communication and decision-making. GridWise also recognizes the need for an overarching initiative to provide perspective to these efforts as contrary approaches may lead to confusion and duplication of efforts. It is proposed that tight coordination with the GridWise Architecture Board be established so that the results of IECSA can provide a foundation for any architecture work that GridWise may undertake.

6.6.5 Recommendations for stakeholder outreach

Ongoing stakeholder outreach is critical for ensuring successful implementation and adoption of IECSA. In addition to getting the end product into the hands of those who will be building equipment and systems utilizing the architecture, it is essential to extend and build upon the stakeholder outreach conducted during the requirements gathering and development phase. This is necessary to continue collecting additional use cases to support expansion of the architecture as well as ensure awareness and acceptance of it.

Conducting effective stakeholder outreach to potential implementation targets, as well as the various stakeholder publics, will facilitate adoption and implementation as well as reinforce the perceived merits and benefits of the architecture. This can help to inform and obtain support from individuals who may not be directly involved in implementation, but who can aid in getting IECSA before regulators and standards making organizations.

Key goals for the ongoing stakeholder engagement process include:

- Establish and build an IECSA as a brand name within the electric power industry – e.g., 'IECSA Inside'
- Educate audiences on what IECSA is and why it is needed
- Provide timely, accurate information on the IECSA development and implementation process and scope to stakeholders and other interested parties
- Facilitate awareness of what IECSA is (and what it isn't)
- Facilitate stakeholder awareness, understanding, and buy in of IECSA
- Bring to the table and discuss concerns and issues that audiences may have about IECSA and implementing it
- Establish dialogue and facilitate public involvement in the implementation of IECSA on a national and international level and within the various stakeholder groups – utility personnel, vendors, regulators, standards making organizations
- Provide a consistent baseline message to all the stakeholder groups and the general public
- Facilitate the implementation of IECSA within the CEIDS community
- Provide a support mechanism for implementation of IECSA through training programs and ongoing support via a users group
- Lay the basis for IECSA to be incorporated into standards and regulations – ideally as a whole but probably either in pieces or as an example of best practices

Effective stakeholder outreach lays the foundation for implementing IECSA out in the field. Ongoing information dissemination and education/tech transfer will reinforce stakeholder outreach conducted

during the development phase and maintain support for the end product and its implementation. Targeted audiences for these efforts include:

- **Utilities:** There is a definite need to educate utility employees on the vision and value of IECSA; create buy-in of the concept with utility executives; and engage key employees (managers and technical leaders) regarding the architecture to facilitate its adoption and implementation.
- **Regulators and Auditors:** Regulators and auditors have an interest in ensuring that power systems meet their reliability, performance, market, and financial obligations. There is a need to assist regulatory commissions in understanding the nature and need for an industry-wide architecture and the benefits of implementing IECSA.
- **Vendors and Suppliers:** Vendor stakeholders are interested in designing, building, integrating, and servicing products that would effectively become a part of the implementation of the IECSA. These individuals would be adopters of the architecture specifications and associated standards. The purpose of outreach to this audience is to raise awareness and obtain buy-in and acceptance. Many vendors participate in standards bodies and IECSA must be presented in the context of building upon existing standards development work.
- **RTOs / ISOs**: Regional Transmission Organizations and Independent System Operators are responsible for the real-time dynamic operation of the electric power grid. There is a need to continue outreach to gain acceptance of the scope and concepts of the IECSA project. This is an audience sector similar in scope and purpose to utilities.
- **Industry Groups:** Industry groups include utility associations and organizations, customer representative groups, users groups, standards organizations, technology development associations, and other groups involved with energy and technologies. There is a need to build awareness and gain acceptance and support of implementation from industry groups such as the Edison Electric Institute, UCA Users Group, DNP Users Group, ModBus Users Group, NERC, GRI, APPA, ASHRAE, SEMI, 24/7 Group, etc. who represent important sectors of the energy, electric power, related and supporting industries. These groups will play a large part in generating a favorable reception to the implementation of IECSA by facilitating industry sector 'buy-in'.
- **Government Institutions:** Government institutions are looking to the utility industry to develop its own solutions to the new demands of deregulation, security, and enabling technologies. The technologies need to be founded upon existing standards and industry-at-large solutions where possible, but also through the development of architectures and roadmaps that address the unique requirements of energy systems. The governmental institutions need to feel comfortable that IECSA will meet the societal obligations of a reliable and safe power infrastructure, the financial obligations of a fair and strictly managed electricity market, and the security obligations for a robust and flexible information infrastructure able to meet future challenges. The goal of engaging this audience is to educate about the needs and issues of the national power grid as well as to gain acceptance of IECSA from influential agencies or commissions. Government organizations are likely to become a driving force for change and thus, once educated about IECSA, will push for national acceptance of the architecture.
- **End User Groups / Organizations:** Direct end users include those whose jobs would be directly impacted by implementation of IECSA including customer energy managers, energy services providers, and other users. Many energy consumers would fall into this category as well as building owners and consumers whose lives may be impacted by rate structures and other concepts enabled by the IECSA. The purpose is to inform representatives of key groups of energy users about IECSA, its benefits, and how it will be implemented. Interest in IECSA generated by end-users is crucial to initiating demand for the advanced end-user services that the IECSA can facilitate. This in turn results in vendors creating products to satisfy that demand.

