Microsoft Power and Utilities

Smart Energy

Reference Architecture

October 14, 2009

www.Microsoft.com/Utilities

The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.

This Reference Architecture is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT.

Contents

Figures

The Microsoft Smart Energy Reference Architecture

Introduction

The structure, engineering and objectives of the world's power systems are undergoing dramatic rethinking and significant change. New driving forces – like climate change, novel market participants such as plug-in hybrid electric vehicles, and increasing energy demands – are combining to drive the development of what is being referred to as the smart grid.

Many observers believe that the extent of change and its impact on societies could be on the same scale as the inception of the grid itself and will affect every single part of the power utility industry.

Because of the wide range of the participants who will be affected by this transition, Microsoft believes it's more accurate to refer to the new utility landscape as a "smart energy ecosystem" that's collaborative and integrated.

As a result, Microsoft is focused on enabling the technology innovation and advancement needed to create such an ecosystem.

Around the world, governments and standards bodies at all levels are considering or adopting various foundational elements of the smart energy ecosystem:

- The European Commission has created an initiative called the European Technology Platforms (ETPs) for creating the electricity networks of the future.
- China has announced an aggressive framework for smart grid deployment and is supporting it with billions of dollars.
- The International Electrotechnical Commission (IEC) is spearheading a global initiative to support the new "smart" electric power grids around the world with a comprehensive framework of common technical standards.
- The Institute of Electrical and Electronics Engineers (IEEE) is developing a Draft Guide for Smart Grid Interoperability of Energy Technology and Information Technology Operation with the Electric Power System (EPS), and End-Use Applications and Loads called IEEE P2030.
- In the United States, the National Institute of Standards and Technology (NIST) is leading the effort for developing a framework of Smart Grid standards for device and system interoperability.

Microsoft is committed to supporting these global efforts by taking a leadership role in the development of the smart energy ecosystem.

Anoop Gupta, Microsoft Corporate Vice President of Technology Policy and Strategy, summarized Microsoft's contribution to this body shortly after his May meeting at the White House with U.S. Energy Secretary Steven Chu and U.S. Commerce Secretary Gary Locke:

> "The energy grid becomes 'smart' by injecting software into the various control points in the grid, so that people and businesses have ready access to timely, user-friendly information that can help them make smart choices about their energy use. We can envision a world where thousands of smart appliances can seamlessly plug into homes thanks to common standards and interoperability frameworks, just as the 'plug and play' model allows thousands of devices to seamlessly plug into PCs today."

In addition to the role that standards' play in enabling the development of the smart energy ecosystem, Microsoft views as equally important the establishment of an architectural philosophy with a vision and strong foundation for migrating to the new infrastructure and services necessary to monitor, control and report on the assets of this new power system.

In support of that view, Microsoft has endeavored to offer this reference architecture to articulate an industry vision for the smart energy ecosystem. Observers will note that this architecture is designed to maximize agility and enable role-based productivity while ensuring secure IT and operations with the very best ROI for all participants of the smart energy ecosystem, both now and as system requirements expand to meet the increasing complexities of the market. Our reference architecture is comprised of four major sections that seek to address the questions and concerns of differing audiences:

- The first section, **Evolution of the Grid**, describes the forces shaping industry direction and is intended to provide an overview of the challenges coming to the fore.
- The second section, **Changing Demands on the Business**, offers an industry architectural vision that details the entire value chain from the utility to the end-use consumer, whether they are commercial, industrial, or residential. Business decision makers will gain a greater understanding of the business challenges they will face as the smart energy ecosystem emerges.
- The **Architecture** section will be the most useful to software developers, system integrators and solution specialists who already have an in-depth understanding of the industry and information architecture and are most focused on Microsoft technologies.
- The **Microsoft Technology Stack** section identifies Microsoft products and solutions, as well as partner-led solutions in some cases, that enable this architectural vision.
- Finally, throughout this document we offer detailed guidance and hyperlinks to the specific topics and solutions mentioned. The document provides references where available and applicable to accelerate development and guide deployments for the smart energy ecosystem.

Even while we endeavor to offer this view of an underlying framework, Microsoft urges the reader to acknowledge with us that the achievement of the smart energy ecosystem is a journey and not a destination.

This reference architecture seeks to establish a vision that maximizes Microsoft's value to customers by articulating a clear vision for the smart energy ecosystem and then describing the Microsoft and partner

technologies that can realize that vision. Just as the smart energy ecosystem initiatives are global in nature, Microsoft has endeavored to present globally applicable reference architecture.

1.0 Evolution of the Grid

Historically, the electricity grid has been an infrastructure deployed by utilities with the arguably "simple" mission of transmitting electricity from generators for distribution to customers. The basic electrical components that comprised the grid included objects such as generation plants, transformers, conductors, circuit breakers, fuses, switches, capacitors and machines.

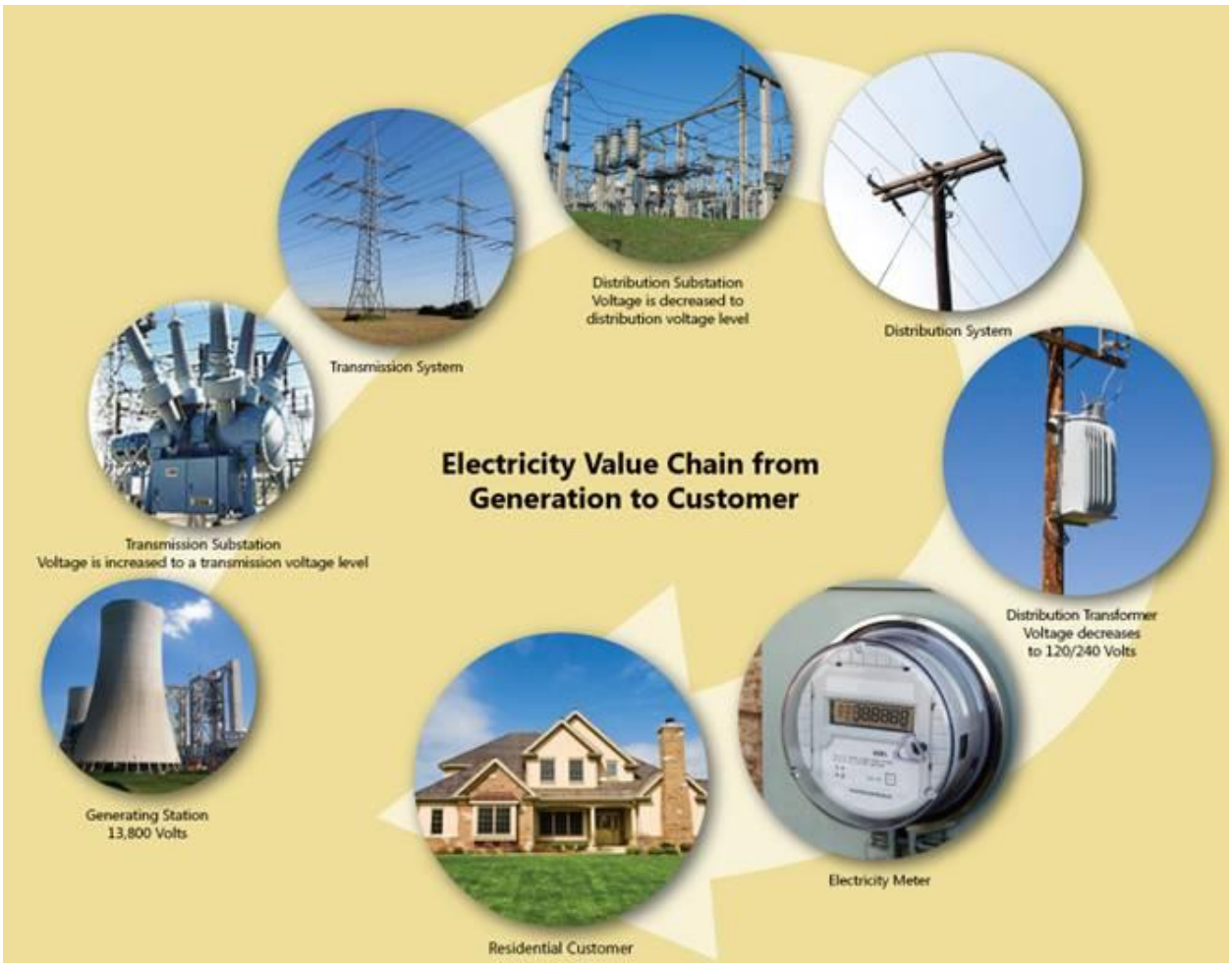

Figure 1 - Electricity Value Chain from Generation to Customer

This infrastructure is monitored and controlled by a set of devices that communicate with each other and various control centers through a field network.

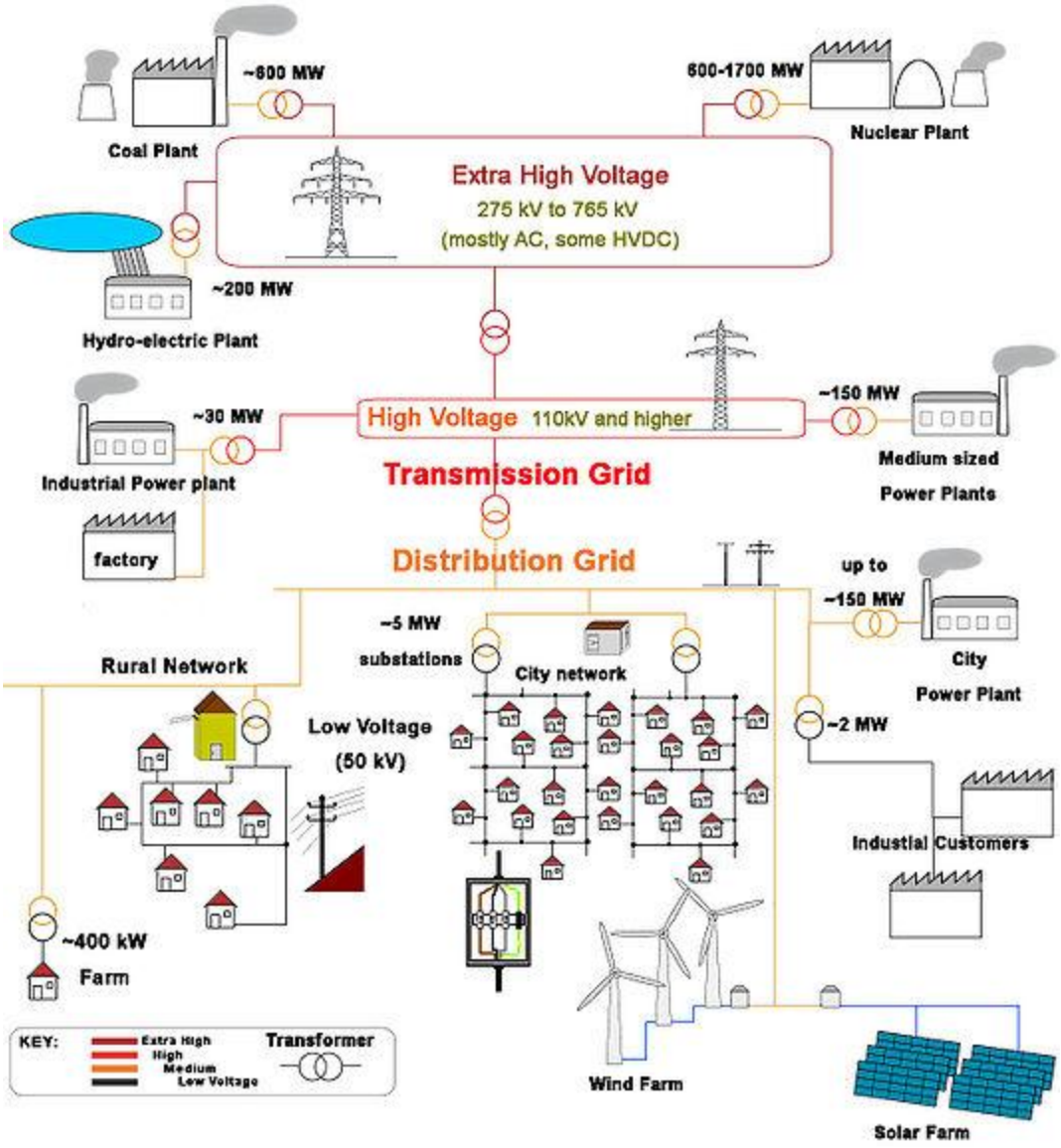

Figure 2 - Broader Perspective of Electricity Value Chain (Source: Wikipedia)

As technology has advanced with dramatic improvements in microprocessor, software and communications, these grid-enabling devices have been increasing in capability (and quantity) to the point that not only can they take measurements and respond to commands, but they also react independently and cooperatively with other devices in a coordinated manner in the field. This level of device-oriented collaboration has now extended past the substation to devices on feeders, to distributed resources, and to end-use customers.

As example, phasor measurement units (PMUs) are just one important improvement in device capabilities that's occurred as a result of advanced technology development. By using accurate GPS synchronized clocks, PMUs are able to measure power frequency phase angles at many points on the grid, allowing for game-changing improvements in real-time monitoring and analysis of the grid. PMUs

will help with grid operation and visualization, as well as supporting reliable and automated incorporation of variable power sources like wind and solar into the grid.

As technology has advanced, so have industry standards. Funded by utilities, the Electric Power Research Institute (EPRI) led several efforts to address interoperability issues. The results were then advanced to the International Electrotechnical Commission (IEC) for standardization and led to the development of active users groups. These included the:

- Inter-Control Center Protocol (ICCP)
- Utility Communication Architecture (UCA)
- Common Information Model (CIM)

Other standardization efforts are worth mentioning as well:

- The IEEE, a professional association for the advancement of technology, has helped create many important communications and power engineering standards.
- In 2004, the U.S. Department of Energy (DOE) and the GridWise Alliance agreed to work together to realize the vision of a transformed national electricity grid in the United States.
- An effort from the International Council on Large Electric Systems (CIGRE) called D2.24 is driving requirements and architecture for next-generation energy market and energy management systems.
- Standards developed by the IEC and IEEE are now finding their way into NIST-led efforts related to the Smart Grid.
- Finally, as the Smart Energy Ecosystem evolves to include the end use consumer, either commercial or residential, Web services standards bodies such as OASIS will play a greater role.

1.1 Emergence of the Smart Energy Ecosystem

A smarter grid comprised of these new or improved grid connected devices will enable the smart energy ecosystem to offer many new capabilities that respond to, as well as drive, changing consumer behavior and attitudes toward energy.

For instance, the smart energy ecosystem will likely need to accept power coming from the solar arrays on the rooftops of commercial buildings and private homes. It will also need to incorporate power coming from strong, but variable, wind farms. When millions of individuals own plug-in hybrid electric vehicles (PHEVs), a smart energy ecosystem will conceivably allow them to buy electricity from the grid during late night, non-peak hours. Then, if the grid needs power during peaking events, the utility might draw from the stored power in those very same PHEVs.

Figure 3 - A Smart Energy Ecosystem Driven by Innovation

Indeed, utilities are already deploying many devices with the microprocessors and two-way communication that will enable a wide variety of capabilities not possible before, including collection of more information, local decision-making and coordination.

1.2 Participants within the Smart Energy Ecosystem

There is a wide and growing set of active participants within the smart energy ecosystem, each having its own roles, interests and associated responsibilities. Participants can be organizations, people and intelligent devices and include:

- Utilities and related companies, including:
  - Distribution companies
  - Independent System Operators (ISOs)
  - Regional Transmission Operators (RTOs)
  - Transmission market operators
  - Transmission companies
  - Generation companies
  - Distribution balancing authorities
- Service providers, including:
  - Energy aggregators
  - Maintenance service providers
  - Metering service providers
  - Weather forecasting
  - Retail energy providers
  - Equipment providers (PHEVs, solar panels, storage, etc.)

- Customers, including:
  - Residential
  - Commercial
  - Industrial
  - Governmental

PJM Interconnection developed the following diagram to illustrate the different actors in the smart grid and how they communicate and collaborate to accomplish their various roles.

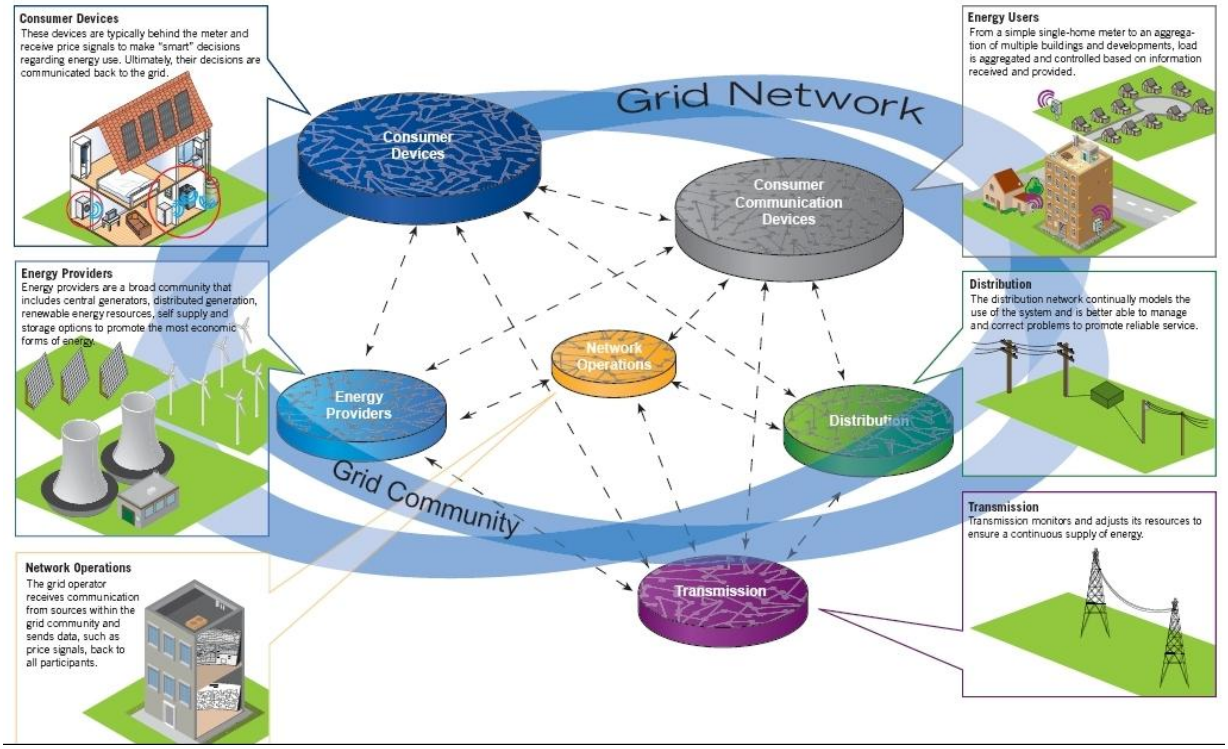

Figure 4 - Smart Grid Participants (Source: PJM Interconnection)

The reference architecture that follows describes how these participant interchanges will work, and provides guidance for implementing these systems based upon Microsoft platform technologies.

1.3 Collaboration within the Ecosystem

By viewing the smart grid as an energy ecosystem, it becomes immediately evident that there is serious need for that grid to be enabled by collaboration between organizations and equipment.

Collaboration and associated business processes must occur between users, businesses, individual customers, and a variety of technology systems, resources and intelligent devices. Collaborative relationships may be cooperative or competitive. Utilities and market operators may cooperate to resolve a critical outage that threatens grid stability. Market participants may collaborate with the electricity market in a competitive environment.

Indeed, collaboration must occur for many purposes:

- To operate the electricity grid
- To buy and sell energy through an energy market
- To cost effectively utilize energy
- To participate in energy (e.g. demand response, efficiency) programs to better manage use of energy
- Scheduling of resources
- Scheduling of consumption
- Settlement of accounts
- Maintenance of the electrical infrastructure

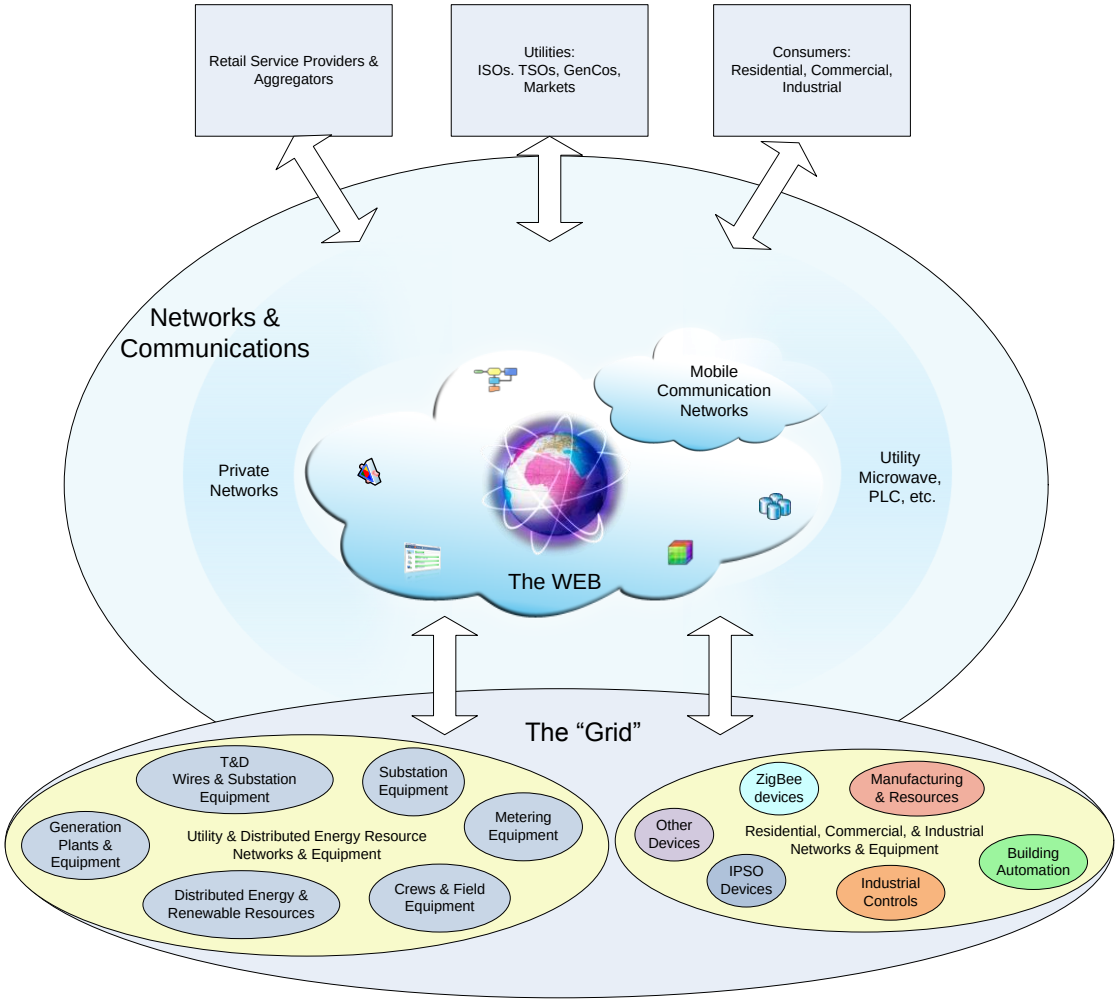

Figure 5 - Overview of the Smart Energy Ecosystem

Responsibilities within the ecosystem are federated, where there may be interactions between different types of organizations, as well as their interactions with the electricity grid and customer infrastructures. Some organizations may take on multiple roles, as in the case of a vertically integrated utility that may have combined responsibilities for generation, transmission and

distribution. There also may be many types of service providers, such as those offering metering, maintenance, weather forecasts or load aggregation for participation in demand response programs.

In addition, all of them will need to interact and collaborate. Historically, participants have been people or organizations, but the capacity for local decision making by devices extends the participant/participation model.

2.0 Changing Demands on the Business

The new smart energy economy will cause utilities and market participants to engage in a variety of new relationships and to adopt business models that will evolve as the shape of the smart grid becomes more evident and opportunities present themselves.

In fact, we believe these new relationships and changing business models will be one of the more interesting outcomes as the smart grid evolves. This new business environment will make it imperative to have a readily understood architecture in place to aid the capture of those opportunities as they arise.

This section considers:

- Energy Resources and Constraints
- Business Factors
- Technology Enablers

2.1 Energy Resources and Constraints

The increasing diversity of energy resources will be one notable driver of new business models.

For example, while wind, solar and other forms of distributed energy generation are becoming common and more cost effective, they have far different operational, economic and control characteristics than conventional plants. Consider the operational complexity when a utility combines such variable generation sources with demand response, where the energy not used (sometimes referred to as a 'negawatt') can be considered an energy resource if demand can be controlled.

This new and very diversified generation model (of renewables, distributed generation and so-called 'negawattage') transforms the electricity grid from an operating model where power flows one way starting at a reasonably small set of generation plants, to that of a two-way flow with a mixture of a large number of small, medium and large energy resources, many having much more diverse operational characteristics. As mentioned previously, one extreme example of this dynamic will occur when the batteries in PHEVs are used as storage for the grid, where they can be drawn upon as energy resources as needed during peak hours and then recharged during more cost effective off-peak hours.

Today though, the transmission grid has operational constraints that still need to be carefully managed. Distribution network constraints will become more apparent as consumers purchase more PHEVs and deploy more distributed resources. Where a distribution feeder may have been designed for average customer loads of 1.5KW, the charging cycle of a single PHEV can add a load of up to 20KW. As more PHEVs come onto the grid, they can easily exceed the capacity of a distribution feeder, requiring large scale physical upgrades and/or coordination of PHEV recharging. The utility will prefer the coordination option, in order to minimize peaks and provide for balanced operation of feeders within their designed limits.

Finally, new factors and their constraints are emerging around the basic utility function of metering. In the past, it was only possible to measure usage for all but large consumers on an aggregate monthly basis. With advanced meter deployments, it is now possible to measure usage for all customers in near real-time on an interval basis, where all customers' usage may be reported every 15 minutes. Such interval reporting provides new opportunities to charge customers more for electricity consumption during more expensive peak hours, or provide reduced rates for usage during off-peak hours. This time-of-use pricing provides customers with the incentive to change their consumption behaviors and/or leverage devices within their home or business to rationalize overall energy costs. The communication infrastructure used for the advanced meter then becomes a gateway between the customer and utility or service providers for additional services including demand response, outage detection, power quality monitoring, etc.

2.2 Business Factors

The wide variety of economic and technical changes that will occur with the advent of the smart energy ecosystem will require everyday business processes to increase in their ability and flexibility to adapt.

The new marketplace will offer many new opportunities to profit – if a company can change its business processes quickly and cost effectively. Such flexibility will require an information technology architecture that supports and anticipates each next stage of the evolution toward the smart energy ecosystem. The architecture's value will be gained from the implementation's cost effectiveness on the ongoing evolution of specific business process. In fact, that ongoing flexibility and capability to adapt will be the primary reason that an architectural framework is needed from the outset. The following industry issues demonstrate the challenges facing utility businesses and the technology solutions that may address them.

2.2.1 Utility Workforce Optimization

Like companies in other industries, utilities face mounting pressures to minimize the number of people needed to support their business processes. Whereas business process execution in the past may have required several persons with knowledge of specific applications, it is now possible to leverage workflow technologies to hide the underlying application details from users. Doing so can provide users with a simplified, streamlined view of the process so that it can be executed more efficiently, even with less training. Workflow technologies also automate

many steps and avoid redundant data entry, improving accuracy and efficiency and ensuring that business process execution follows corporate compliance policies and procedures.

2.2.2 Workforce Demographic Changes

The architecture supporting the smart energy ecosystem will also need to consider and enable new dynamics occurring within the changing utility workforce. Much has been written about how the aging of the baby boomer generation will equate to senior resources – and their experience – leaving the workplace. In addition to the proverbial brain drain, a new workforce demographic will demand new work tools: the so-called millennials who are entering the workforce have heightened expectations for sophisticated tools they'll be using to execute the utility's work processes.

These dynamics will drive businesses to seek technology systems that will address both workforce demographic challenges. Those businesses that adapt the most quickly to these changing conditions will benefit more quickly. But in order to achieve this flexibility, people throughout the business will require timely access to information they need in a form they can use, through tools that create collaboration, knowledge management, data repositories and process integration. Businesses will need an architecture that is able to support pragmatic integration as an enabler of their evolution to the smart energy ecosystem.

2.2.3 Equipment Collaboration Optimization

Adding equipment to the grid also serves as an example of a process where workflow automation can facilitate the updating of planning and operations models, as well as asset management systems, geospatial information systems, and, potentially, customer information systems (in the case of phase rebalancing).

2.2.4 Outsourcing and Contracting Optimization

Utilities are now contracting new or outsourcing existing services from specialized service providers. This practice increases the need to shield enterprise applications from direct access, leveraging façade patterns that may be implemented using workflow or portal technologies. The outsourcing and contracting dynamic also creates need for location agnostic access, while at the same time highlighting the need for a robust multi-enterprise security infrastructure. Utilities might consider cloud services as a potential strategy if security and performance considerations are properly managed in the solution.

In sum, as customers leverage technical advances and rationalize their energy consumption, and as other outside factors affect how utilities must change their business operations, utility companies will need to leverage a variety of technical and business innovations to assist their journey toward a smart energy ecosystem.

2.3 Technology Enablers

The technology architecture of the smart energy ecosystem won't be confined to the need to revise business practices for workforce, consumer and regulatory changes. It will also need to be an enabler of new technologies, some we know about, and some that are yet to come.

2.3.1 Advanced Sensors and Web Integration

New, advanced sensors will expand the capabilities of the smart energy ecosystem with increased integration with the Web. These include:

- Global Positioning Systems (GPS)
- Phasor Measurement Units (PMU)
- Interval Meter Readings
- Centralized Remedial Action Schemes (C-RAS)

For instance, by leveraging technologies like GPS, it is now possible for devices to take measurements with a very precise view of time. This makes it possible to measure phase angles at locations on the grid using PMUs and to take grid-wide measurement snapshots. Interval meter readings will enable more accurate load models.

Together, these technologies provide new opportunities for improvements in network analysis, monitoring, and control, thereby offering improvements in grid stability and security, as well as facilitating better grid utilization.

Another example of advanced sensors and Web integration is C-RAS. Utilities have demonstrated that C-RAS can be used to create fast grid event mitigation schemes that can lead to material reduction in reserve margins while maintaining or improving overall reliability. The ability to automatically trigger pre-enabled grid response actions greatly enhances autonomous reliable grid operation.

Other core components of the smart energy ecosystem technology architecture will be the Web technologies, integration standards and related products that now offer increased collaboration at many levels. These technologies provide opportunities for more pragmatic, lower cost implementations and will overcome previous cost barriers to integration.

2.3.2 AMI and Communication Networks

Advanced metering infrastructures (AMI) is yet another important enabler that some people often consider synonymous with smart grid. Because of its two-way communication capabilities, AMI has created many new opportunities including:

- More timely measurement of usage, providing opportunities for new pricing options beyond billing that's based on total monthly consumption.
- Automatic detection and confirmation of outages, with automatic verification of restoration.
- Detection of customer-level power quality issues, such as momentary outages and voltage levels.
- Providing a gateway to home area networks, such as those now provided using ZigBee, where home devices can react to pricing and load control signals as needed to implement demand response programs.

- Management of schedules for local energy consumption, where the user can minimize costs based upon their preferences and the utility can balance loads and make better utilization of the distribution networks.

Because of their role as an enabler of the smart energy ecosystem, communication networks should be considered a primary component in any architectural blueprint. The field networks currently used to communicate with AMI devices are typically private, often using proprietary or utility industry-specific protocols.

Alternatively, broadband internet services offer a communication infrastructure that is open, cost effective, higher bandwidth and already widely deployed.[1] Because it is already deployed, it is already cost competitive with the lower performing utility-specific infrastructure. The recent FCC commitment to "net neutrality" removes the biggest remaining broadband concern. As long as security is addressed up front, metering and home area network (HAN) communications infrastructures allow new families of devices to be added to the set of monitored and controllable devices on the grid, including:

- Smart thermostats
- Smart appliances
- Plug-in hybrid electric vehicles (PHEVs), which can be in states for charging, storage and discharging
- ZigBee[2] Smart Energy (SE) profile devices
- HomePlug devices
- IPSO devices
- Residential solar and wind
- Building automation

A new generation of field and home devices that have the ability to make local decisions using two-way communication capabilities will allow customers to better monitor, control and schedule energy consumption, as well as respond to demand response events and pricing signals. Utilities or independent service providers could use these devices to extend their operational capabilities by facilitating registration of the devices in energy programs that permit the power provider to adjust schedules to provide more efficient and balanced operation of distribution networks.[3]

---

[1] It should be noted that there is a price for openness and cost effectiveness: As metering infrastructures and gateways to HANs leverage the internet, the overall architecture must pay careful attention to security issues.

[2] ZigBee is a set of specifications created by the ZigBee Alliance and built around the IEEE 802.15.4 wireless protocol, and targeting low-power, low-cost, sensor networks.

[3] It is also import to note that HAN technologies provide a monitoring and control infrastructure that can extend beyond electricity to include other energy and non-energy related services including: gas; water, home security, home monitoring and remote control; pre-payment metering services and home healthcare.

2.3.3 New Computing Paradigms

New computing paradigms will require new approaches to the smart energy ecosystem. These paradigms include:

- Computing technologies
- Advances in storage
- Advances in communications technology
- Scale
- Participation of unreliable entities

For example, multiple cores in processors will be commonplace. Applications will need to transition to multi-core, multi-processor, multi-threaded design. Inexpensive, low-power, massively-parallel computing will dominate infrastructures and drive application design. Even while preserving existing investment through co-existence, application disaggregation will be necessary to capitalize upon new hardware platforms.

In addition, communication capacities – both wireless and hardwired – continue to expand. Indeed, bandwidth is expanding faster than Moore's Law. However, the communication can be unreliable, either at certain times or geographic locations (commonly referred to as "cell holes"). Solutions will need to be flexible and resilient to momentary loss or interruptions of communication. As a result, autonomous operation will need to be a constant consideration.

The scale of connected smart energy systems will grow to new levels with the addition of the active participation of loads (end-use customers) and a multitude of tiny new devices. Tight coupling of unreliable autonomous participants will be proven unreliable. Systems will need to be designed to be flexible and adaptive to autonomous behavior. The true measure of success will be building a working system out of small autonomous independent unreliable devices and participants.

As a result, for some parts of the smart energy system, mastership cannot be assumed. The system will require design that should expect the same computing problem to be addressed in multiple locations. For example, micro-grids and integrated control centers may both calculate energy balancing of a given distribution segment:

- In the case of micro-grids, the solution can support effective operation of the micro-grids in the event of loss of control center communications.
- In the case of control centers, the solution can be coordinated between all neighboring feeders.

Real-time energy management systems, whether at the transmission or distribution levels, will continue to have rigorous performance and reliability constraints. The smart energy reference architecture recognizes that close coupling of all the new participants to the operation of the real-time systems will prove to be fragile and unreliable over the long term. Systems must be designed to be adaptive and resilient to autonomous, independent, potentially unexpected or

non-responsive behavior of the new participants – whether at scale as in the case of end use residential customers, or in bulk such as large scale renewable energy sources.

3.0 Architecture

This section describes the Microsoft Smart Energy Reference Architecture (SERA). A reference architecture is a consistent framework that can guide implementation within a particular domain. The Microsoft SERA reflects best practices and attempts to understand and incorporate the likely impacts of technical, business and regulatory trends. The resulting implementations and deployments then form a smart energy ecosystem.

The incredible diversity of energy generation and delivery systems make it absolutely impossible and beyond human capability to coherently offer a single, detailed view of one particular architectural framework that will work in every single instance. The Microsoft SERA is instead intended to address prevailing systems and issues in enough detail to be useful, but without so much detail as to be untenable. The NIST appears to be addressing the problem of too many standards – including international standards – with no clear path. The NIST effort, despite being driven in the United States, is a global effort that will accelerate the development and deployment (in conjunction with this reference architecture document) of smart grid solutions worldwide.

The SERA should be viewed as serving as a bridge from NIST standards to specific Microsoft products and technologies. It seeks to provide – in one place –a level of understanding about those products and technologies that exist in dozens of sources. It's our hope that if an organization is interested in some specific smart grid component, say, implementing demand response solutions, they will find enough information here to know that Microsoft and its partners have the technology components that would fit a larger framework of capability. The components of SERA include:

- Approach
- User Experience
- Collaboration
- Information
- Integration
- Application Architecture
- Security

3.1 Approach

The Microsoft SERA is based on five foundational "pillars" – Performance Oriented Infrastructure, Holistic Life-User Experience, Energy Network Optimization, Partner Enabling Rich Application Platform and Interoperability – as shown in the diagram below:

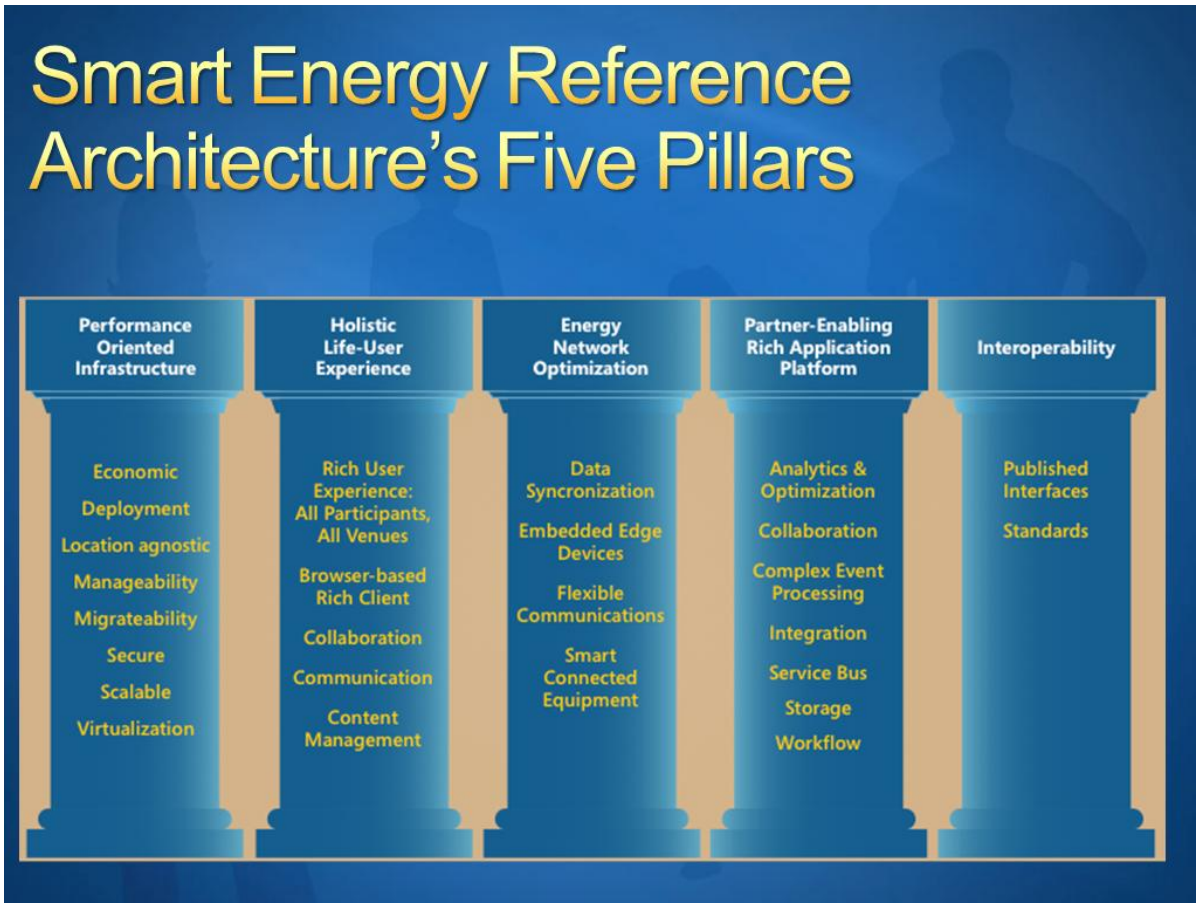

Figure 6 - Foundational pillars of the Microsoft Smart Energy Reference Architecture

3.1.1 Performance Oriented Infrastructure

A performance oriented infrastructure includes those features that make an architecture complete and appropriate to business needs. These include:

- **Economic**: The infrastructure must provide cost effective means to deploy and integrate functionality.
- **Deployment**: Components have to consider flexibility in how and where they can be deployed.
- **Location agnostic**: Services are designed so that they can be deployed on-premise or in the cloud.
- **Always connected**: Users and software components have access to platforms and services wherever they are located.
- **Manageability**: Infrastructure components can be efficiently deployed, managed and monitored.
- **Transferability**: Functionality and information can be migrated easily from one version of underlying infrastructure components to another with minimal interruption or intervention.

- **Secure**: Deployed components, functionality and associated information are protected from unauthorized access or malicious attacks.
- **High performing and scalable**: Support for more users, larger models, increased transaction volumes, etc. can be accommodated through increasing hardware performance (scale-up) or the linear addition of hardware and network resources (scale-out).
- **Virtualization**: Components can be deployed in a manner that optimizes the use of hardware resources.
- **Highly available and self-healing**: Support for transition to new equipment in the event of equipment failure.
- **Disaster recovery and backup**: Capability to move to a new platform or facility or recovery from a natural disaster or terrorist event and the back-up of results to facilitate the transition.

3.1.2 Holistic Life-user Experience

A holistic life-user experience enables all participants to view the smart energy ecosystem from the perspective of other participants.

To Microsoft, this equates to ensuring that the host company understands how customers experience the world and how technology fits into that experience. A technology architecture that facilitates the smart energy ecosystem will then necessarily consist of:

- **A rich, integrated technology user experience** for home, car, control center and field workers.
- **Browser-based collaboration** using rich clients rendered appropriately across a multitude of devices.
- **Supporting functionality for collaboration** and mashups through the use of Microsoft® Office SharePoint® Server and services.
- **A unified communications infrastructure**, where the nature of the underlying communication infrastructures are transparent to users.

3.1.3 Energy Network Optimization

The Microsoft SERA permits an energy network to connect smart devices. An optimized energy network incorporates:

- **Flexible communications**: Deployments can leverage a variety of communications paths and technologies and are easily reconfigured minimizing the time required to make new information available to users.
- **Smart connected devices**: Intelligence is added to devices and they are connected to the communications network enabling both intelligent autonomous operation and visibility of the operation of the network.

- **Desktop, server, embedded and mobile operating systems**: Operating systems (OS) can be effectively employed leveraging the right OS, at the right level, for the right role, with the right performance.
- **Application architecture**: This is the architecture for applications infrastructure and services for commonly used capabilities so developers can focus on domain-specific functionality optimizing speed to market and the reliability of solutions.