- **Standards Bodies:** The purpose of outreach to these groups is to gain acceptance and incorporation of IECSA into current and proposed standards. Outreach to standards groups such as the IEEE, IEC, ASHRAE, NIST, and others will need to continue. These groups are positioned to provide ongoing input for refining and enhancing the architecture as well as playing a large part in facilitating industry sector 'buy-in'. Since an ultimate goal is to standardize the IECSA work through one or more of these organizations, buy-in is critical to the success of the project.
- **International Community**: The United States accounts for only 25% of the world market in utility spending. As such, in order to obtain world-class manufacturer buy-in, IECSA needs to appeal to the larger world market. Learning from the lessons of UCA, we can draw the conclusion that overall acceptance of the IECSA will come only after international acceptance. To that end, it is important to engage international stakeholders in conjunction with the other category groups.

Stakeholder outreach, training and support should consist of the following components

- **Information and Promotion** – to inform the overall stakeholder community about IECSA, the value it provides, and how it can and will be implemented.
- **Education and Training** – developing and delivering training in the development, construction, and implementation of IECSA.
- **Support –** developing and delivering a support mechanism, providing a distribution means and tools for implementing IECSA.

Information and Promotion

The information and promotion component should consist of various communications strategies and tactics, including a rollout event, technical papers, articles, presentations, etc., to raise awareness and acceptance of IECSA within the electricity industry and associate stakeholder communities. Key items include:

- **IECSA Website** – the collaboration web (www.iecsa.org) is already in existence and will require migration to support stakeholder engagement in the development phase An IECSA website will continue to be a depository for press releases, white papers, background materials, Frequently Asked Questions (FAQs) and other content. This material needs to remain publicly accessible (requires no user identification or password) and will be branded as a central destination where anyone can be directed for more information. Getting the site listed with the major search engines will be a key priority. The website will serve as the main avenue for support – housing the help desk/hotline and serving as the gateway for the IECSA users group website. The site will need to be updated to describe the final deliverables and provide a means to operate the support mechanism – hot line, FAQs, etc. Additionally, the site will serve as a depository for new use cases and implementation success stories, utilities using products that utilize IECSA, etc.
- **Brochure** – An overview brochure on IECSA was developed to support stakeholder engagement in the development phase. This brochure could still be utilized, but an expanded brochure should be created explaining what IECSA is, its scope, its benefits, how it will be implemented, and how it will be supported. This brochure could be distributed in hard copy and electronically at conferences, meetings, training events, presentations, and in person-to-person and group interactions. It will also be made available in electronic format on the IECSA website. There should also be an effort to develop a product explaining IECSA in non-technical terms for the general public.
- **Newsletter** – Develop a regularly-distributed newsletter will inform audiences about IECSA, its goals, case studies of successful implementation, scheduled events (training events, annual user group conference), news, etc. The newsletter should be distributed in electronic format to individuals who sign up on the IECSA website, attend workshops, or who are identified as

targeted audiences. A limited number of hard copies could be produced for distribution at conferences, workshops, and other appropriate forums.