3.1.4 Partner-enabling Rich Applications Platform

The Microsoft SERA acknowledges from the outset that no one vendor will be able to provide all of the application functionality needed to implement the smart energy ecosystem. This reference architecture seeks to offer a rich platform that makes it easy for partners to develop and deploy their applications. Notable aspects of the applications platform include services for:

- **Analytics**: Rich statistical and analysis packages for data mining, discovery and reporting for diverse information consumers.
- **Collaboration:** Tools, services and applications enabling interaction between users and equipment.
- **Complex event processing**: Stream processing engines that can detect and filter events.
- **Integration**: Messaging and database technology for linking together workflow, processes and data optimization.
- **Service bus**: Services and components for the communication of device and equipment data.
- **Storage**: Repositories for capturing and enabling analysis of utility operational and business data.
- **Workflow**: Services for managing the automation of applications as well as business processes.

By providing these services to developers, Microsoft partners will only need to worry about using their expertise for the solution of domain-specific problems, leaving the platform to provide the common capabilities needed across many vertical domains. As a result, multiple vendors can provide competitive platform-consistent products and services, giving customers better offerings and more choices that are easy to leverage.

3.1.5 Interoperability

The Microsoft SERA must enable interoperability in order for the ecosystem to develop in a cost effective manner. Otherwise, the vision for the ecosystem will go unfulfilled.

New solutions must work with previous utility technology systems in order to protect those investments. Pragmatic integration approaches will need to be considered and the SERA should be flexible to allow deploying new components without custom integration.

Interoperability considerations include:

- **Standards** that define a consistent industry-wide interface to allow new component deployment.
- **Published interfaces** that are transparently publicized for open industry use even if a standard is not available and also satisfy important interoperability needs.
- **Information models**: Consistent ontology for referring to equipment and assets to enable exchange of information throughout the enterprise and the value chain.
- **User interfaces**: Consistent content and behavior in presentation of information and interaction with the user.
- **Components**: Well defined sets of functionality packaged for developer and integrator reuse.
- **Message formats**: Key construct of service-oriented architecture (SOA)[4] defining format and content that enables services exchange messages using the defined format (e.g. publish–subscribe pattern).
- **Interface definitions**: All the elements of an interface so that applications can be independently developed to leverage the interface.
- **Communication protocols**: Format, content and exchange mechanism so applications can be written to transfer information using the protocol definition.
- **Security**: Definition of the security implementation including authentication, authorization, identity lifecycle management, certificates, claims and threat models to enable secure interoperable design and deployment.

3.2 User Experience (UX)

In addition to the reference architecture having a codified approach, the overall framework must identify several goals and characteristics. This and the next several sections discuss those characteristics.

This description includes how interfaces must provide users with access to information and services appropriate for his or her organization and roles. Such a user experience will depend upon the availability of secure, location independent access to functionality. The user interface should also allow for a composable front end that provides consistency in how data is displayed but does not lock an enterprise into using yet another standalone portal that does not integrate with one the enterprise already owns. Beyond these basic requirements, there is a need for richness, efficiency, quality and consistency of the user experience that depends upon information technology systems that enable visualization, analysis, business intelligence and reporting.[5]

[4] "In computing, **service-oriented architecture** (**SOA**) provides a set of principles of governing concepts used during phases of systems development and integration. Such an architecture will package functionality as *interoperable services*: software modules provided as a service can be integrated or used by several organizations, even if their respective client systems are substantially different." Wikipedia.org

[5] Collaboration is another component of User Experience but warrants discussion in its own section.

3.2.1 Visualization

The ability to integrate information from many sources into a visual representation in a location agnostic manner is a primary tenet of the reference architecture.

Figure 7 demonstrates how visualizations can be created from a variety of information sources. It should be noted that whereas many sources are read-only, some may be transactional through underlying services.

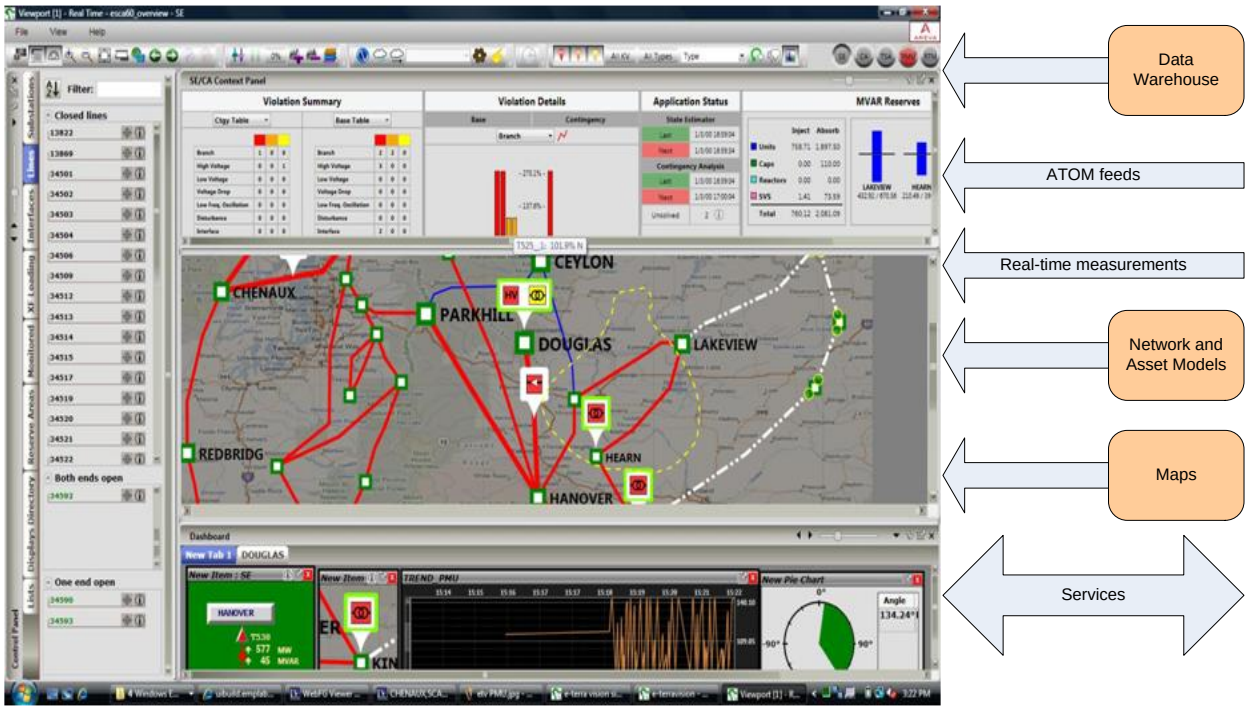

Figure 7 - Information for Visualization (Source: AREVA)

One simple example of the power of visualization that's now in common use at many utilities and grid operations is the real-time, integrated weather information overlaying the electricity grid, as shown in Figure 8.

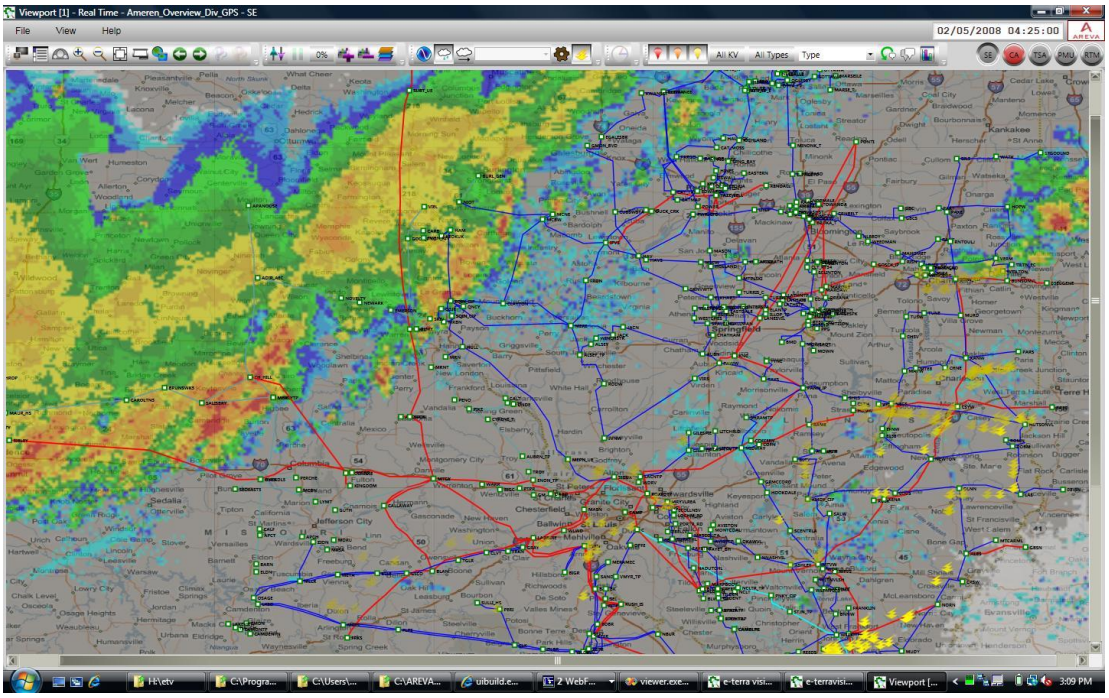

Figure 8 - Spatial Integration of Weather and Networks (Source: AREVA)

This visualization integration has produced numerous useful applications, including:

- **Distribution operations staff** can prepare emergency and repair crews at times when bad weather (e.g. high winds, ice and lightning) may cause outages.
- **Network operations** can use anticipated changes in temperature, wind and luminosity to revise load forecasts and adjust generation and interchange schedules.
- **Detections of changes in wind patterns** that may affect output from wind farms require replacement energy to be purchased or produced by alternate generation sources.

Figure 8 clearly demonstrates the wide-area situational awareness capabilities that are available to manage the grid. Another type of visualization might show real-time phasor measurements across a grid. Visualization tools can offer the user the ability to select which data types, often referred to as a thematic layer, that they want to view.

The important technology factors to consider for a visualization tool include:

- the ability to link to a variety of data sources, and then correlate objects to a geo-coded spatial position,
- rich graphics rendering,
- user configurable composite applications,
- the ability to overlay geospatially a wide variety of information,
- computing performance,
- the ability to connect to a diverse set of data feeds securely, and

- the ability to “drill through” the display and view the underlying data that drove what was presented to the user. This requires mapping and information integration of the underlying data for the graphics rendered on the display.

3.2.2 Analysis

Electric utilities perform a variety of electrical network analytical computations in the course of their everyday work managing the grid. Some of these computations are very highly specialized and complex and often involve taking a model and applying current, historical or possible future states using a diverse set of data sources. Examples include:

- **Power flow**, where power, current and voltages are calculated for a point or node in the network.
- **Contingency analysis** to determine if the network will remain stable if one or more pieces of equipment fail.
- **Outage analysis** to determine the point of failure given a set of trouble calls and other inputs.
- **Reliability analysis** to determine the failure rates of certain types of equipment.
- **Market analysis** of customer responsiveness to demand response programs.
- **Dynamic feeder loading analysis** for customer energy usage at the distribution feeder level.
- **Feeder analysis**, where the voltage and loading characteristics of a given feeder can be studied.

Some of the factors that should be considered for analysis tools include the ability to:

- drive the analysis using different input sources,
- produce high-speed, low-latency, easily configurable and rich expressions,
- look at the underlying network models at different points in time, and
- integrate the output of the analysis with a variety of visualizations.

Historically, these analysis functions have been implemented as applications in energy management systems and distribution management systems. New smart devices and more powerful computing platforms enable new architectures for deployment.

For example, metering systems have access to customer outage information and can identify outages much closer to the field equipment. Contingency analysis requires significant compute power solving many individual power flows with potential failed equipment removed, so massively parallel high-performance computing provides the potential for detecting contingencies much more quickly than conventional deployments. Packaging the analysis functions as location agnostic services allows for execution at the most appropriate location.

3.2.3 Business Intelligence

Utilities use business intelligence to help executives and managers acquire a better understanding of the commercial context of activities, thereby improving the value of their decisions and enhancing their decision-making capabilities.

Business intelligence tools often leverage information captured within a data warehouse to create information and then present that intelligent data to the right people through a variety of visual mechanisms that make the most sense to the task at hand.

Figure 9 provides an example of how a distribution company can use geospatially-oriented (e.g., ESRI GIS & Live Maps) business intelligence about tree-caused outages to focus vegetation management exclusively on certain high outage areas.

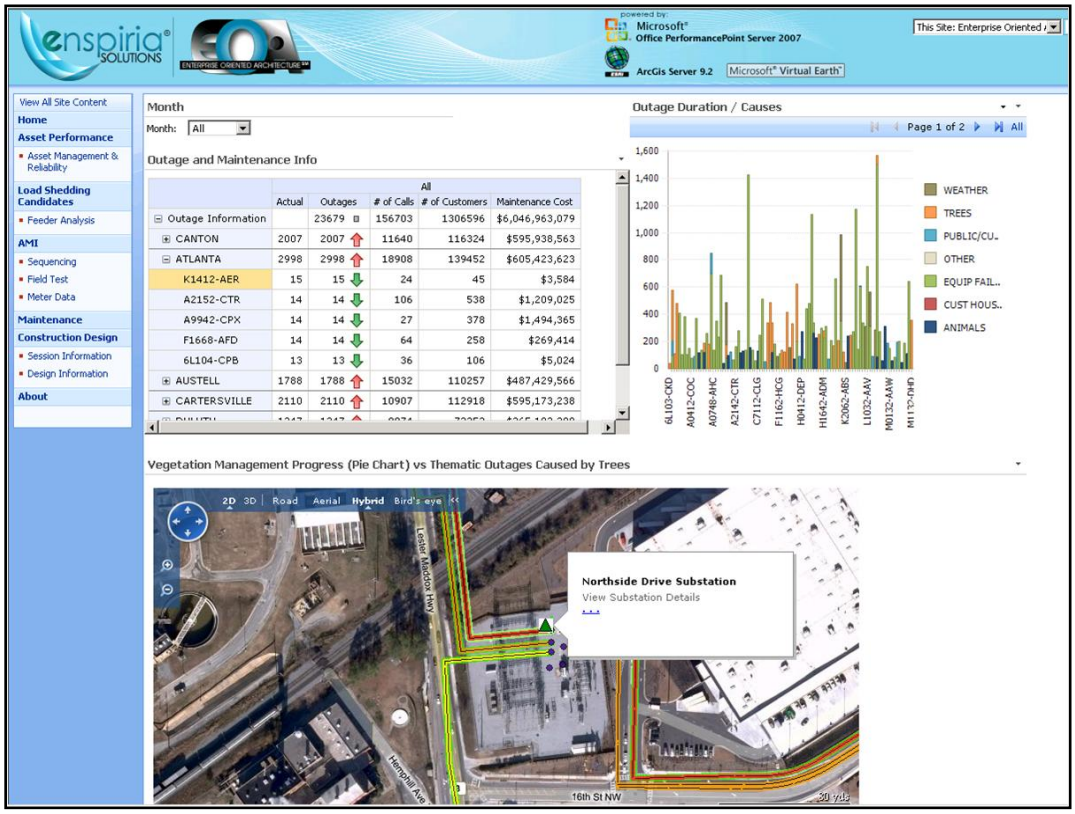

Figure 9 - Business Intelligence Example (Source: Enspiria Solutions)

Some of the technology factors that need to be considered include:

- Ease of development (including composability such as third party Web parts)
- Breadth of visualization capabilities
- Integration capabilities
- Ease of deployment
- Ease of maintenance & support
- Secure access

3.2.4 Reporting

In addition to business intelligence tools, a utility, market operator or service provider may define, create, maintain, publish and/or use a variety of reports, including:

- Meter usage
- Outage history
- Market transaction history
- Load forecast
- Load history
- Generation schedules
- Outage schedules
- Equipment failures
- Demand response event history
- Market nodal prices

While some of the reports may be generated periodically for widespread distribution or long term retention, others may be generated on an on-demand basis, where a user may request a report with specific filters for a given period of time. There may also be constraints on access, where some reports may be public, but others may only provide specific information for specific sets of users.

Where business intelligence focuses on making better decisions, reporting is more general in nature, providing information for a broader set of users for a broader set of purposes.

3.3 Collaboration

Collaboration will be another characteristic of the smart energy ecosystem of the future.

By collaboration, we mean the need for people, organizations, applications and/or devices to actively participate and interact upon sets of inter-related business processes. Some examples of collaboration in the utility context include:

- **Energy markets**, where organizations will register resources and participate in the trading and settlement of energy in different markets.
- **Aggregation**, where a service provider will identify, register and manage a set of resources (e.g. distributed generation, controllable loads, etc.) and their participation in market programs.
- **Demand response**, where, as an extension of the energy market processes, devices may respond automatically to market pricing signals to take local actions related to energy usage.
- **Load balancing**, where load and available energy supply must be balanced. For example, the charging of plug-in vehicles may require coordination between devices (including vehicles) on the feeder, between devices within substations and with energy market dispatch schedules.

This section describes various information and data exchange styles including:

- Collaboration
- Orchestration
- Notification Infrastructure
- Chain of Command – Notification plus Workflow

3.3.1 Collaboration

In order to create a collaborative environment, utilities will use Web and associated technologies and products as the primary infrastructure.

Collaboration can take several forms including:

- **Human-to-human collaboration** with delivery mechanisms such as Web portals and messages.
- **System-to-human and vice-versa** with delivery mechanisms such as messages, emails, instant messages, feeds, alert indicators, etc.
- **System-to-system collaboration** with automated data exchange automated via orchestrations or publish-subscribe message collaboration.

The underlying services can be deployed through cloud-based computing as provided by Windows® Azure™ or within an enterprise with secure external access through a portal. Protocols that simultaneously address both security and privacy will be required to enable Web-based collaboration, as well as associated orchestration and notification.

3.3.2 Orchestration

The term *orchestration* is usually applied to more complex, long running processes that coordinate the execution of multiple Web services into automated business processes and may have many steps and require user interaction (whereas the term *workflow* is commonly applied to a set of coordinated short running tasks).

The users involved in business processes, which have been automated using orchestration (either as specific users or those with the role in an organization) and/or systems, participate in business processes either within an organization or across organizational boundaries.

3.3.3 Notification Infrastructure

Collaboration requires the ability to notify a user or group of users whenever there is a condition of potential interest so that, if necessary, they can take appropriate actions.

One example would be when an industrial participant in a demand response program would be made aware that a load curtailment is scheduled for later in the day. The industrial participant can then revise factory production schedules.

Notifications also can include a wide range of other conditions, including:

- perimeter security notices,
- equipment state changes, and
- alarm limit violations.

Since users are fundamentally mobile – they may be at work, at home or otherwise away from their personal computer – notifications can be issued using a variety of means including:

- e-mail,
- Web feeds (such as RSS or ATOM),
- dashboard icons,
- SMS messages (to mobile devices), and
- voice, where voicemail can be issued.

For some notifications, the need for a positive acknowledgement is important. The basic need is to be sure that the user received and acknowledged the message within a reasonable time, and, if not, it may be necessary to escalate that message to another user. Examples of this could be for planned outages or emergency load reductions, where the user needs to be aware that power may be out for a period of time so they have appropriate advance warning. In other cases, such as voluntary load reductions, the acknowledgement may need to be more involved, where the user can indicate if they will participate or not.

Business process automation also requires the ability to filter notification types that a user or group will receive and how they receive them. Role-based notifications limit the distribution to subscribers relevant to the event, and the notion of presence can ensure notifications go to users that are available at the time of notification. Subscription patterns and rules engines can be used to decouple notification subscriptions from actual business process flow. For example, some users may be interested in informative events such as pricing signals, where others are only interested in emergency events.

3.3.4 Chain of Command – Notification plus Workflow

Combining notification with managed workflow can be an effective way to organize human process within the smart energy ecosystem.

As the number of participants in the ecosystem increases and the nature of activities becomes more diverse, assigning tasks and tracking the completion of activities will be challenging. Combining notification with managed workflow can also be a way to improve the timeliness of resolution of issues, be they field or enterprise related. Cross-organizational boundaries can be efficiently handled through managed workflows, and notification automates collaboration for resolution of the issues. Tracking and reporting on the managed workflow can also provide evidence of timely response and notification for regulators.

3.4 Information

Information within the smart energy ecosystem can take many forms.

These forms include logical models and physical models that would be used to describe database schemas, message structures and interface definitions. Due to the complex nature of the electricity infrastructure and the associated business processes, many different systems, applications and sources of information are used.

Figure 10 demonstrates how information can be organized physically, logically and conceptually, as well as by functional area:

	Business	***Information***	***Application***	***Technology***
Conceptual	▪Use Cases And Scenarios ▪Business Goals And Objectives	▪Business Entities And Relationships	▪Business Processes ▪Service Factoring	▪Service Distribution ▪Quality Of Service Strategy
Logical	▪Workflow Models ▪Role Definitions	▪Message Schemas And Document Specifications	▪Service Interactions ▪Service Definitions ▪Object Models	▪Logical Server Types ▪Service Mappings
Physical	▪Process Specification	▪Database Schemas ▪Data Access Strategy	▪Detailed Design ▪Technology Dependent Design	▪Physical Servers ▪Software Installed ▪Network Layout

Figure 10 - Types of Information Organization

This information section discusses:

- Standards and Domain Models
- IEC Utilities Common Information Model
- Metadata Management
- Master Data Management
- Historians
- Operations Databases
- Data Warehouses
- Interoperability
- Messages and Interfaces
- Event Cloud

3.4.1 Standards and Domain Models

The smart energy ecosystem will require a wide variety of information to be managed, accessed and analyzed. Some of this information is specific to the domain of the electricity industry, while some is common to a wide variety of other industries.

No matter the case, the specific information models can be viewed as an ontology. In computer science and information science, an **ontology** is a formal representation of a set of concepts within a domain and the relationships between those concepts. It is used to reason about the properties of that domain, and may be used to define the domain.[6]

Many of these information models are either directly or indirectly defined by industry standards, such as the IEC Common Information Model (CIM), while others can be a consequence of more broad-based standards or even proprietary information models that are defined by systems vendors.