- **Briefing Materials** – Presentations on IECSA and the process and progress of the project have already been developed. These should be revised to reflect the final deliverables and focus on implementation rather than on the development. Both short form and long form versions should be developed, as well as versions specifically targeted at various audiences – utilities, vendors, regulators, etc. A presentation describing IECSA in easy to understand, non-technical terms would be useful as well.
- **Conference Presentations and Speeches** – A pool of speakers consisting of key E2I/EPRI leaders and technical personnel, CEIDS partners and advisers, early adopters of IECSA concepts, IECSA and other CEIDS project contractors, and other industry experts should be identified and matched to potential speaking/presentation opportunities. A list of presentation venues running the gamut from 'big think' talks to technical papers should be compiled and speakers targeted at those events.
- **Articles** – as with conference presentations, these would consist of 'big think' pieces targeted towards high-level and general audiences and technical pieces oriented towards key groups – utilities, vendors, regulators, and standards making organizations. Targeted publications range from utility and communication industry trade press to 'op-ed' pieces with bylines for senior E2I/EPRI management that could go into the Wall Street Journal or the New York Times. The targeted audiences for these include policy makers, utility managers, and designers/implementers.
- **Fact Sheets** – these should reflect the final deliverables and address a range of topics related to particular audience groups – utilities, vendors, standards making organizations, etc. These would be posted on the website and made available at workshops, conferences, and events as well as directly to stakeholders.
- **Press Releases and Kits** – There should be a concerted, aggressive process for generating and approving press releases and distributing them. Press releases could be distributed via the wire service utilized by E2I/EPRI and also sent directly to targeted media. Contacts should be made to targeted media to pitch press release and stories about IECSA, especially focusing on demonstration projects and success stories.
- Editors and writers with utility and communications industry trade publications (including websites and information services) as well as general press (particularly business or technology oriented newspapers, magazines, and broad/webcast outlets) can be a key ally in helping to implement IECSA. Effective, positive coverage of IECSA can aid in the implementation process and maintain a flow of information that keeps the various stakeholder groups and general audiences interested. This is particularly important given the demographic and geographic diversity of the various stakeholder groups. Also, media coverage can aid in reaching international audiences.
- **Media Events** – A series of media events should be held shortly after the release of IECSA. These could be held in various locations and possibly in conjunction with already scheduled industry events. The goal would be to provide a venue to reach and inform the press and the stakeholder communities.

Education and Training

A key component in implementing IECSA will be the development and delivery of training programs. This will facilitate transfer of technology as well as build support for the adoption and implementation of IECSA. It is recommended that there be the development, scheduling, and delivery of a series of workshops discussing the benefits and scope of IECSA, the final

deliverables, and how the results can be applied to new systems, legacy equipment, and the entire utility enterprise.

These workshops will range in scope and tone from high-level overview to nuts and bolts "here's the architecture, here's how to use it." This should begin with the development of a series of outlines targeted towards specific audience groups, then move towards development of presentation materials, scheduling the workshops, identification of the best resources to teach the workshops, and actual conducting of the workshops.

The IECSA workshops would be 1-3 days, with 1-3 speakers, depending upon the area and degree of interest. The workshops would include presentations, hands-on examples of using the IECSA Use Cases, hands-on examples of using the IECSA Reference Architecture, and other topics. A key component would be the IECSA User's Guide, discussed above.

It is suggested that the workshops be handled using a 'train the trainer' approach where implementation facilitators undergo training on IECSA and are then 'certified' to teach the workshops to others.

These workshops should be scheduled in conjunction with industry conferences and other events – especially related to the standards making organizations and conducted on both a regional basis and as requested to ensure that everyone has an opportunity to attend a workshop. In addition to in person training, there should be an effort to put together WebEx™ conferences to address audiences – primarily utilities – that have limited travel budgets.