The collective set of information models used by the electricity industry can be viewed as a federation of ontologies.

Figure 11 illustrates a view of the logical relationships between domain models either defined or implied by the various standards and specifications that are being proposed by NIST for use within the Smart Grid Interoperability Standards Framework.

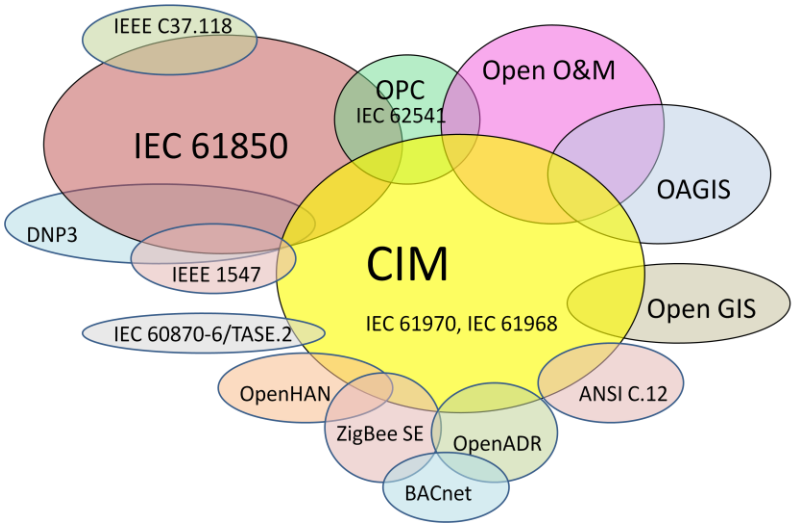

Figure 11 - Logical Relationships between Smart Grid Standards

[6] See definition of "Ontology" in Wikipedia.com

For purposes of simplicity, Figure 11 does not show the relationships to more general IT standards or security standards. IT standards and security standards can be viewed for the most part as implementation layers.

NIST is proposing the following NIST-Recognized Standards Release 1.0 to become a set of recognized industry standards and specifications to provide an interoperability framework.

NIST- Recognized Standards Release 1.0	
Standard/Specification	**Application**
AMI-SEC System Security Requirements	Advanced metering infrastructure (AMI) and Smart Grid end-to-end security
ANSI C12.19/MC1219[7]	Revenue metering information model
BACnet ANSI ASHRAE 135-2008/ISO 16484-5	Building automation
DNP3	Substation and feeder device automation
IEC 60870-6 / TASE.2	Inter-control center communications
IEC 61850	Substation automation and protection
IEC 61968/61970	Application level energy management system interfaces
IEC 62351 Parts 1-8	Information security for power system control operations
IEEE C37.118	Phasor measurement unit (PMU) communications
IEEE 1547	Physical and electrical interconnections between utility and distributed generation (DG)
IEEE 1686-2007	Security for intelligent electronic devices (IEDs)

[7] ANSI is the American National Standards Institute, a private non-profit organization that oversees the development of voluntary consensus standards for products, services, processes, systems and personnel in the United States. The organization also coordinates U.S. standards with international standards so that American products can be used worldwide. For example, standards make sure that people who own cameras can find the film they need for that camera anywhere around the globe. Wikipedia.org

NERC CIP 002-009	Cyber security standards for the bulk electric power system (wholesale/transmission)
NIST Special Publication (SP) 800-53, NIST SP 800-82	Cyber security standards and guidelines for federal information systems, including parts of the bulk electric power system
Open Automated Demand Response (Open ADR)	Price responsive and direct load control
OpenHAN	Home Area Network device communication, measurement, and control
ZigBee/HomePlug Smart Energy Profile	Home Area Network (HAN) Device Communications and Information Model
Standards Added September 2009 to NIST – Recognized Standards 1.0	
AEIC Guidelines v2.0	
C12 Suite: ANSI C12.1 C12.18/IEEE P1701/MC1218 C12.20 ANSI C12.21/IEEE P1702/MC1221 C12.22-2008/IEEEP1703/MC1222 C12.24	
ANSI/CEA 709 and CEA 852.1 LON Protocol Suite ANSI/CEA 709.1-B-2002 Control Netwoark Protocol Specification ANSI/CEA 709.2-A R-2006 Control Network Power Line (PL) Channel Specification ANSI/CEA 709-3 R-2004 Free-Topology Twisted-Pair Channel Specification ANSI/CEA 709.4:1999 Fibre-Optic Channel Specification CEA 852.1:2009 Enhanced Tunneling Device Area Network Protocols Over Internet Protocol Channels	
CableLabs PacketCable Security Monitoring and Automation (SMA)	
FIXML Financial Information eXchange Markup Language	
IEEE 1588	
Internet Protocol Suite including, but not limited to: IETF RFC 791 (IPv4) IETF RFC 768 (UDP) IETF RFC 2460 (Ipv6)	

Standards Added September 2009 to NIST – Recognized Standards 1.0 ***(Continued from previous page)***
ISO/IEC 15045, "A Residential gateway model for Home Electronic System."
ISO/IEC 15067-3 "Model of an energy management system for the Home Electronic System."
ISO/IEC 18012, "Guidelines for Product Interoperabillity."
ITU Recommendation G.9960 (G.hn)
MultiSpeak
OPC-UA Industrial
Open Geospatial Consortium Geography Markup Language (GML)
US Department of Transportation's Federal Highway Administration's Intelligent Transportation System (ITS) Standard NTCIP1213, "Electrical Lighting & Management Systems

Figure 12 - NIST – Recognized Standards Release 1.0 and September 2009 Update

It is important to note that some of these are actually specifications, as opposed to standards:

- Some, such as AMI-SEC and OpenHAN, are more at the stage of requirements specifications as opposed to actual standards that can be used for interfacing systems and products.
- Some of the standards identified, such as IEC 61850, IEC 61968 and IEC 61970, are series with multiple parts, where some parts may or may not be appropriate, or may only be in a proposed or draft form.
- There are some large gaps that need to be filled, such as the definition of a standard interface to a ZigBee Smart Energy profile Energy Service Portal.
- At a minimum, the applications and information exchanges within the smart energy ecosystem will leverage the domain models provided by the CIM (as defined by IEC 61970 and 61968), as well as the related IEC 61850 models that are realized in the form of the 61850 System Configuration Language (SCL).

Many of the efforts identified on the NIST roadmap will benefit from the formation of the new OASIS Energy Market Information Exchange (eMIX) Technical Committee.[8] This technical committee will define how to exchange energy characteristics, availability and schedules to support free and effective exchange of information in any energy market. This group will cooperate with other standards groups including the IEC.

3.4.2 International Electrotechnical Commission (IEC) Common Information Model

At the core of many IEC standards is the IEC Common Information Model (CIM).

Within transmission and distribution, the CIM has been officially adopted to allow application software to exchange information about the configuration and status of an electrical network.

The CIM is currently maintained as a Unified Modeling Language (UML) model.[9] It defines a common vocabulary and basic ontology, covering important subjects unique to the electric power industry.

The central package within the CIM is the 'wires model,' which describes the basic components used to transport electricity.

The CIM can be used to derive design artifacts as needed for the integration of related application software.

Figure 13 illustrates this dynamic:

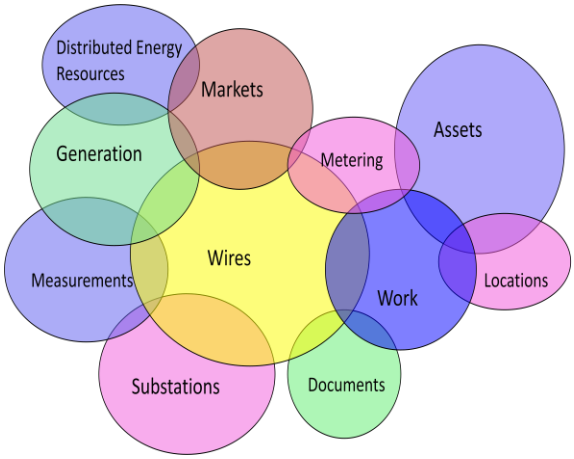

Figure 13 - CIM as Ontology

[8] OASIS (Organization for the Advancement of Structured Information Standards) is a not-for-profit consortium that drives the development, convergence and adoption of open standards for the global information society. The consortium produces more Web services standards than any other organization along with standards for security, e-business, and standardization efforts in the public sector and for application-specific markets. Founded in 1993, OASIS has more than 5,000 participants representing over 600 organizations and individual members in 100 countries.

[9] The Unified Modeling Language™ (UML®) is an Object Management Group (OMG) modeling standard that enables visual design of application structure, behavior, architecture, as well as business processes and data structures. UML and the OMG META Object Facility (MOF) are key elements of the OMG Model Driven Architecture.

- The **IEC 61970-301** standard defines the core packages of the CIM, with focus on the needs of electricity transmission, where related applications include energy management systems (EMS), supervisory control and data acquisition (SCADA), planning and optimization.
- The **IEC 61970-501** and **61970-452** standards define an XML format for network model exchanges using RDF, sometime referred to as CIM XML.
- The **IEC 61968** series of standards extend the CIM to meet the needs of electrical distribution, where related applications include distribution management system, outage management systems, planning, metering, work management, geographic information systems, asset management and customer information systems.

Figure 14 provides an overview of the equipment inheritance hierarchy found within the IEC CIM. This diagram represents only one aspect of a portion of the CIM, but offers some insight with respect to the set of objects that provide the core framework of the CIM.

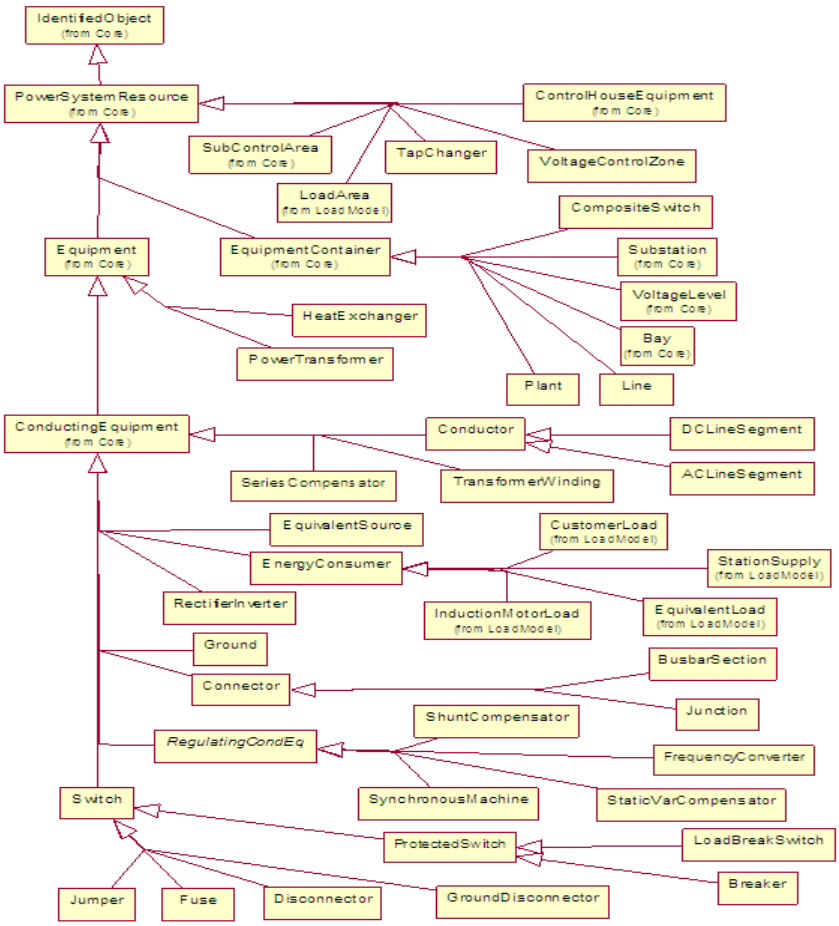

Figure 14 - CIM Inheritance Hierarchy for Wires Model

As previously identified, the CIM attempts to govern a number of subject areas related to the physical infrastructure of the electricity grid. Examples include measurements and assets, where the measurements that are obtained from telemetry identify the current state of the infrastructure and assets and how and where the infrastructure is constructed.

3.4.3 Metadata Management

Within an enterprise, there may be a wide variety of metadata (data about data) that needs to be managed.

This metadata describes the information that is managed within databases and in the definition of information exchanges. The metadata can represent both logical data models (e.g. using UML) and physical design artifacts (e.g. XML Schemas, DDL, RDF Schemas, etc.).

For integration purposes, it is important to be able to define and manage the mappings between models and artifacts. For example, when integrating systems, the source and target systems may use different but overlapping models, where it is necessary to 'map' (transform/translate) the information from one system into a form needed by the target.

Metadata is typically derived from a variety of sources including:

- CIM logical model as defined in UML, which provides logical coverage for a variety of standards including IEC 61970, 81968 and 61850.
- Other standard logical models, including those defined by MIMOSA and the Open Geospatial Consortium (OGC).
- Proprietary logical models, as might be either provided by vendors or reflected by their products.
- Design artifacts as provided by a variety of standards and specifications, including IEC 61968, MultiSpeak, IEC 61970, IEC 61850 and OpenADR.
- Design artifacts as provided by vendors that are reflective of their product interfaces.
- Design artifacts that are a consequence of locally developed applications.

A repository can be used to manage metadata. The metadata can take a variety of forms, including UML, XMI, XSDs, RDFS, OWL, etc. The primary use of the metadata is to support integration efforts.

Within the IEC standard efforts, interfaces and information exchanges are defined using a three-layer model:

1. **Information models** are the highest level. Within an enterprise and associated integration, the information models that form an overall enterprise information model may be derived from the IEC CIM, extensions to the CIM and other models as may be sourced from other standards and vendor products.
2. **Contextual profiles** define the next level. A contextual profile is a formal subset derived from the information models that defines the content of an information exchange.

3. **Design artifacts** comprise the lowest level. Design artifacts consist of
   a. XML Schemas
   b. RDF Schemas
   c. Database schemas, which are used to define physical models in the form of interfaces, messages and databases.

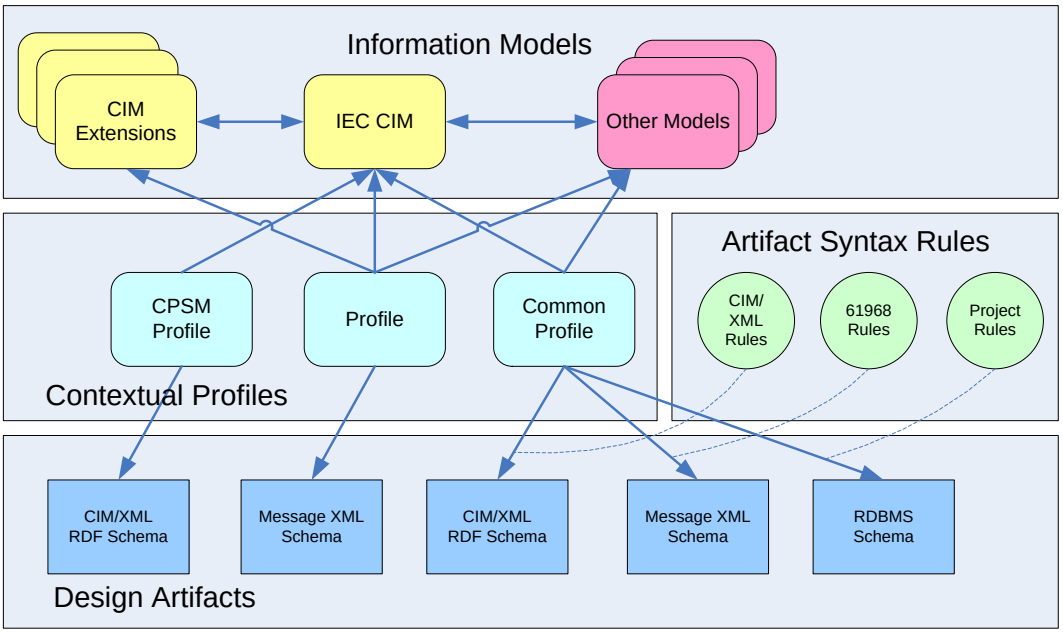

Figure 15 - Information Models and Contextual Profiles

The contextual profile concept is a crucial consideration because each profile defines a logical model for an information exchange. These profiles form the basis of many IEC standards, such as those used for network model exchanges and IEC 61968 messages.

Given the diversity of needs, standard models such as the IEC CIM are commonly extended. The extensions are driven by utility-specific model needs, with features provided by vendor products and/or draft extensions to standards that may be works in progress but not yet formally incorporated into the standard model.

Figure 16 shows two notable environments, one for modeling and the other for development. The modeling environment is primarily focused on developing models and interfaces and designing artifacts that can be used by developers to perform integration develop software components and user interfaces.

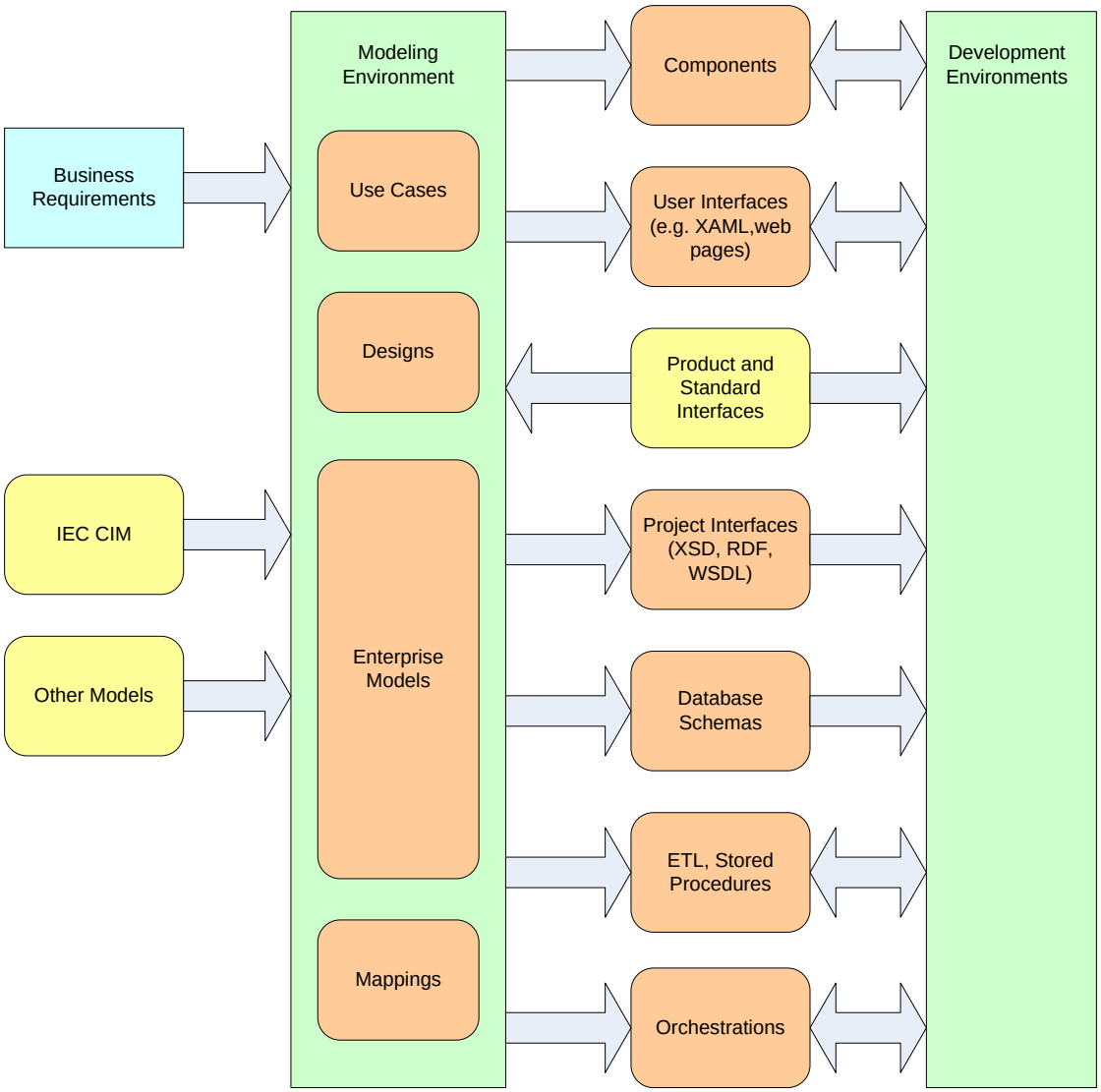

Figure 16 - Modeling, Development and Artifacts

Within the modeling environment, the IEC CIM, other models and interface standards are used to construct an enterprise data model. The enterprise model is often extended to reflect extensions needed to support local business processes and applications. The design artifacts that may be generated from a modeling environment are derived from the enterprise models. The artifacts may be generated in many forms, including:

- XML Schema for message and interface definitions
- WSDL for definition of Web services, which will typically reference XML schemas
- RDF Schema for definition of model exchange profiles
- XAML, for definition of user interfaces
- DDL for the creation of scripts to create database tables and indexes within a database management system
- C# classes, for the construction of software components

- C++ classes, for the construction of software components
- Java classes, for the construction of software components
- BPEL or XLANG process orchestrations
- XSLT for XML transformations

It is becomingly increasingly common in the utilities arena to use a wiki to manage other forms of artifacts that are important to a given organization or project. Using a wiki, these artifacts can be readily found, accessed and maintained.

3.4.4 Master Data Management

Diverse sets of business processes within an electric utility or ISO are supported by a diverse set of applications. Consequently, a number of different types of master data must be managed. Information of interest to master data management includes:

- **Network models**, which may include electrical transmission and/or distribution
- **Resources**, which are primarily generation resources
- **Customer data**, as needed to identify customer accounts and service locations
- **Geographic information**, which may be used to derive network models especially in distribution
- **Assets**
- **Settlements**
- **Work orders**
- **Measurement history**

The temporal nature of master data must be recognized as well:

- The structure of the electricity grid changes over time, typically through the process of construction, upgrades and decommissioning.
- The connectivity of the network changes over time, as the position of breakers and switches are changed.
- The state of the network also changes as load and generation changes or tap positions are altered.
- Through the process of maintenance and repair, assets may be replaced.

Each master data manager will have an internal physical model, where data may be exposed or exported using either standard or proprietary interface mechanisms, ranging from files to APIs to messages to database table access.

3.4.5 Historians

Historians provide the means to capture, store and retrieve measurement history. Such histories are important records for grid, transmission and distribution operators because each measurement is related to an object in one of the master data managers.

Operational historians are important records of operational history and have a wide variety of uses. Two types of historians are in common use, each with subtle but significant differences:

- **Measurement historians** (e.g. OSIsoft PI), which collect real time measurements obtained from real-time telemetry.
- **Meter data managers (e.g. Itron MDM)**, which collect readings from meters with a focus on electricity usage.

Historians may offer multiple ways of accessing information:

- Through the use of a Microsoft® SQL Server®-compliant interface
- Through an industry reference e.g. OPC Data Access or UA[10]
- Using an application programming interface (API) or Web service
- Through a product-specific user interface

As a consequence of the high volumes of data that are managed, the structure of information within the historian is often proprietary. In the case of a measurement history, analog values obtained from thousands of data points may be collected and stored every two seconds. In the case of a meter data manager, data may be collected from millions of meters every 15 minutes.

3.4.6 Operations Databases

Operations databases are typically part of enterprise or operations applications. These databases focus on online transaction processing (OLTP) and are typically normalized data stores with proprietary models. While the industry has trended toward the use of relational databases, or minimally databases with SQL Server-compliant interfaces, this is not always the case.

Different operational databases face synchronization issues, especially from the perspective of models, where updates are often continually applied to a network; sometimes those updates are only reflected on a daily, weekly or even monthly basis in the model.

While the industry has been moving toward adoption of the IEC CIM as a common logical data model, it is important to note that there is no IEC standard that defines a 'CIM compliant' relational database structures. Instead, it can be best said that databases may be 'consistent' with or 'inspired by' the CIM.

3.4.7 Data Warehouses

Data warehouses are typically de-normalized, dimensional data stores that provide information related to a given set of subjects used for online analytical processing (OLAP). The databases focus on decision support and are either part of a vendor product suite or custom in nature.

[10] OPC UA is a Unified Architecture for data access described by a 12 part specification. These specifications are primarily enabled via Web Services but can be supported by a variety of transports. OPC UA has been created among other reasons because Microsoft has de-emphasized COM which was the basis for the original OLE for Process Control specification.

While data warehouses typically are implemented using SQL Server-compliant relational databases, there are meaningful opportunities, if not requirements, to leverage proprietary database features, primarily for indexing.

Data warehouses are often organized using a 'star schema' structure that is characterized by tables for dimensions and facts, where a fact table identifies a set of quantities that are related to a number of dimensions.

Figure 17 offers a generic example:

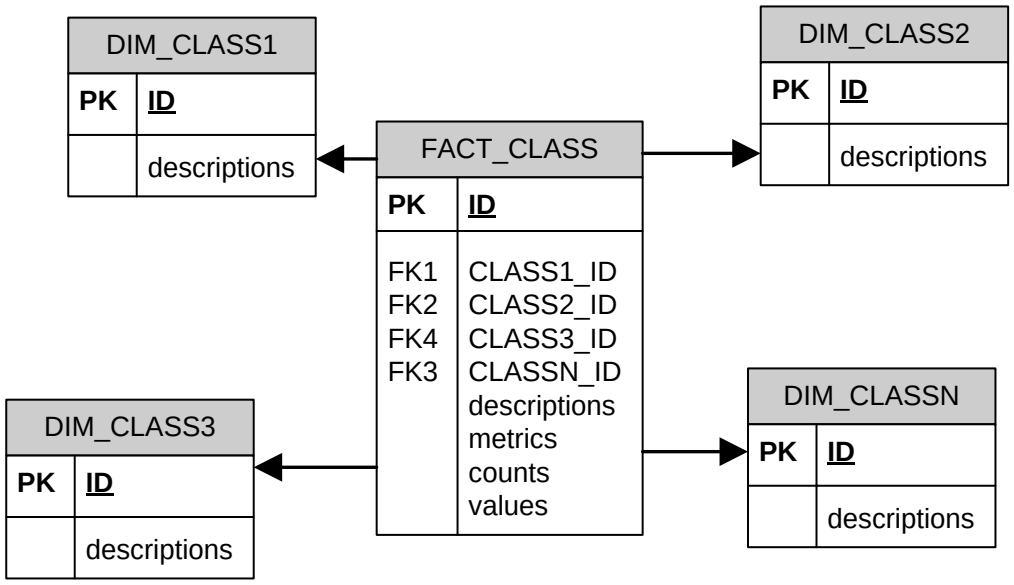

Figure 17 - Star Schemas

A data warehouse design for problems in the electric utility domain would typically leverage the IEC CIM. Where the IEC CIM is a logical data model, there is a level of design necessary to leverage it for the realization of a data warehouse. Such a data warehouse would be said to be 'CIM inspired' and would include such dimensions as:

- **Time**, where data will be typically aggregated within time intervals, where depending upon data the finest level of granularity within the data warehouse, may typically be 2-15 minutes)
- **Equipment hierarchy** (e.g. describing the hierarchical relationships between regions, substation, voltage level, bay, lines, equipment)
- **Functional type** (i.e. inheritance) hierarchy for equipment (e.g. conducting equipment, switch, breaker)
- **Geographical location hierarchy**
- **Organizational hierarchy**
- **Customers**

- **Assets**
- **Asset type hierarchy**

Figure 18 represents a portion of a data warehouse that uses the CIM model, where a fact table leverages several dimensions. Note how the dimensions are typically hierarchical, providing the means to 'slice and dice' information in many different ways.

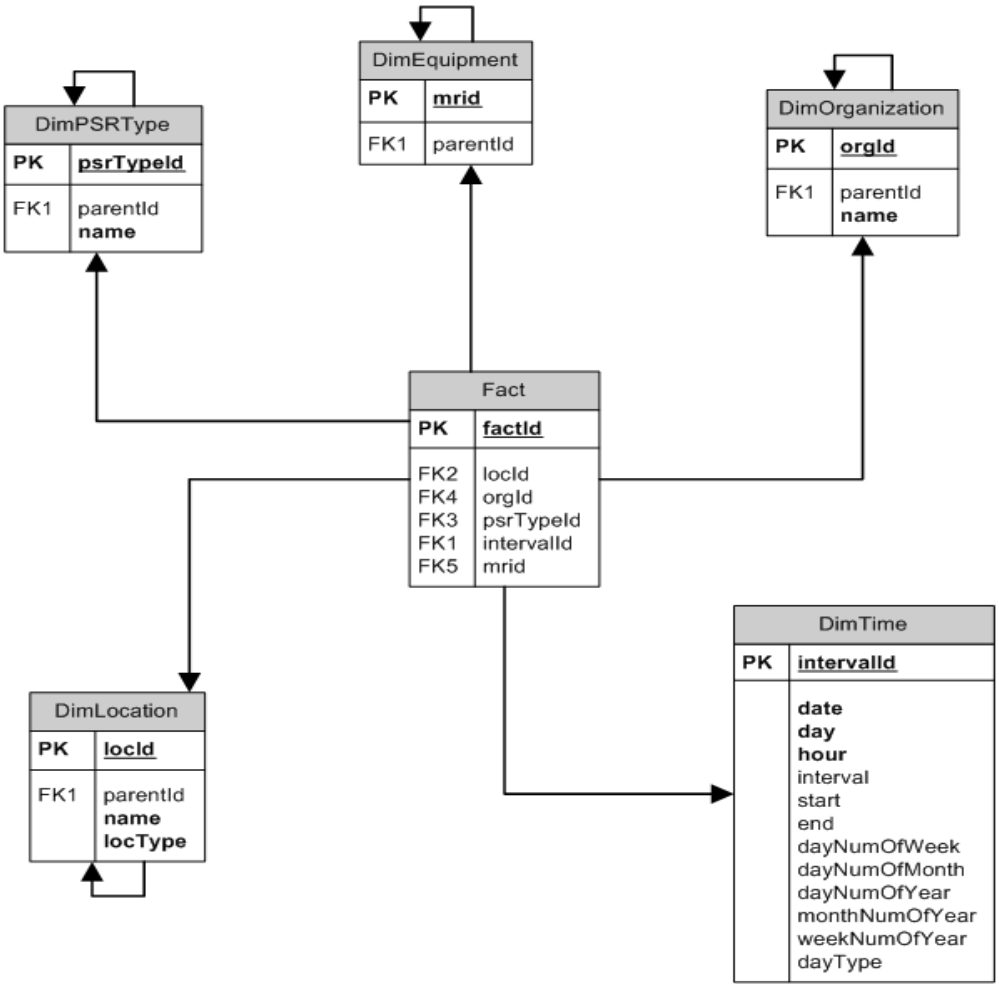

Figure 18 - Example of CIM-inspired Star Schema

Figure 19 shows how data can be integrated within the enterprise. Note the population of data into the warehouse and the use for visualization, reporting and analysis. The data warehouse is typically populated using ETL and processes that load data from staging tables, although there may be cases where the data warehouse may be updated using the ESB.

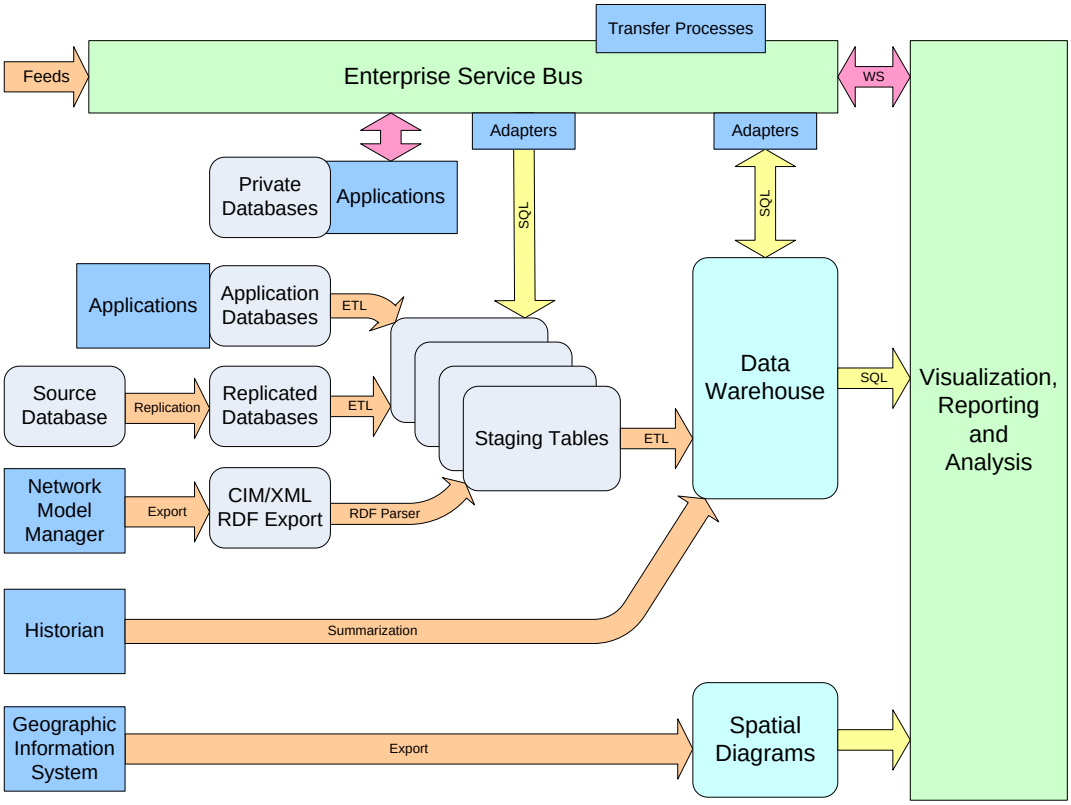

Figure 19 - Data Warehouse Integration

The staging tables in Figure 19 are used to collect data from various sources prior to aggregation and insertion into the data warehouse. The sources of data and methods of movement can include:

- **Databases** used by other enterprise applications, using ETL
- **ESB processes**, which may involve event driven or periodic processing to place data in staging tables or sometimes directly into the data warehouse
- **Databases replicated from other databases**, where ETL is then used to transform and populate data in staging as appropriate
- **RDF parsers**, where a CIM/XML model in RDF format is used to populate structures in staging tables
- **External data feeds**, where adapters in the ESB can be used to populate staging tables or the data warehouse directly
- **Applications through ESB interfaces**, where the application database is private or of a proprietary nature
- **Directly from an application** such as a historian, where it can be configured to periodically aggregate, summarize and export desired data

The staging tables are used only to prepare data for the warehouse and are not used for any transactional or visualization purposes. The data warehouse itself is not a transactional

database, and is a read-only data store from the perspectives of visualization, reporting and analysis.

Figure 19 also shows integration of the data warehouse with a geographic information system (GIS). This is important, as more visualization and reporting will allow information to be presented spatially. CIM XML exports may also provide geo-coded locations for network objects.

Also in Figure 19, the integration of the historian reflects the fact that it might be more efficient to aggregate and/or summarize information from a historian rather than to try to always retrieve and summarize data from this historian on the fly when needed for analysis. Where the historian may have measurements for a given data point for every two seconds, the data warehouse would store the average, minimum and maximum values for a measurement over a much wider time interface, such as 5-15 minutes. This would provide a convenience by simplifying many types of analysis, where it would always be possible to retrieve the detailed measurement history from the historian if needed.

The structure of some staging tables may be derived from the CIM, and extended as needed. Some staging tables may leverage other models. Whatever the case, the staging table design must allow for efficient aggregation and population of data to be inserted into the data warehouse.

3.4.8 Interoperability

Standards promote interoperability through the definition of messages and interfaces. However, standards can vary with respect to the degree of interoperability they provide. For example, standards can be:

- **Plug and play** with automatic discovery or minimal configuration
- **Interoperable** with some pre-configuration
- **Interoperable with mapping** and/or some modest level of integration effort

Figure 20 illustrates this process and demonstrates how an integration layer is often used to connect information flows between applications by performing mappings that may be needed in cases where an interface standard is less than plug and play.

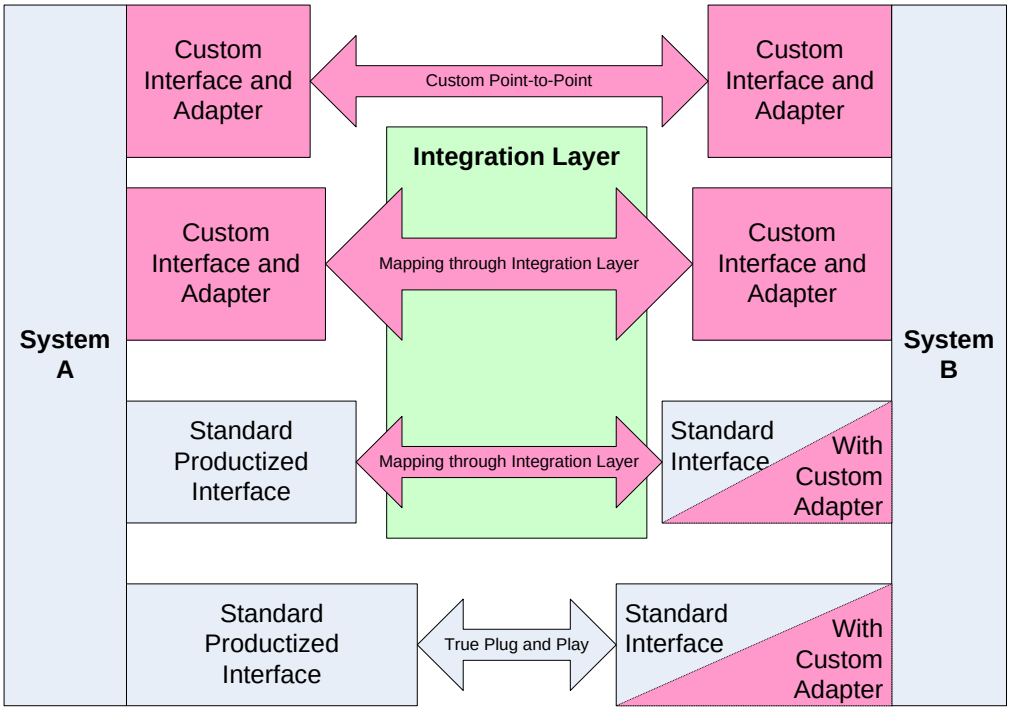

Figure 20 - Interfaces and Integration

When the number of integration points is high, such as the case with device integration, plug and play is mandatory, either through the use of standards or proprietary interfaces. However, there are also cases where some aspects of integration may not be covered by widely adopted plug and play standards. As examples, the integration of distribution, market and work management systems are commonly dependent upon some level of integration effort in order for them to exchange information with other enterprise systems. This is especially true of domain-focused applications that are implemented, sold and deployed by vendors in quantities of 1, 10 or even 100; as opposed to much more broadly deployed software applications such as Microsoft® Office or Microsoft® Exchange Server.

The use of an integration layer as provided by an ESB is the recommended approach for "impedance matching." The need to impedance match or perform custom integration is typically a consequence of the diversity of business processes, immaturity of standards and consequences upon related applications, as well as evolving needs of the business and industry.

3.4.9 Messages and Interfaces

While a variety of standards can be leveraged for integration, the primary concern is to choose an approach that:

- minimizes integration costs for the initial implementation,
- provides opportunities for reuse,
- is supportable longer term, and
- enables the flexibility needed for evolution over the long term.

For integration purposes, the following choices are ordered for preference:

1. Use a **standard interface** supported by vendor products.
2. Use a **productized, but potentially proprietary interface** supported by a vendor product and map as needed within the integration layer (i.e. ESB).
3. Select an **appropriate interface standard** that can be readily adapted to interface to products or applications of interest.
4. Define **new interfaces** leveraging appropriate integration standards.

As one example, the IEC 61968 standard focuses on the integration of electrical distribution systems. However, IEC 61968 has also been applied to the integration of applications related to transmission, generation and energy markets. These are subject areas where the IEC CIM is often leveraged. Within IEC 61968, messages are defined using a message envelope that has three primary parts:

- A verb, to identify an action such as CREATE, CHANGE, DELETE
- A noun, to identify the contents of the message payload
- A payload, which is an XML document derived from some subset of the classes, attributes and relationships typically identified by the IEC CIM, although other domain models can also be leveraged

Using the verb/noun scheme, a given application can be characterized in terms of messages it produces and consumes. Figure 21 provides an example of system characterization.

System: Whiz-Bang MDM
System Type: MDM
Vendor: Acme

	Client or Event Subscriber											Server or Event Publisher										
	Requests						Events					Requests						Events				
Message Type (noun)	get	create	update	delete	cancel	close	created	updated	deleted	canceled	closed	get	create	update	delete	cancel	close	created	updated	deleted	canceled	closed
MeterReadings							x					x										
EndDeviceEvents		x					x					x										
EndDeviceControls		x			x		x			x												
EndDeviceAssets							x					x	x	x	x			x	x	x		
CustomerMeterDataSet												x	x	x	x			x	x	x		
MeterReadSchedule		x			x		x			x												

Figure 21 - System Characterization Worksheet

One realization of an IEC 61968 message is through an envelope defined by an XML schema that has a header to contain the noun and verb. The header may contain other parameters, such as

timestamps and user IDs. Other structures are added to the message envelope structure to convey information such as request parameters and error strings.

Figure 22 illustrates the IEC 61968 Message Envelope and the associated headers and strings. The relevant information is conveyed using the payload structure within the message envelope.

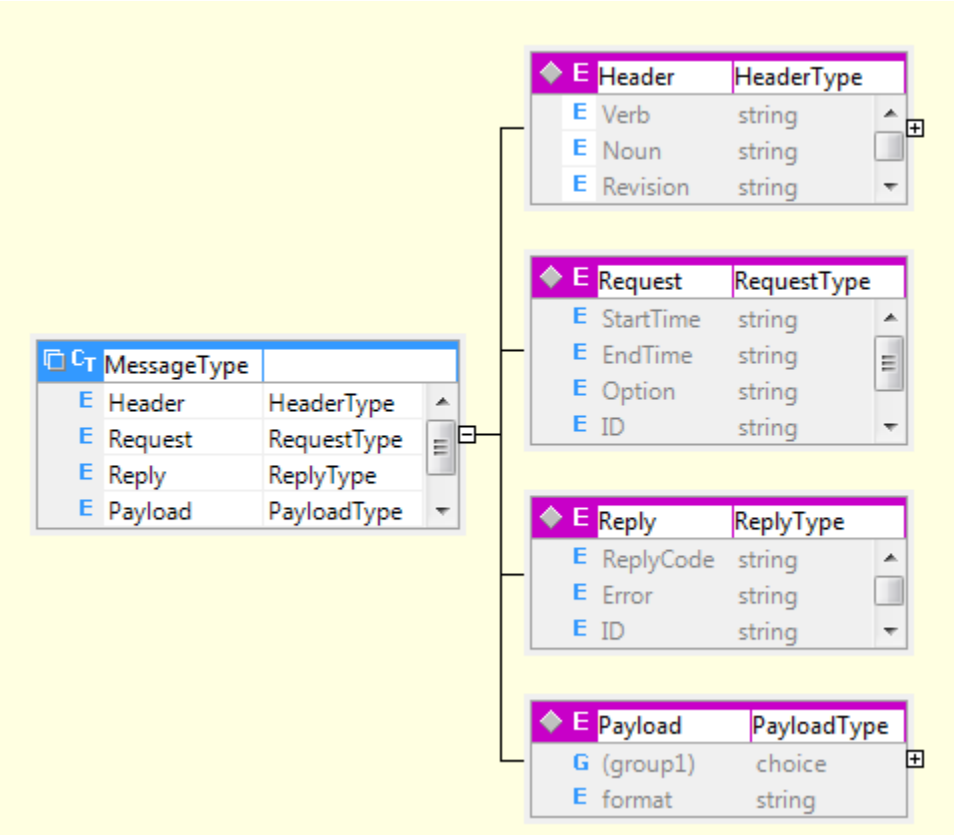

Figure 22 - IEC 61968 Message Envelope

Figures 23 and 24 describe example payload structures from IEC 61968-9 that are used to convey end device controls and events. The message structures are derived from a contextual profile of the IEC CIM.