Support

In addition to information/education and training, ongoing support will be a key component in ensuring the successful implementation of IECSA. E2I/EPRI and CEIDS should consider a commitment to making this support available 24/7 to the various stakeholder categories. Key activities include:

- **Support Hotline and Website**. An IECSA Answers Hotline should be established to receive and answer questions. The hotline does not necessarily have to be a 24/7 operation, but there should be experts available to field calls and answer questions. When the line is not staffed, calls should be recorded and followed up within 24 hours. The IECSA website should feature a strong support section housing the final deliverables, training materials, supplemental use cases, and a Frequently Asked Questions page that will address both technical and non-technical questions related to IECSA and its implementation. The site should be accessible to registered users, who would not pay for registration. Also, as implementations are conducted and experience gained, it is important to incorporate lessons learned, new use cases, case studies, and other information into the on-line deliverables section of the IECSA website.
- **IECSA Users Group.** An IECSA Users Group needs to be established and supported. This would be open to membership by any interested party, although utility, vendor, regulatory, and standards making organization personnel would be encouraged to join. The user group would maintain a website located off the main IECSA website and would aid in the development and posting of FAQs, all supporting materials, and assistance with hot line questions. It is suggested that the group be governed by an advisory council of selected individuals representing key sectors – utility, vendor, government, etc. that provide direction to the group and advise on group and implementation activities. The group should have at least one meeting per year that is open to the public and feature both a technical – seminar, workshop – and administrative component targeted at discussion of implementation concerns, scheduling, etc. The advisory council and the group as a whole would provide input into development of information and education materials and the implementation process as a whole. In order to accelerate creation of the IECSA Users Group, it is recommended that the

UCA International Users Group, as a funded and viable body, be considered as a means for making it happen.

6.6.6 Recommendations for integration with other architectures

It was identified in the introduction that the successful enterprise and industry-wide scope of IECSA will interact with in whole or in part parallel efforts by other large stakeholder groups. Included are other key architectures in development at Federal, State and even International levels. It is essential to avoid the need for duplication and proliferation of translation layers and gateways that convergence be pursued between the energy industry and IECSA, and, the following efforts.

Major architectural frameworks:

- Federal Enterprise Architecture
- Department of Defense Architecture Framework (DODAF)
- State Level Architecture Developments
- International Level Architectures

In addition, the following commercial and standards based architectural frameworks will impact products and services of use to the energy industry:

- OMG's Model Driven Architecture, MDA
- ISO/IEC 10746 Reference Model for Open Distributed Processing, RM-ODP
- Grid Computing (www.gridforum.org)

7. CONCLUSIONS

This section presents the conclusions resulting from the development process that took place during the past 18 months. The conclusions are divided into two sections:

- A summary of how IECSA hopes to satisfy the industry drivers.
- A commentary by the project team on the results and the process used to develop them.

7.1 The Initial Steps Have Been Taken: Satisfying Industry Drivers

IECSA was an endeavor to address a set of industry drivers. Specifically, how has the effort addressed these drivers?

Driver 1: Cost effective use of emerging technology

With its emphasis on incremental deployment of applications within a framework of interoperable boundaries, IECSA provides the ability to add functionality without a requisite construction of infrastructure. Yet, as applications cross boundaries they can fuse with others without significant re-engineering, as is the case with today's technical islanding approach.

Driver 2: Higher levels of integration across traditional boundaries

The IECSA has validated the original hypothesis of the energy industry needing higher levels of integration. This was in part validated by requirements gathered within this project as well as by one of the most significant events that occurred in the electric industry's history. The August 14, 2003 blackout brought to the surface many of the technical issues that are directly addressed in the IECSA project and recommendations.

Driver 3: Infrastructure development and standards coordination

The initial steps have been taken to match emerging stakeholder requirements with emerging and developing standards and infrastructure. Many of the key standards and related technologies as well as other key infrastructure elements that can be used as part of an overall industry infrastructure are in development and emerging today. Project recommendations summarized here and presented in greater depth in other volumes point to these technologies based on their ability to satisfy architectural level requirements. More work is required however to bring them into full use to meet the demanding needs of future advanced automation systems.

Driver 4: Responding to new and emerging requirements

By providing a framework for applications integration and development, IECSA provides an ongoing repository for requirements adoption and refinement. By concentrating at the abstract level of IECSA, such requirements can be dovetailed into a growing infrastructure with minimal perturbation of previous applications.