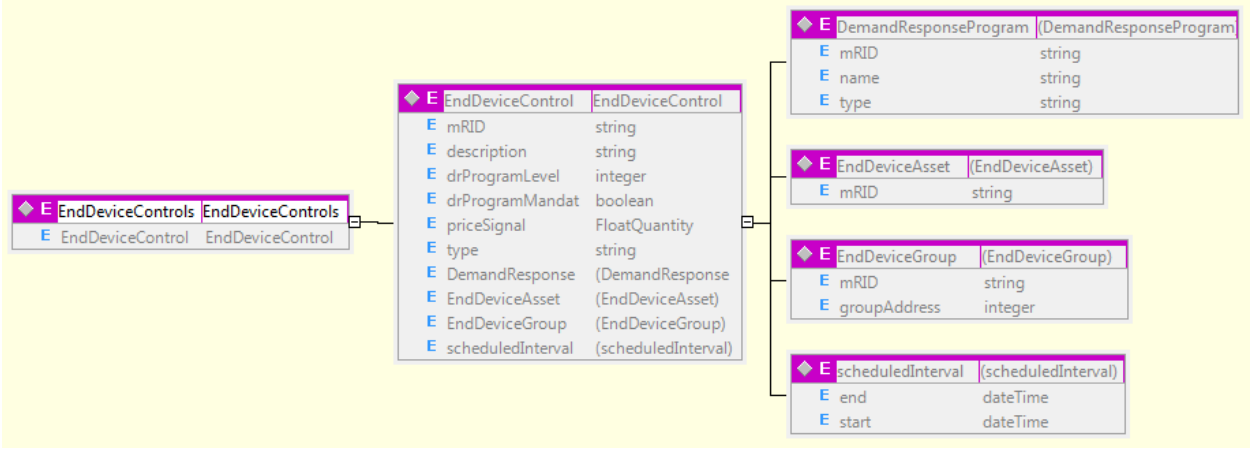

Figure 23 - End Device Controls Payload Structure

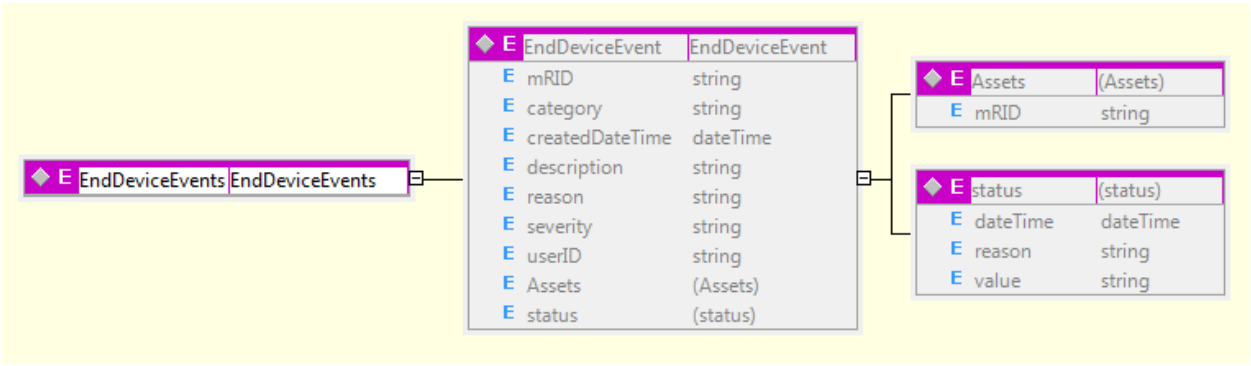

Figure 24 - End Device Events Payload Structure

It's important to note that IEC 61968 is transport independent so that it can be implemented using technologies such as Web services, Microsoft BizTalk® Server messages and even technologies yet unknown. For use within Web services, message definitions are simply referenced within Web Service Description Languages (WSDLs)[11]. The use of XML also permits these messages to be managed by a collaboration infrastructure, where references to the messages can be conveyed using links in ATOM feeds.[12]

MultiSpeak is an industry specification developed by the National Rural Electric Cooperative Association (NRECA) that deals with the exchange of information between distributed-related applications. Within MultiSpeak, interfaces are defined as Web services. Where there are differences between the models used by MultiSpeak and the IEC CIM, they are not significant

[11] "The Web Services Description Language (WSDL, pronounced 'wiz-dəl' or spelled out, 'W-S-D-L') is an XML-based language that provides a model for describing Web services. The meaning of the acronym has changed from version 1.1 where the D was standing for Definition." Wikipedia.org

[12] "The name **Atom** applies to a pair of related standards. The *Atom Syndication Format* is an XML language used for web feeds, while the *Atom Publishing Protocol* (*AtomPub* or *APP*) is a simple HTTP-based protocol for creating and updating web resources." Wikipedia.org

and can be accommodated through mapping. It is better to have an application interface that can be mapped and leveraged for integration as opposed to not having an interface at all.

Another integration standard often used for process control integration is Object Linking and Embedding (OLE)[13] for Process Control (OPC) as defined by the OPC Foundation. OPC and the newer OPC Unified Architecture[14] are technologies used across process control-related domains for information exchanges. Many interfaces are defined by OPC, such as those for conveying measurement data. OPC UA is now an IEC standard known as IEC 62541.

An important trend of note is that of 'shallow integration,' where standard interfaces are defined in a manner that minimizes the depth of understanding a client must have of the models and processes internal to a service. In this way, it is possible to support integration of a diverse set of systems and allow for innovation.

3.4.10 Event Cloud

An Event Cloud is a logical construct where events generated by a wide variety of sources can be accessed, filtered, correlated and analyzed.

This type of analysis is called Complex Event Processing (CEP). CEP can be applied to many types of problems, including those related to Business Activity Monitoring (BAM). Some of the events that may be useful for complex event processing include:

- Device status changes
- Measurement limit violations
- Large differences between scheduled and measured values
- Phasor measurement snapshots
- Meter outage reports
- Meter power quality events
- Trouble calls
- Circuit overloads
- Pricing signals

[13] "**Object Linking and Embedding** (**OLE**) is a technology that allows embedding and linking to documents and other objects developed by Microsoft. For developers, it brought **O**LE **C**ontrol e**X**tension (OCX), a way to develop and use custom user interface elements. On a technical level, an OLE object is any object that implements the **IOleObject** interface, possibly along with a wide range of other interfaces, depending on the object's needs." Wikipedia.org

[14] **OPC Unified Architecture** is the most recent OPC specification from the OPC Foundation and differs significantly from its predecessors. After 3 years of specification work and another year of prototyping the first version of Unified Architecture is now being released. The OPC Foundation's main goals with this project was to provide a path forward from the original OPC communications model (namely COM/DCOM) to a current communications model namely SOA and introduce a cross-platform architecture for process control, while enhancing security and providing an information model. Wikipedia.org

- Demand response events
- Market submissions
- Resource availability changes & forecasting
- Processing errors
- Virtual Execution Environment changes

Figure 25 illustrates the relationships between Complex Event Processing (CEP) engine and ESB:

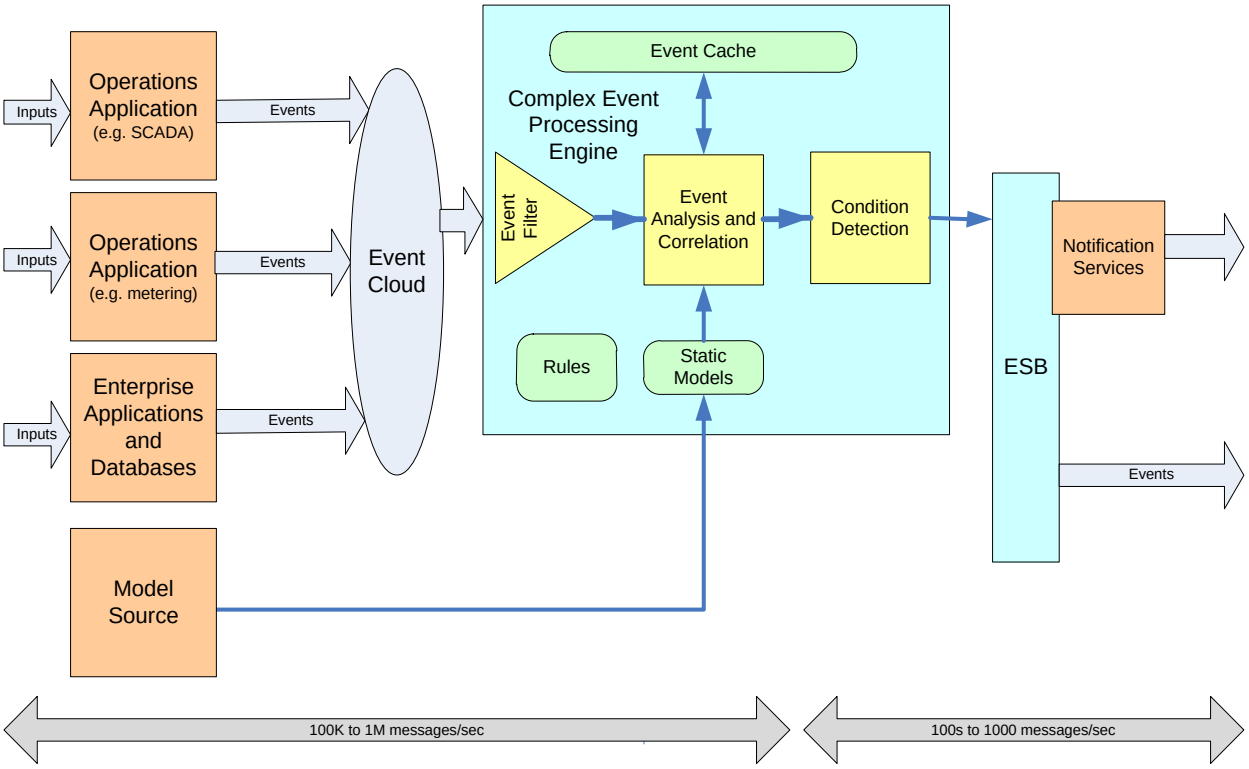

Figure 25 - Complex Event Processing

Events generated by various event sources are forwarded to the CEP engine, where the first process filters events that are not of interest. Events of potential interest are then added to a cache and an attempt is made using correlation rules and models to identify conditions of interest. If such a condition is detected, rules are applied to determine the necessary actions. Typically when a condition of interest is encountered, a notification service will issue an appropriate message to potentially interested persons (e.g. via e-mail) or components (e.g. via invocation of a Web service). Typically the automated detection of a condition of interest will trigger a business process.

Event messages are often candidates for use in complex event processing. Some measurements, such as status changes and analog measurements (especially those that might identify a limit violation), can be obtained using a variety of standards and are useful inputs to CEP. In many cases the CEP engine and rules must be able to use a model, such as a network topology model,

in order to analyze events. This aspect of ESB[15] integration demonstrates the usefulness of a common message envelope, where events from different sources can be conveyed to the CEP engine in a common way, avoiding the need for additional translations.

3.5 Integration

As previously discussed, tomorrow's energy environment will feature a wide variety of participants who will take on one or more roles in effecting the smart energy ecosystem.

Vertically integrated electric utilities will likely take on many roles, while other types of electric utilities may be content with more limited roles because of deregulation or outsourcing to service providers.

Therefore, the Microsoft SERA focuses on reducing integration costs for either situation through pragmatic, product-based approaches that avoid the costs and time-sinks of custom integration when and where possible.

Ignoring specific integration approaches, examples where integration may occur include integration between:

- Enterprise applications
- External Enterprise applications (e.g. load aggregators)
- Enterprise and the network operations center
- Enterprise and mobile users
- Network operations center and devices in the field
- Network operations center applications
- Orchestrated business processes and applications
- Orchestrated business processes and users
- Portals and enterprise applications
- Users and portals
- Users and devices

Figure 26 offers a template that accommodates four different aspects of integration:

- **Process-centric application integration**, where enterprise or control center applications are integrated through a service-oriented architecture (SOA). This may involve services, messaging between processes, short running workflows or the more complex interactions between services and resources through orchestration.

[15]" In computing, an **enterprise service bus** (ESB) consists of a software architecture construct, which provides fundamental services for complex architectures via an event-driven and standards-based messaging-engine (the bus). Developers typically implement an ESB using technologies found in a category of middleware infrastructure products, usually based on recognized standards." Wikipedia.org

- **Database-centric application integration**, where information exchanges between databases are driven through the use of Extract Transform Load (ETL) mechanisms.
- **Grid integration**, where the enterprise interacts with devices using standards defined by the IEC, IEEE and ANSI, where a variety of private and public networks can be leveraged as transports.
- **Web integration**, where users and organizations collaborate using Web-based technologies over the internet, intranet or virtual private network.

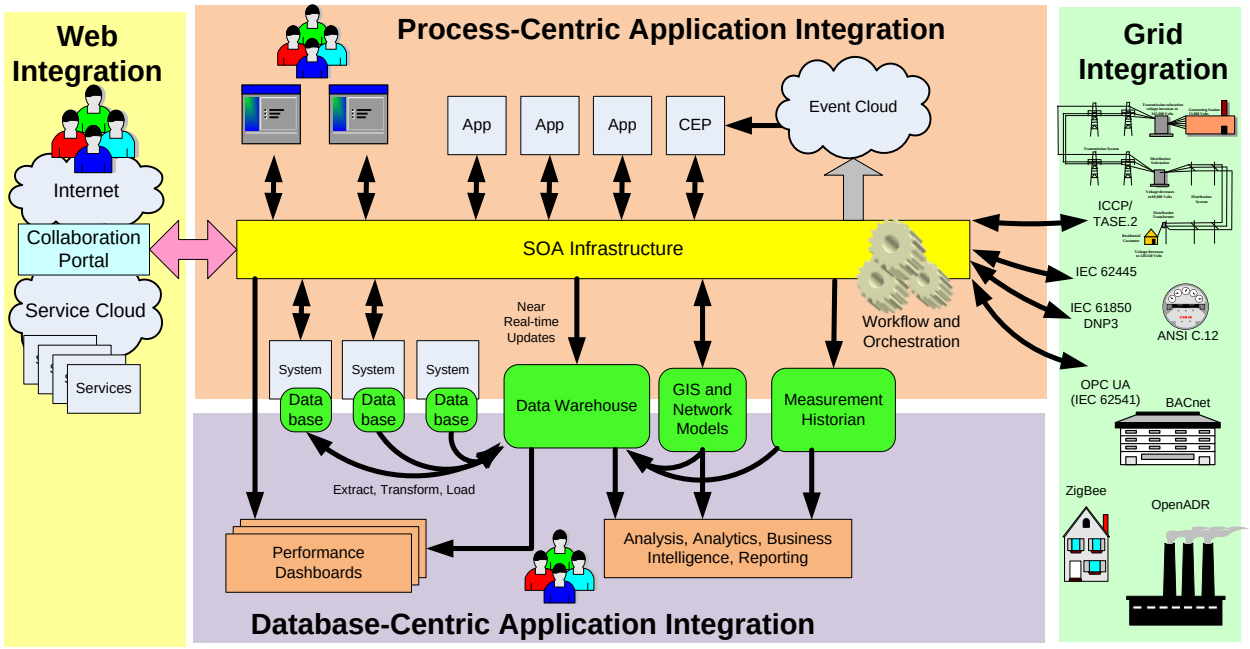

Figure 26 - Integration Overview

This section discusses the following integration concerns:

- Integration Patterns
- Service-Oriented Architecture
- Enterprise Service Bus in SOAs
- Applications
- Network Operations Centers
- Business-to-business Integration
- Customer Integration
- Power System Grid
- Common Services
- Cloud Services.

3.5.1 Integration Patterns

Integration patterns are used to design and build an integration architecture. Within the reference architecture there are three strategies for integration layers:

- **Entity aggregation**, providing unified data access across systems
- **Process integration**, which focuses on the orchestration of interactions between systems
- **Portal integration**, providing a unified view to the user

Several integration topologies may exist within each integration layer, including:

- Point-to-point connections
- Brokers
- Message buses

Identifying sets of patterns will be useful for integration efforts. These patterns may be implemented using off the shelf components, locally defined components or templates that provide a starting point for implementation. Integration patterns offer many benefits, as they fundamentally promote the reuse of designs and components.

3.5.2 Service-Oriented Architecture

Service-oriented architecture (SOA) is a design philosophy that is increasing in use and popularity within the utility industry as evidenced by its recognition in utility industry standards like IEC 61968.

While SOA has many different definitions, the World Wide Web Consortium (W3C) refers to SOA as "a set of components which can be invoked, and whose interface descriptions can be published and discovered." While Web services specifications provide an open standard on which SOAs are commonly built, a service-oriented architecture infrastructure still leaves many integration challenges. Figure 27 portrays a SOA reference architecture:

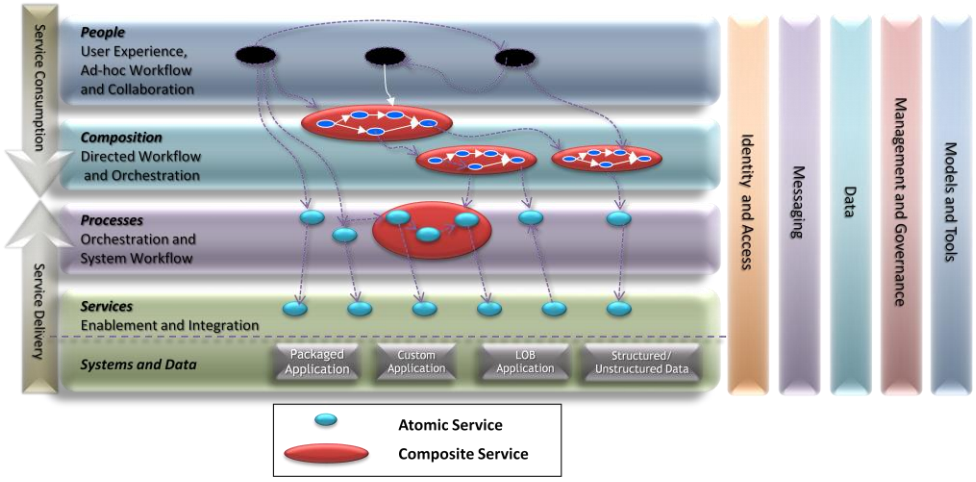

Figure 27 - SOA Reference Architecture

The SOA reference architecture illustrates both atomic and composite services, where workflow and orchestration may be used to coordinate services for consumers.

A simpler view is shown in Figure 28 from the perspective of service consumers and providers within an SOA.

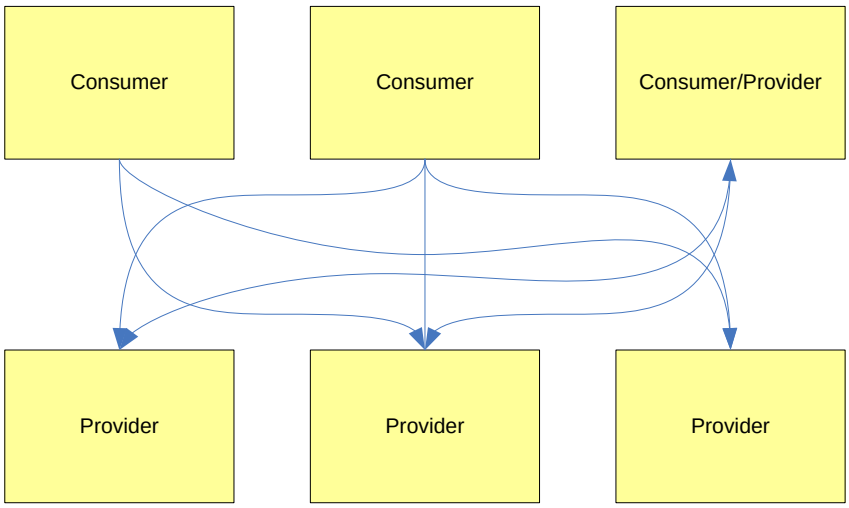

Figure 28 - Consumers and Providers in an SOA

While many SOA implementations focus on synchronous request messaging patterns, there is also the notion of an event driven SOA, where messaging patterns are expanded to include support for asynchronous messages, including events.

3.5.3 Enterprise Service Bus in SOAs

The term Enterprise Service Bus (ESB) is one pattern of messaging infrastructure and is widely used to form the backbone of the infrastructure of a service-oriented architecture. The characteristics common to ESB products include:

- **Brokered communication.** The basic function of an ESB is to send data between processes on the same or different computers. Like message-oriented middleware, the ESB uses a software intermediary between the sender and the receiver, providing a brokered communication between them.
- **Address indirection and intelligent routing.** ESBs typically include some type of repository used to resolve service addresses at run time. They also typically are capable of routing messages based on a predefined set of criteria.
- **Basic Web services support.** A growing number of ESBs support basic Web services standards including SOAP and WSDL as well as foundational standards such as TCP/IP and XML.

- **Endpoint metadata.** ESBs typically maintain metadata that documents service interfaces and message schemas.

Figure 29 shows a set of service consumers and providers integrated via an ESB. Aside from providing for reliable messaging, process orchestration, common services (sometimes called 'utility services') and other functionality, the ESB makes the integration much more manageable, especially when the integration is grown to dozens or more components.

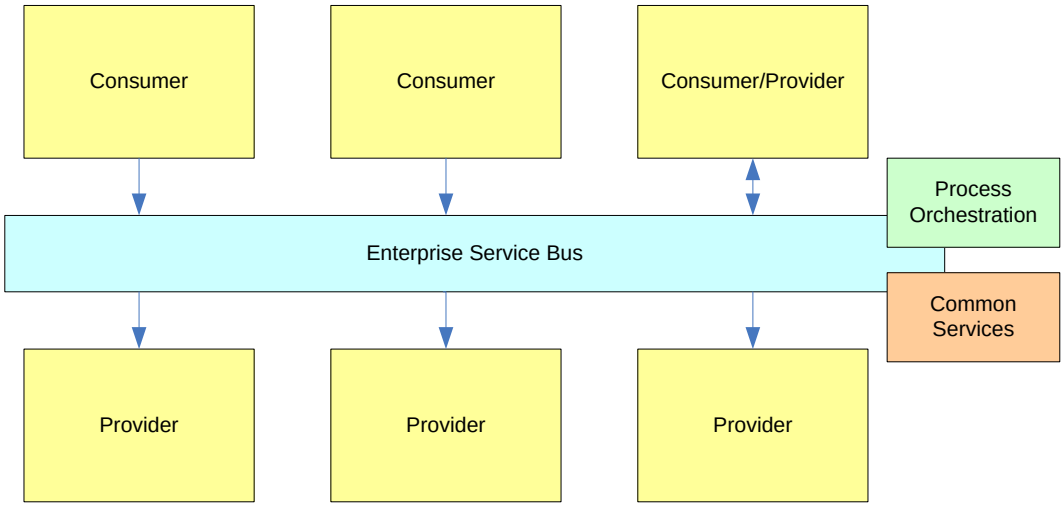

Figure 29 - SOA Using an ESB

An ESB is one of many building blocks that comprise a comprehensive SOA. The messaging capabilities required in an SOA extend the functions of traditional Enterprise Application Integration (EAI) and Message Oriented Middleware (MOM[16]) to include first class support for Web service standards and integration with other infrastructure components such as policy management, metadata registry, and operational and business monitoring frameworks.

It is important that an ESB enhance the ability to leverage existing assets in a service-oriented world. Many enterprise applications were not designed with SOA in mind. This is especially true, given the diverse and evolving nature of the many recommended standards for use within the smart grid.

3.5.4 Applications

An enterprise may need to integrate many varied applications in order to support business processes.

[16] Note: MOM in this context should not be confused with Microsoft Operations Manager.

For example, some applications are highly productized and have well defined interfaces, while others may be custom developed or highly customized to meet the needs of a specific company or a market. Others may be deployed within an enterprise or use cloud-based services.

For these reasons, the integration infrastructure should readily accommodate the "impedance mismatches" between applications and prevent the need for further application customization.

As such there is real need to leverage mechanisms to easily automate various business processes. In contrast to a user needing to interact directly with individual applications (i.e., working with code), it is now possible to construct composite applications where users are shielded from the underlying details of the related applications.

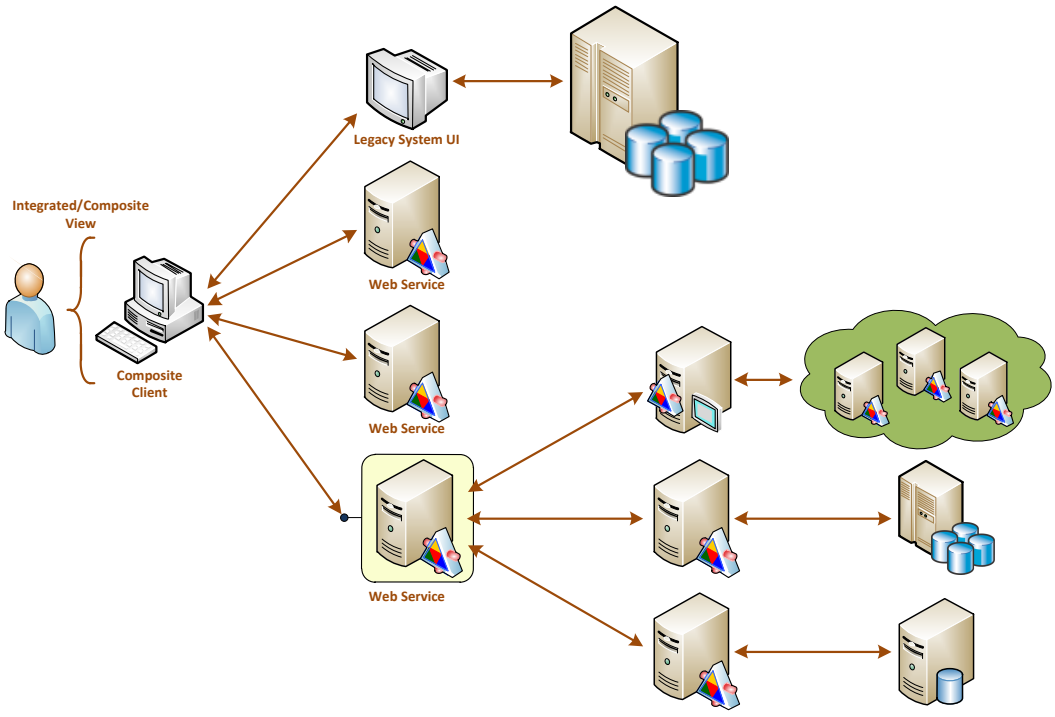

Figure 30 - Composite Applications

Instead, the user's view is often constructed as a Rich Internet Application (RIA). Information can then be collected from many systems, and underlying transaction functionality may be an orchestration, via a set of Web service interactions.

3.5.5 Network Operations Center (NOC)

Because of its emerging nature, the smart energy ecosystem is introducing the need to segregate applications into two types:

1) **Those used to support business processes within the network operations center (NOC)**. The NOC can be used for any combination of management of the grid, transmission

networks or distribution networks. The technical infrastructure supporting the operations center business processes is typically responsible for management of the electricity grid, which is a critical infrastructure. For this reason it is rigorously protected from the perspective of security, availability and performance.

2) **Those used elsewhere in the enterprise**. While the rest of the enterprise still requires a high level of security, requirements for availability and performance may be relaxed. In response, the reference architecture provides for the use of multiple buses, where bridges used to pass messages between the buses can serve as insulation, thus isolating the impacts of servicing information to the enterprise from the operational systems.

In Figure 31, a variety of standards are used to integrate the databases and applications within the network operations center with components outside of the NOC. The IEC and IEEE provide many of these standards, especially those to other operations systems or the field.

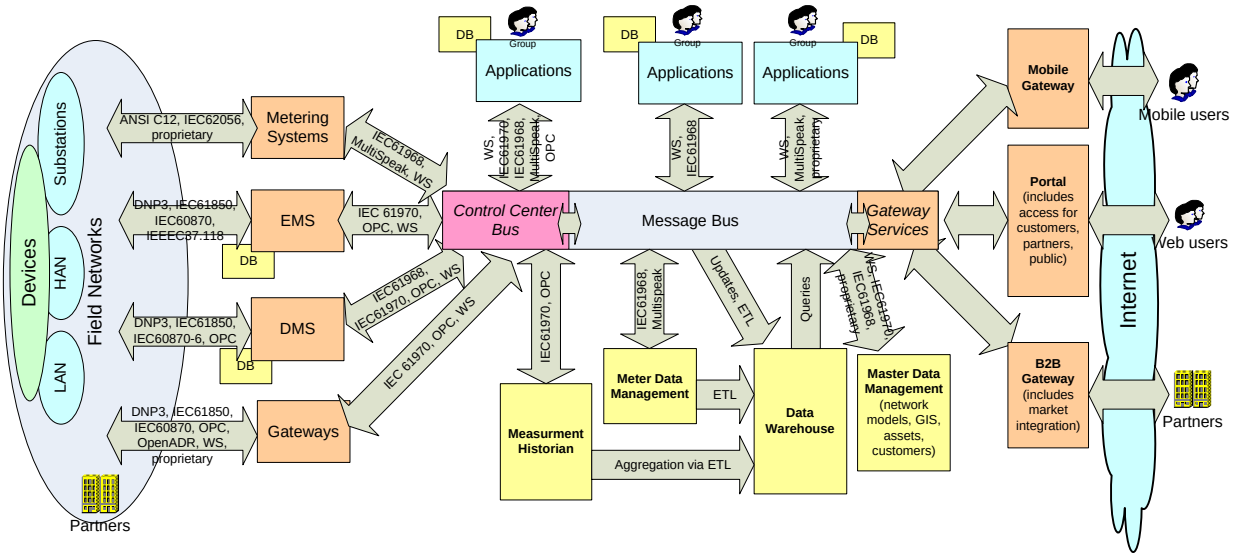

Figure 31 - Use of Standards for Integration

From an integration perspective, these interfaces are implemented using productized adapters and gateways. The following examples are those standards supported by such adapters and gateways:

- Inter-control center data links using IEC 60870-6, also known as ICCP and TASE.2[17]

[17] The **Inter-Control Center Communications Protocol** (ICCP or IEC 60870-6/TASE.2) is being specified by utility organizations throughout the world to provide data exchange over wide area networks (WANs) between utility control centers, utilities, power pools, regional control centers, and Non-Utility Generators. ICCP is also an international

- Substation communications using IEC 61850 and DNP[18]3
- Process control communications using OLE for Process Control (OPC), where the new OPC Unified Architecture (UA) is standardized as IEC 62541
- Model exchanges using IEC 61970 standards
- Meter integration using IEC 61968-9 and ANSI C12 standards
- Demand response integration using OpenADR and ZigBee specifications
- Communications to and between smart devices on home area networks using IPSO, [19]ZigBee and/or HomePlug.
- Application integration based upon IEC 61968, IEC 61970 and MultiSpeak specifications

In situations where the network operations center is required to operate flawlessly in a 24-7 environment, it is common for NOC functionality to be supported using redundant networks and hardware. In some cases, this may be extended so that the NOC is deployed at two different geographically distinct sites in order to protect against a variety of physical threats, including but not limited to earthquakes, fires and acts of terrorism. Consequently, support for inter-site failover of NOC functionality is often a requirement. See Figure 32.

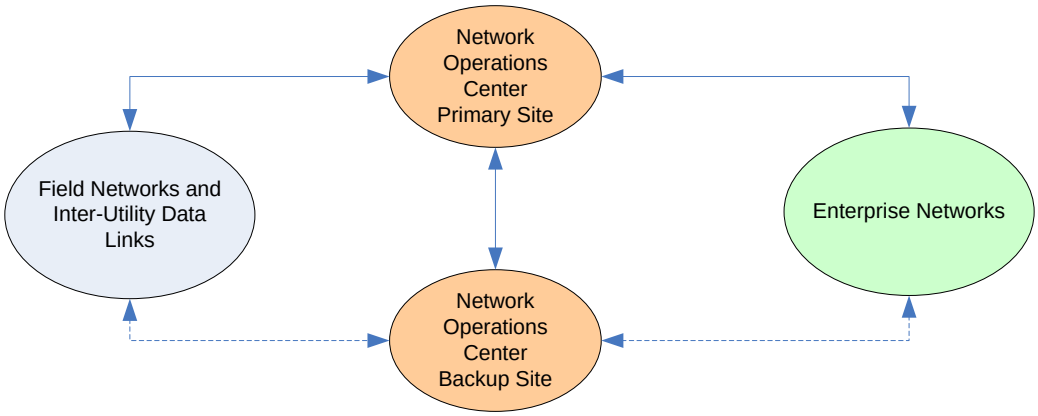

Figure 32 - Network Operations with Backup Sites

---

standard: International Electrotechnical Commission (IEC) Telecontrol Application Service Element 2 (TASE.2). Wikipedia.org

[18] The development of DNP3 was a comprehensive effort to achieve open, standards-based Interoperability between substation computers, RTUs, IEDs (Intelligent Electronic Devices) and master stations (except inter-master station communications) for the electric utility industry. dnp.org

[19] IPSO is an alliance for promoting the use of IP-based technologies for smart objects, including those found on a home area network.

When there are multiple NOCs, at any point in time, one NOC is typically designated as the on-line NOC where the NOC applications are running on local hardware in an on-line mode. The databases at the backup site are kept up-to-date to mirror the contents of the online databases so as to be concurrent within a small time interval. When circumstances or operational procedures dictate, on-line functionality can be transferred from the primary site to a backup site. Users can be physically located at either site, where their ability to access the functionality provided by the on-line NOC is unimpaired except for obvious cases where their physical location is not functional or cannot access the on-line site.

A NOC also has provisions for development, training and testing environments. These environments are often built upon a network, with hardware and application software that enables operations staff training and application software testing, particularly for new software versions. See Figure 33.

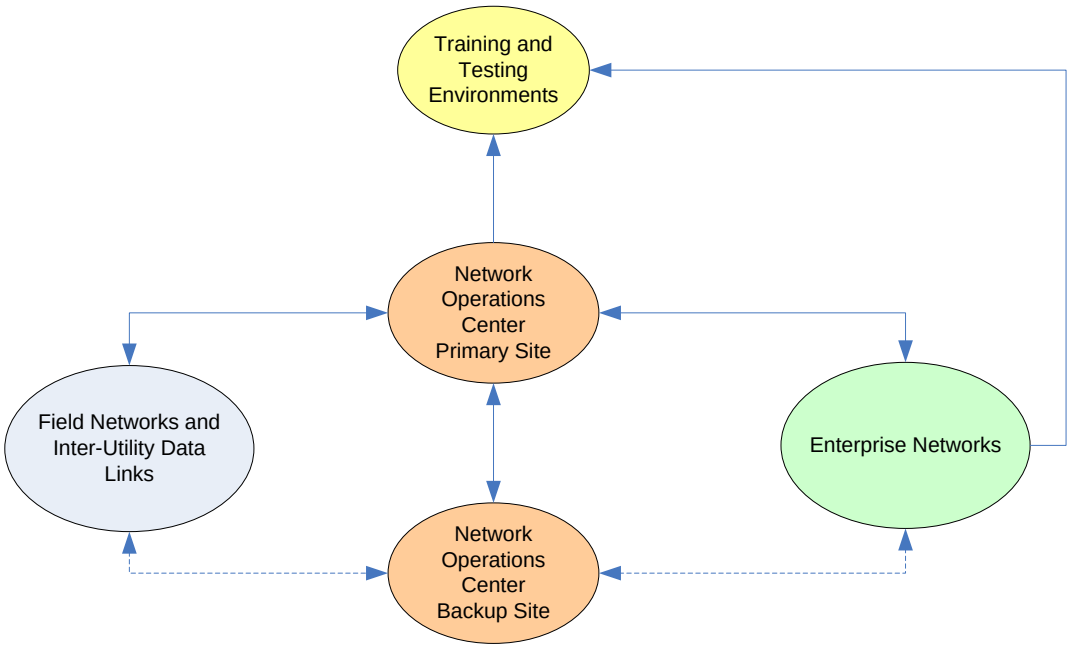

Figure 33 - Configuration of Training and Testing Environments

The underlying databases for training or testing environments can be initialized using either current or recent data from the NOC as well as potentially some enterprise systems. However, information or operational requests from training or testing systems should never be propagated back to a NOC or other enterprise system, as this would effectively contaminate those systems with invalid data.

3.5.6 Business-to-business Integration

The Smart Energy Ecosystem contains many examples of need for business-to-business integration, including integration between ISOs, utilities and service providers.

Such integration is becoming increasingly dependent upon the Internet, as opposed to private data links, which creates several notable requirements for message transport:

- **Mutual authentication**, typically using X.509 certificates
- **Encryption**, typically leveraging TLS[20]
- **Signatures for non-repudiation of transactions**, typically leveraging WS-Security

There are three primary patterns for one business to obtain information from another:

- **Request/reply integration** via secure Web services (noting that Web services may not need to be secured if only public information is conveyed)
- **Publish/subscribe integration**, where an organization may publish information to registered partners
- **Portal integration**, where a registered user for an organization can log into a partner portal to interactively submit transactions or view reports.

Information within messages is now typically conveyed using XML documents, replacing the situation where a variety of proprietary formats were common in the past. Aside from the fact that many standards now specify information exchanges in the form of XML documents, they also have the advantages of being structured, self-descriptive and can be leveraged by a wide variety of tools.

All integrations require observance of information protection and privacy concerns. For example, where an ISO maintains demand response program registrations, those registrations may need the approval of only certain details by different organizations. That means that other details must be hidden from organizations who do not share the "need to know." Indeed, each piece of information maintained by an organization may have a different level of confidentiality. These levels would include:

- **Public**, where the information has no confidentiality restrictions
- **Shared** by a set of designated organizations, such as market participants
- **Specific accessibility** by one or more identified organizations
- **Private**, where the information is not shared externally

Additionally, there is typically the need for role-based access control (RBAC) where:

- Each organization has a set of users
- Each user has one or more roles within the organization
- Each role identifies privileges, allowing access to resources, such as the ability to read certain sets of information and/or submit certain types of transactions

[20] **Transport Layer Security** (**TLS**) and its predecessor, **Secure Sockets Layer** (**SSL**), are cryptographic protocols that provide security for communications over networks such as the Internet. TLS and SSL encrypt the segments of network connections at the Transport Layer end-to-end. Wikipedia.org

A notable example of RBAC is the separation between the unregulated side of the utility business (generation and traders) from the internal transmission network operations information such as grid status, which could give them an undue competitive advantage. Traders could “game” the market knowing when and where congestion might occur due to transmission network operations.

3.5.7 Customer Integration

Within the smart energy ecosystem, a wide variety of customers will collaborate with utilities, service providers and devices. Those customer types include:

- Residential
- Commercial
- Industrial
- Wholesale

For the purpose of the following discussion, it’s important to note that some aspects of the reference architecture may be more appropriate for one group than another.

As previously discussed, customers are changing, becoming active participants on the electric grid by engaging with new technologies. Customers are now more than energy consumers. Regardless of whether they are large or small, they may now export energy to a distribution network, or potentially the transmission network in the case of very large customers.

Figure 34 illustrates how a residential customer may interact with the smart energy ecosystem though collaboration portals and home area networks.

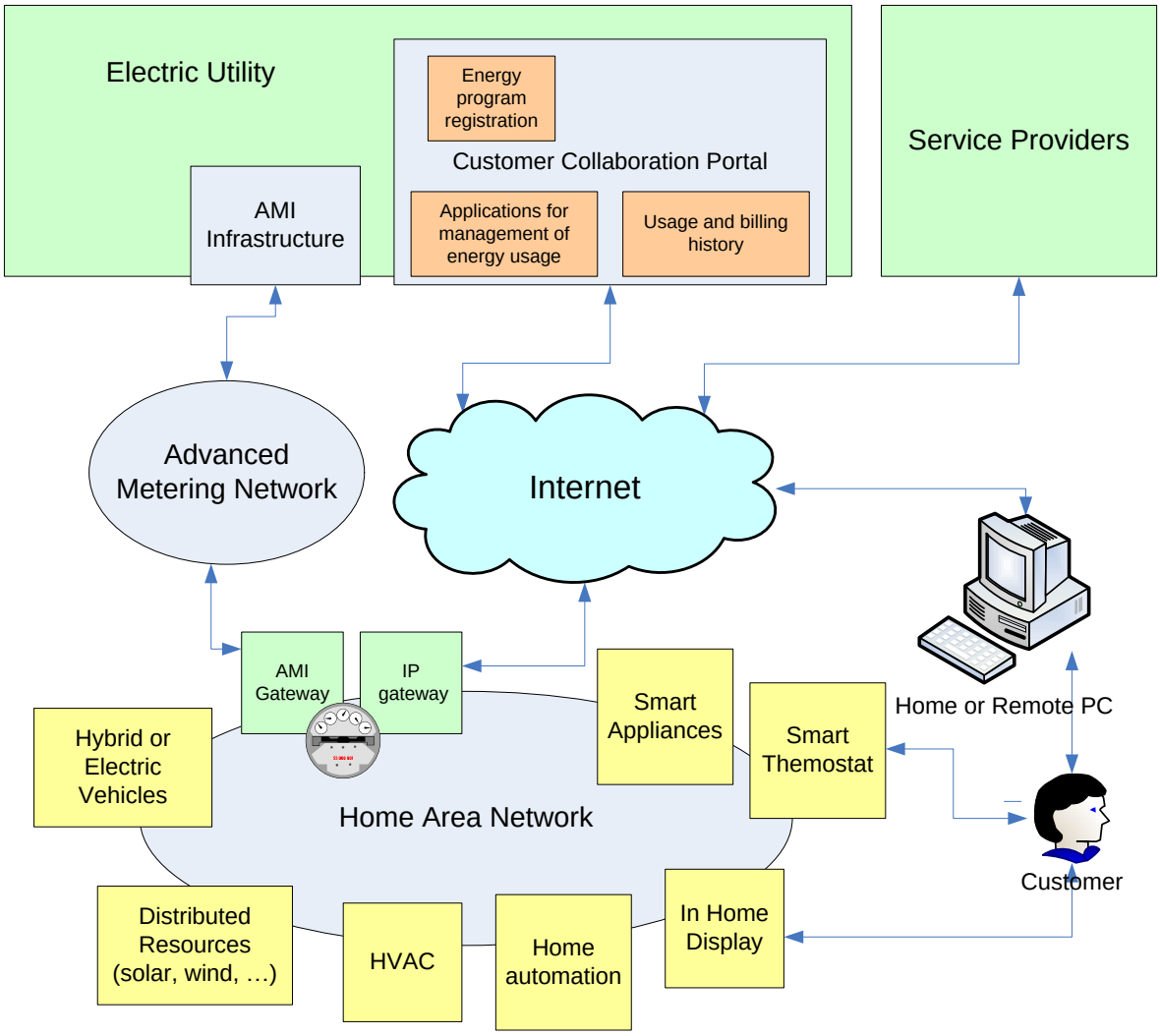

Figure 34 - Residential Customer Interactions with Smart Energy Ecosystem

Customer-focused portals provide access to billing, usage history and energy programs. Customers may be able to participate in demand response programs or offer distributed energy resources to the energy market.