Driver 5: Industry visioning and enabling a robust future

This section briefly reiterates the basic principles of the architecture. The IECSA reference architecture is based on state-of-the-art communications concepts and trends in information engineering, stemming from:

- The description and analysis of communication and information **requirements of power system operational functions**
- The use of **system and data modeling** to capture and analyze these requirements
- The definition of utility-specific **environments** having common sets of requirements
- The use of **layered technologies** to separate levels of abstraction and functionality

- The use of **common services, information models,** and **technology-independent interfaces** to create an architecture that is not dependent on one set of technologies.
- The recommendation of **specific standard technologies and best practices** that can meet the power system architectural requirements
- The identification of **missing or overlapping technologies** as a tool for making **technology recommendations**.

7.2 Commentary on the Process

This section provides the qualitative conclusions of the project team regarding the results of the IECSA project and the process used to develop them. Those preparing to continue the work on IECSA or develop similar projects may find these conclusions useful.

The IECSA team was challenged at the outset to devise a starting point for an energy industry architecture that could evolve, grow, and mesh with the efforts of architecture work in other spheres of commerce and communications. In this time of rapid technological evolution and insertion of communications into every aspect of energy delivery and use, it was necessary to grab a toehold so that projects incorporating communications technologies could have a path towards integration. It is easy for an office worker to upgrade his or her technology with a replacement computer every two or three years. Yet, with capital-intensive facilities such as those operated for the generation, transport, and use of energy, a far longer-term perspective is required.

With these two conflicting goals juxtaposed, the IECSA project was funded and directed to accomplish its work in an 18-month timeframe. Why 18 months? Because a shorter timescale would preclude serious in-depth work, and, a longer timescale would come too late to be useful.

The IECSA team endeavored to take a systems engineering approach to distilling stakeholder requirements into an architecture definition. Due to the large scope of the project, the team focused their efforts in certain areas. These focuses and other observations are summarized in the sections that follow. They are described in roughly the order they were encountered in the project.

All in all, the team believes that an appropriate balance was indeed achieved in the varied activities of the project. Obviously, time will tell whether this is correct, and, we will have to observe the application and extension of IECSA to ultimately judge these choices.

Depth vs. Breadth

During Task 1, the team sought to identify an appropriate goal for coverage of utility operations for the project. We quickly found that the most architecturally interesting future applications for the industry involved transfer of information across departmental and institutional boundaries, and especially, involved varied interactions with customers. The team agreed that if we studied the communications requirements of these cross-organizational types of applications, we could identify most significant industry requirements. This is especially true because those communications that remain within a constrained environment are already well understood and often covered by well-documented industry standards and art.

The IECSA project was able to study communications requirements from markets to consumers, from power plants to substations and pole-tops, and permutations of this breadth. For depth, the applications were studied with a primary focus on the identification of the participants in communications, the kinds of information exchanged, and, the simplified exchange sequences that would typify such applications.

To bring the applications that were reviewed in this manner to the point where the documentation fully specifies an implementation would require several additional levels of detail. It would be necessary for the models of data to be exchanged and all the details of the exchange sequences,

fault accommodation and recovery, etc. to be captured. As noted elsewhere in the Conclusions and Recommendations, IECSA is an ongoing process, and further development of the depth of analysis would be very useful.

Stakeholder Requirements

A pure systems engineering approach to any problem will use stakeholder engagement to obtain requirements from potential users and providers of services. Systems architects then analyze these requirements in a formal process to identify commonality of need and the technically detailed design requirements they imply.

In the IECSA project, stakeholder requirements were captured primarily through the development of a document called the 'Domain Template'. This document and process were designed to obtain detailed information from 'domain experts' so we could obtain a quantitative view of industry application requirements. This process is described in Volume II.

While we had great success in obtaining entrée to those experts in the industry that could provide us with input, these same experts had very limited time with which to devote on our behalf. Therefore, in most cases we first populated a series of Domain Templates from the knowledge and experience of the members on the team. We then presented these for discussion with industry experts to refine their content. In a few instances, we were actually able to obtain full Domain Templates from specific stakeholders, but these cases were not very common

It would therefore be desirable to populate a greater number of Domain Templates. While the project applied the 80/20 rule, the last 20% of potential applications can be expected to introduce some new concepts. This will be recommended for future work.

Functional Requirements Analysis

The IECSA Domain Template incorporates a detailed spreadsheet. This spreadsheet identifies hundreds of potential architectural requirements that are evaluated by the analyst for each of the specific steps in the implementation scenario being described.

This analysis was time consuming and proved to be beyond the effort that the stakeholders were able to invest. Therefore, based on the engagement interviews, members of the IECSA team performed this analysis on most of the Domain Templates. Several of these spreadsheets were not completed, and it would be desirable to complete this in the future.

Mapping to UML

The requirements were represented in the Domain Template in the form of a natural language document and an analysis spreadsheet. The template was arranged to have a careful and specific correspondence to RM-ODP constructs, the methodology adopted by the team. These same constructs were then represented in UML using an automated tool, for import into the Magic Draw modeling tool.

It is possible to achieve several roughly equivalent mappings that make logical sense in UML. Ultimately, the team chose an approach that would optimize the match between the modeling tool, the feature set of the Domain Templates, and the relationships we wanted to preserve. The team was able to achieve a substantially satisfying result in this manner. The resulting model carefully preserves all of the semantics obtained through the Domain Template capture and analysis process, and provided an explicit means to correlate actors, information objects, data exchanges, requirements, services, environments, and technologies

However, we used more of a reliance on tagged values (a UML extension mechanism) than we would have desired, due to their unique ability to hold multi-valued constraints (a technical but important detail). In the future, we might prefer to use UML constraints rather than tagged values because they explicitly describe constraints on interfaces, objects and methods.

Template Import

The templates were designed to be self contained and populated by independent individuals and groups. After they were internally complete, a normalization process was used to make the nomenclature used in the various templates consistent with each other. This process of normalization tended to be time consuming since the many objects identified in each template – actors, information objects, etc. needed to be compared to similar ones from other templates. A from/to list had to be constructed and the results reviewed to ensure consistency and sanity of the results.

Although tedious, this was considered a preferable approach to trying to coordinate all template population efforts to use a consistent nomenclature while the nomenclature was being discovered through the engagement process. However, in the future, the extensive list of names (terms) identified can be used in subsequent uses of the template as a suggested list to avoid redundant creations.

Parallel Studies

While the stakeholder engagement process was expected to derive substantial requirements from an application standpoint, the team believed that it was necessary to perform a parallel investigation into general topics such as security and network management, and, the relationship of IECSA to other architectures. This analysis was able to produce the next level of detailed requirements that are beyond the scope of most stakeholders, yet crucial to the proper operation of a distributed computing environment.

The IECSA model of services first relies on a set of simple primitives. These primitives can be combined to allow high level services to be described. In the course of the project, it was possible to identify an extensive set of high level abstract services and to somewhat represent their relationship to architectural elements of IECSA. However, there was not sufficient time to apply these high-level services to the individual steps in the Domain Template scenarios as would be desirable. All the necessary information is in fact in the IECSA model to permit this to be done. It is suggested that this might be a desirable component of future work.

Aggregation of Atomic Requirements

The requirements that were filled out in the spreadsheets associated with the Domain Template were termed the atomic requirements/questions because they were formed as questions using terms that would be familiar to power system engineers. These 400 atomic requirements/questions were therefore combined into 63 Aggregated Requirements that more clearly identified the architectural requirements. Examples of this mapping from atomic requirements/questions to Aggregated Requirements are:

- "Are the distances between communicating entities a few to many miles?" plus "Location of information producer (source of data) is outside substation, or another corporation or a customer site while the Location of the information receiver is outside a substation, or another corporation or a different customer site" became the Aggregated Requirement to "Support interactions across widely distributed sites"
- "Eavesdropping: Ensuring confidentiality, avoiding illegitimate use of data, and preventing unauthorized reading of data, is crucial" plus "Information theft: Ensuring that data cannot be stolen or deleted by an unauthorized entity is crucial" became the Aggregated Requirement "Provide Confidentiality Service (only authorized access to information, protection against eavesdropping)"

Development of IECSA Environments

During the analysis of the communication and information requirements of the power system functions, it became clear that the nature of these requirements depend upon a few factors:

- Locations of the entities exchanging information: some were within a particular site, while some involved inter-site exchanges
- The response times and availability required by the functions: some required very rapid, deterministic information flows, while others had less stringent constraints
- The criticality of the information: some information flows were very critical to reliable and safe power system operations, while others had less impact
- Organizational boundaries: some information remained within one organization, while other information flows involved multiple organizations

Atomic Requirements Approach. The atomic requirement correlations were analyzed against technologies and services in spreadsheets and the resulting relationships were imported into the UML model in order to provide a complete integrated object model. The IECSA team is made up of primarily energy industry domain experts. As such the perspective and experience of these members is a necessary and valuable ingredient in the knowledgeable analysis of the data. However, in order to minimize bias in this analysis, the correlations were captured at a more or less 'microscopic' level – that of the individual requirements. This process is based on the idea that if technologies are correlated to individual requirements, and the environments are correlated to the same requirements, there will be a best fit between a set of technologies and the description of an environment. This greatly simplifies the specification process.

Unfortunately, there was not enough time in the project to both capture this detailed analysis and devise an automated optimization tool to distill its results that could be verified to be more accurate than expert opinion. Therefore, while we made the analysis as objective and specific as possible, no such analysis can be performed without the need for educated judgment and this was applied.

Aggregated Requirements Approach. In parallel, the 20 IECSA Environments with their characterizing Aggregated Requirements were linked to the standard technologies, common services, and best practices, using expert opinion from the IECSA team's combined deep and broad experience in the utility and communications industries. Although this approach might have permitted some bias, it was believed that the checks and balances of the different experiences of the team members, combined with long, in depth discussions of the different technologies, have prevented any substantive bias.

This spreadsheet was then used to create documents for each Environment, listing the categorizing Aggregated Requirements and the associated links. These Environments can be found in Volume IV Appendix E and on the IECSA website.

IECSA Web Pages/Website

The IECSA Reference Architecture, the results of these analyses and linkages, along with the key discussions on communication architectural issues were designed to be directly migrated onto the IECSA website. This website will permit users to have more direct access to the IECSA work through standard browsing techniques.

IECSA is indeed a member of the digital society.

Areas Beyond the Scope of IECSA

IECSA makes no recommendations in the following areas because they are considered to be beyond the scope of this project.

Table 7: Areas beyond the scope of IECSA.			
Name	Description	Reasons for Exclusion	Exceptions
User Interface	All information exchanges that were identified as occurring between people and devices in the use cases.	Do not address communications between computer systems.	None.
Industry Organizational Changes	Changes to the overall business and regulatory structure of the industry.	Not technological issues.	Sometimes discussed with respect to a single organization, as needed to deploy particular strategies such as security.
Algorithms and Applications	Details of particular algorithms, such as load shedding, volt/VAR control, or auto-restoration.	Subject to rapid change and innovation, and therefore not a part of a long-term architectural specification.	Where the requirements of particular applications have a specific effect on the communications system, e.g. protection in general, but not specific protection schemes.
Electrical Power Trends	Emerging trends or ideas that have solely to do with the power system, e.g. the use of more DC links	Not communications issues.	Where trends have an impact on the communications system, e.g. the trend to using more DC links does not affect communications, but the trend to more demand-side management does.
Electronic Media	Applications involving the transmission of audio or video within the power system communications network.	To limit the scope, since the logistics and bandwidth needed to implement such applications may outweigh their benefits.	None.

IECSA Project cannot mandate – only recommend

Architecture documents formally developed by enterprises and government are typically characterized by calling out the use of 'mandated' standards (and associated technologies) as well as 'candidate' standards for use in developing information systems. Mandated standards are those that must be adhered to while candidate standards are those that are maturing and may be mandated at a later date. The IECSA project does not have a charter to mandate use, and therefore may only recommend use and back these recommendations with analysis. Users may review both the recommendations as well as the supporting analysis to determine the strength of the recommendation.

Not the Final Word

The work of IECSA is not done. In fact, it has only just started. As noted in the Project Summary, three key steps of system architecture design remain to be executed:

- **Testing** the principles of the architecture in prototypes and pilot projects.
- **Implementation** and validation of the design in real-world, large-scale systems.
- **Integration** of the lessons learned into further iterations of the process.

In addition, for the vision of a safe, self-healing, reliable, optimized, and customer-integrated power network to be realized, the industry must make a cultural and organizational commitment to the *concept* of a common architecture.

For we must admit to ourselves that the digital society has arrived, and we definitely must ensure our industry becomes part of it; but most importantly, we must realize that it is our responsibility to *keep it running.*