One example of a common energy resource will be the storage opportunity that batteries in hybrid or electric vehicles offer. Batteries permit a vehicle to be recharged at those times of the day or night when prices are low. Or the grid operator could draw from the batteries as an energy source at times when prices are higher and somehow compensate the battery owner (as long as this is properly coordinated with the vehicle owner's planned driving schedule).

The communication framework used by advanced meter infrastructures (AMI) may come into use as a gateway into home area network, where a specific HAN technology may be used within the home or business for device integration.

Currently, a ZigBee Smart Energy profile is used to define devices and their interactions within the HAN. In this way, local devices can respond to market price schedules, pricing signals and demand response events.

From a standards perspective, there is currently a standardization gap between the HAN and the utility (or service provider). When this gap is closed, utilities or service providers will be able to interact with the HAN gateway, which, in terms of the ZigBee Smart Energy profile, will be called an Energy Services Portal (ESP). A more general movement towards embracing the use of IP communications to HAN devices is clearly seen through efforts of the IPSO alliance.

Customers may also employ service providers that act as aggregators for purposes of participating in distributed generation or demand response programs, where the aggregator can then competitively participate in an energy market using the integration options provided in a smart energy ecosystem.

In the cases of commercial and industrial customers, BACnet, LonWorks and OpenADR are the current common standards being used for demand response:

- BACnet is a standard used for building automation control systems.
- LonWorks is a standard for building automation networking.
- OpenADR is starting to come into use by utilities and service providers to issue pricing signals and load control events.

Integration solutions at the customer level must be inexpensive and easy to install and maintain. Many factors demand plug and play integration and significant standardization at this level. Customers will also need to have capabilities for more local preferences and control.

3.5.8 Power System Grid

Integrating with the grid involves meshing those devices that are used to monitor and control equipment and resources on the grid.

A number of industry standards are being widely used for such purposes, including those provided by organizations such as the IEC and IEEE. Integration with these standards is typically accomplished using capabilities provided by a vendor system, or through the use of a third party adapter. These adapters then typically use field networks for communication, which are often private, highly isolated or highly protected from use by parties other than the electric utility that owns the equipment being controlled.

Data acquisition from, and control commands to substations, Intelligent End Devices (IEDs), and metering devices often use a variety of networking technologies in the field. Many different types of devices are used in the exchange of measurements, controls, meter readings, signals, events, etc., and many different standards are used to support these exchanges. Some of these standards are very stable and some are still evolving. Figure 35 illustrates integration over networks.

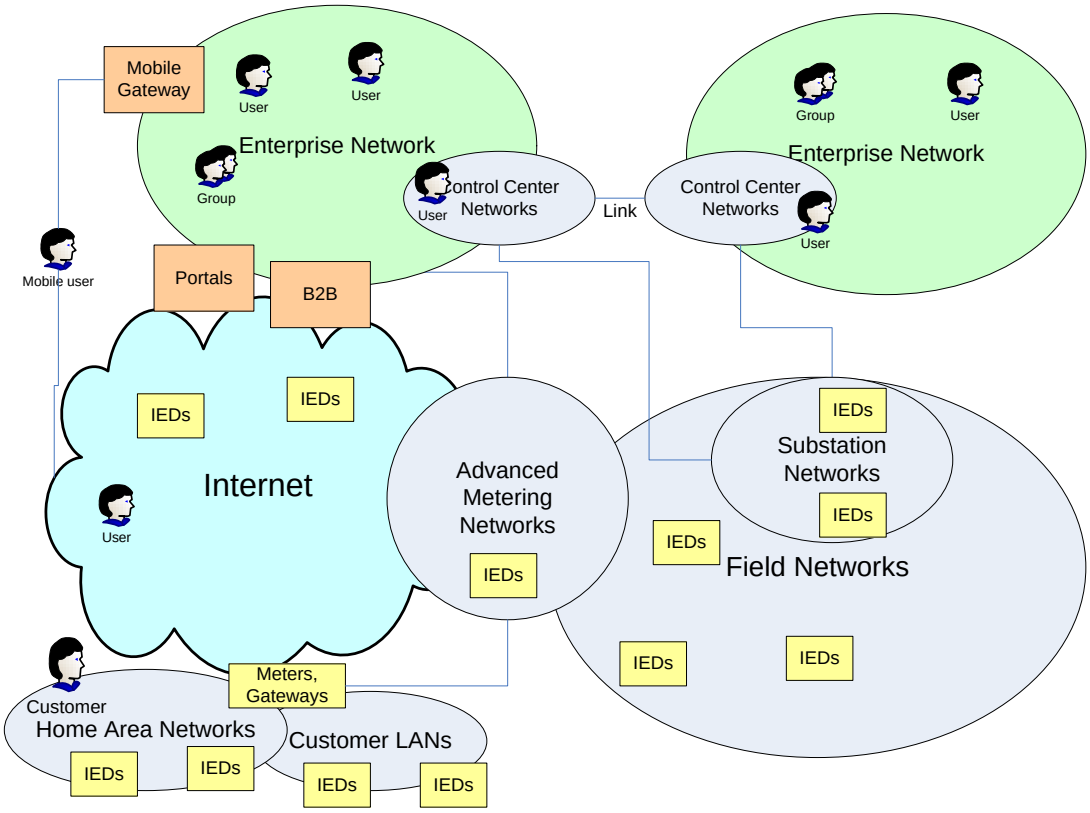

Figure 35 - Integration over Many Networks

The following paragraphs provide a brief introduction to some of the most commonly used standards and how they apply in the overall system architecture. These include:

- Intelligent End Devices
- Distributed Network Protocol
- Inter-Control Center Protocol
- IEEE C37.118
- IEEE 1547.3
- ANSI C12
- ZigBee and IPSO
- Open Automated Demand Response
- BACnet
- LonWorks

3.5.8.1 Intelligent End Devices

Clearly, the various networks will allow more autonomous decision making and controls within substations, on feeders, and locally by resources. To further enable this trend, intelligent end devices (IEDs) need to integrate via plug-and-play standards, especially those

IEDs at the end user level. Devices in substations and on feeders are configured. There is typically no custom software or integration at this level. The IEC 61850 series of standards defines the communication for substation and feeder automation, providing for interoperability between IEDs. This is primarily used for control and protection within substations and on feeders. Within IEC 61850, a dialect of XML called Substation Configuration Language (SCL) is used to describe automation systems and IEDs. A hierarchical model is used within IEC 61850, where a server can have:

- many logical devices
- each with many logical nodes
- each with many data objects
- each having many attributes

IEC 61850 uses a high speed station and process bus, allowing an IED to publish events to other IEDs packaged as Generic Object Oriented Substation Event (GOOSE) messages. There are many vendors providing a wide variety of IEC 61850-compliant devices and applications. There are also gateway products and toolkits that can be leveraged for integration purposes.

3.5.8.2 Distributed Network Protocol

Distributed Network Protocol 3 is another protocol commonly used for communications between SCADA master stations, remote terminal units (RTU) and IEDs. Within DNP 3, data is organized into data types that include:

- Binary inputs
- Binary outputs (e.g. controls)
- Analog inputs
- Analog outputs
- Counters

Data points are defined from these data types to manage a single value. Measured values can be reported periodically or by exception. The DNP3 protocol is supported by products from many SCADA vendors and has been widely deployed.

3.5.8.3 Inter-Control Center Protocol

IEC 60870-6 is a standard used to provide data links between control centers for the exchange of measurements and controls. (IEC 60870-6 is also commonly known as TASE.2 and the Inter-Control Center Protocol (ICCP). This protocol has been in use for many years, and is supported by a variety of SCADA and Energy Management Systems, as well as other vendor products. There are also gateway products and toolkits that can be used for IEC 60870-6 data links.

3.5.8.3 IEEE C37.118

The IEEE C37.118 standard defines synchronized phasor measurements used in power system applications. Given that an IED can leverage GPS for accurate time synchronization, it is now possible to obtain accurate, synchronized measurements of the wave forms for points on the electricity grid. This standard has been submitted to the IEC for inclusion within IEC 61850.

3.5.8.4 IEEE 1547.3

The IEEE 1547.3 standard is a guide for monitoring and exchanging information and controlling distributed energy resources. This document is at the level of use cases and examples, leaving some gaps for future standardization.

3.5.8.5 ANSI C12

ANSI C12 is a suite of standards used to standardize many aspects of meters. These standards range from decide codes to optical ports to protocol specifications, and they recognize that meters are used for water and gas, as well as electricity.

3.5.8.6 ZigBee and IPSO

Two technologies are being proposed for home area networks (HAN), including ZigBee and IP for Smart Objects (IPSO).

- **ZigBee** allows for secure wireless communication between devices, where specific devices may provide specific capabilities useful for energy control and conservation.
- **IPSO** is focused on the use of IP for connections and communication between Smart Objects.

HAN technologies such as ZigBee and IPSO can also be applied to commercial and industrial settings as well as residential settings. Examples of HAN integration include:

- Meters
- In-home displays
- Smart appliances
- Thermostats
- HVAC
- Occupancy sensors
- Lighting
- Pool pumps
- Charging of PHEVs

Where the specifications for communication within the HAN are well defined, the gateway between the HAN and the utility is not and represents a notable gap. Currently,

the gap is often bridged by closed mechanisms, such as the proprietary communications provided by some metering infrastructures. However, this then creates challenges to security, reliability and scalability.

One very challenging security issue relates to making all the devices integrated on the HAN accessible and visible from the internet. Scalability is largely constrained by whether a multicast capability can be leveraged to send signals. An open gateway specification is a likely area for standardization, which would then also likely provide for HAN networks based on a variety of technologies such as IPSO, HomePlug or ZigBee.

3.5.8.7 Open Automated Demand Response

Another specification coming into some use for demand response is Open Automated Demand Response (OpenADR) which allows for the management and execution of demand response programs, where pricing signals and load control requests can be issued to clients. OpenADR supports the communications between client devices and a server for events, pricing signals and bidding.

3.5.8.8 BACnet

BACnet is a standard used for building automation and control networks. Specifications such as ZigBee and OpenADR recognize the need for BACnet integration. Within industrial settings, OPC is another technology that might be used for controlling and monitoring equipment.

3.5.8.9 LonWorks

LonWorks is a protocol standard (codified under ANSI/CEA-709.1-B and ISO/IEC 14908-1,2,3,4) that is used for communications on twisted pair, power line, fiber optic, RF media for data acquisition and control functions in buildings for equipment such as lighting, HVAC and other building controls.

3.5.9 Common Services

Common services provide functionality that can be leveraged by many applications and generally fall within two categories:

1. **Generic** in nature, e.g., for logging and notifications
2. **Domain focused**, e.g., for topology processing and power flow

Common services are sometimes the realization of SOA as a reusable component. They can also be provided as functionality embedded within an integration infrastructure. Some common services may also be obtained as third party products.

3.5.10 Cloud Services

Cloud-based computing is the term for a new computing model where resources are contained on, and delivered to, users via the Internet.

An Internet accessible infrastructure exists within the cloud to provide a platform for the deployment of services and applications. This infrastructure is dynamically scalable and highly available, where virtualized resources are provided as a service. Use of the cloud has enabled several new computing models:

- Software as a service (SaaS), where an application is licensed to a customer for use as a service on demand, usually accessed through a Web browser.
- **Infrastructure as a service** (IaaS), where instead of purchasing and installing servers and software, a computing platform is purchased as an outsourced service (including datacenter space, servers, storage, networking, and software often provided as a virtual machine environment).
- **Platform as a service** (PaaS), also known as "cloudware," where both the computing platform and solution stack are delivered as a service (used to develop and deliver solutions to end users).

Additionally, cloud services:

- May be leveraged by service providers, utilities and ISOs to offer new services
- Can significantly reduce the time to deployment of a new solution for an end-use customer
- Are extremely well suited for delivery of solutions to customers without the expertise, staffing, or deep datacenter capabilities for on-premise deployments
- May be integrated with on-premise platforms to create a truly distributed computing environment

3.6 Application Architecture

The key requirements for application architecture include:

- Efficient construction of high quality software components
- Location independent user interface through a browser
- Interoperability through Web services
- Ability to construct composite applications
- Libraries of reusable components
- Development and testing tools

Application architecture implemented using modern application frameworks such as Microsoft® .NET Framework also provide for the use of managed code to improve application portability and security. Application frameworks can be either all-encompassing or specialized for the needs of certain types of software development, where examples include:

- Graphical user interfaces (GUI)
- Web services
- Rich Internet Applications (RIA)

- Mobile applications
- Embedded applications

Even though applications may be developed using different frameworks, interoperability is provided through various standards, such as the ubiquitous use of Web services. However, within an organization there can be significant advantages to the selection of a single application framework that is encompassing and well supported by development tools.

3.7 Security

Security is an extremely important aspect of a smart energy ecosystem, given the mission critical nature of the infrastructure.

In the past, communicating to field equipment was channeled through closed, proprietary communication infrastructures. Now, open and standards-based infrastructures are being used to a rapidly growing degree.

While the openness and interconnection offer great benefit to businesses and users, they also present security challenges that must be addressed at both the design and operating stages of the smart energy ecosystem. Indeed, security now must be a first-thought consideration and considered holistically. Effective security is not a set of bolt-on products to new or existing infrastructure:

- **Secure development practices** should be used to design and deliver the systems that will power the Smart Energy Ecosystem.
- Owners and operators must exhibit sound and **secure operational practices** in order to help protect these vital services.

3.7.1 Secure Development

In designing their components for the smart energy ecosystem, all software vendors should address security threats. Security is a core requirement for software vendors, driven as it is by market forces, the need to protect critical infrastructures, and the need to build and preserve widespread trust in computing.

All software vendors face the daunting challenge to create more secure software that helps protect users and computers from today's threats while enhancing the manageability of software and services.

For the software providers, the key to meeting demands for improved security is to implement repeatable processes that reliably deliver measurably improved security. Therefore, software vendors must transition to a more stringent software development process that focuses, to a greater extent, on security. Such a process is intended to minimize the number of security vulnerabilities extant in the design, coding, and documentation and to detect and remove those vulnerabilities as early in the development lifecycle as possible.

The need for such a process is greatest for enterprise and consumer software that is likely to be used to process inputs received from the Internet, to control critical systems likely to be attacked, or to process personally identifiable information.

3.7.2 Secure Operations

Ensuring secure operations is also a critical component for reliability of the smart energy ecosystem.

Secure design and deployment of applications and infrastructure can be compromised through failure to adhere to secure operations guidelines. NERC CIPs provide such guidance for the operation of the transmission system. Proper training, qualification and operation should be included in the utility operational security program and the architecture must enable execution and reporting on these programs.

4.0 Microsoft Technology Stack

The smart energy ecosystem could be implemented end-to-end using Microsoft technologies in conjunction with products provided by third party vendors, many that also build on the Microsoft technology stack[21]. Realistically, a homogeneous Microsoft technology deployment is seldom the case, but the use of interoperability standards can effectively overcome any potential challenges.

This section seeks to describe how the Microsoft technology stack can be leveraged and discusses its advantages over other alternatives. The section includes:

- Stack Integration Overview
- Capability-based Information Architecture
- Collaboration Services
- Process Integration
- Databases and Data Warehouses
- Business Intelligence
- Complex Event Processing
- Mobility
- Management and Security
- System Center
- End to End Trust
- Platform
- Virtualization

[21] A technology stack comprises the layers of components or services that are used to provide a software solution or application, according to its definition on Wikipedia.org[21]

4.1 Stack Integration Overview

As overview, Figure 36 provides an integrated view of the overall architecture in an electric utility. The diagram shows:

- The technologies in use within an electric utility
- Applications that are typically provided by third party vendors
- The integration architecture leveraging a variety of Microsoft products to establish an enterprise wide strategy

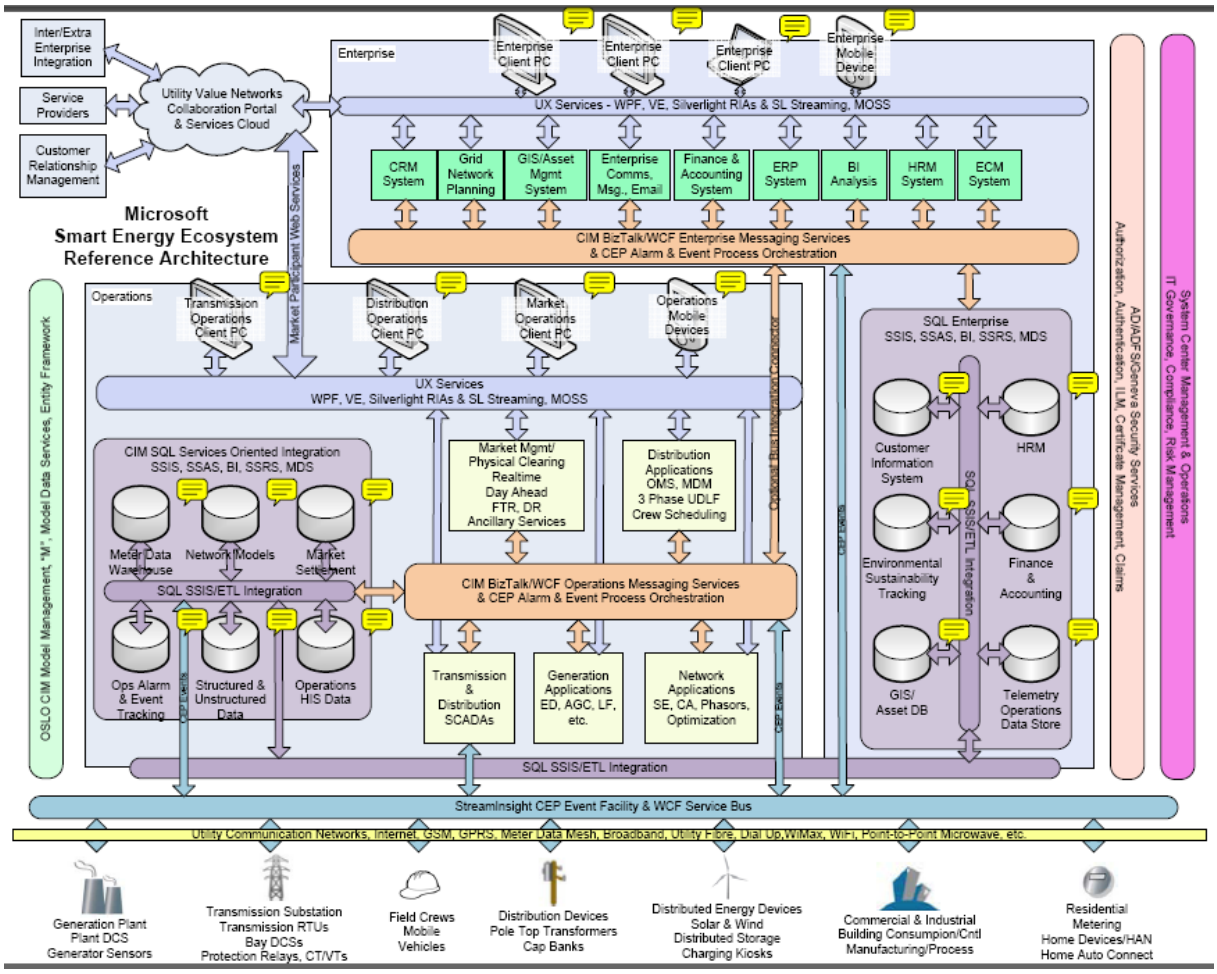

Figure 36 - Integrated View of Overall Utility Infrastructure

The overall reference architecture establishes a messaging and process integration approach, as well as data warehousing and storage approach, consistent with the integration overview of Figure 36.

The overall architecture shown in Figure 36 reflects several key points:

- A variety of communications approaches will exist for field connections, but transition to consistent core communications channels as early as possible limits the impact to the rest of the architecture.

- Data is captured and reduced to information and events as close to the source as possible.
- Consistent integration is enabled via core technologies at the data Integration level, at the messaging/process integration level and at the user experience level.
- StreamInsight CEP is used to service events, both for filtering and analysis of complex composite events, and stream management across the whole architecture.
- The Windows Communication Foundation (WCF) Service Bus is used to transport data both for on-premise and for supply to Windows Azure Services.[22]
- Shallow integration is leveraged to hide complexity and implementation details at interfaces to enable rapid development/deployment and agile response to market forces.
- The CIM is leveraged both as the basis of message definitions as well as a direct contributor to the schema for data marts or data warehouses.
- SQL Analysis for business intelligence is enabled by Extract, Transform & Load (ETL) integration across the architecture. The approach to data replication is described below.

4.2 Capability-based Information Architecture

Business capabilities for the Microsoft reference architecture scenarios drive the decisions for information architecture and are represented by role, tools and most importantly, data timeliness requirements.

This concept, pictured in Figure 37, is coupled with our notion of **service-oriented business intelligence** and guides design preferences for integration.

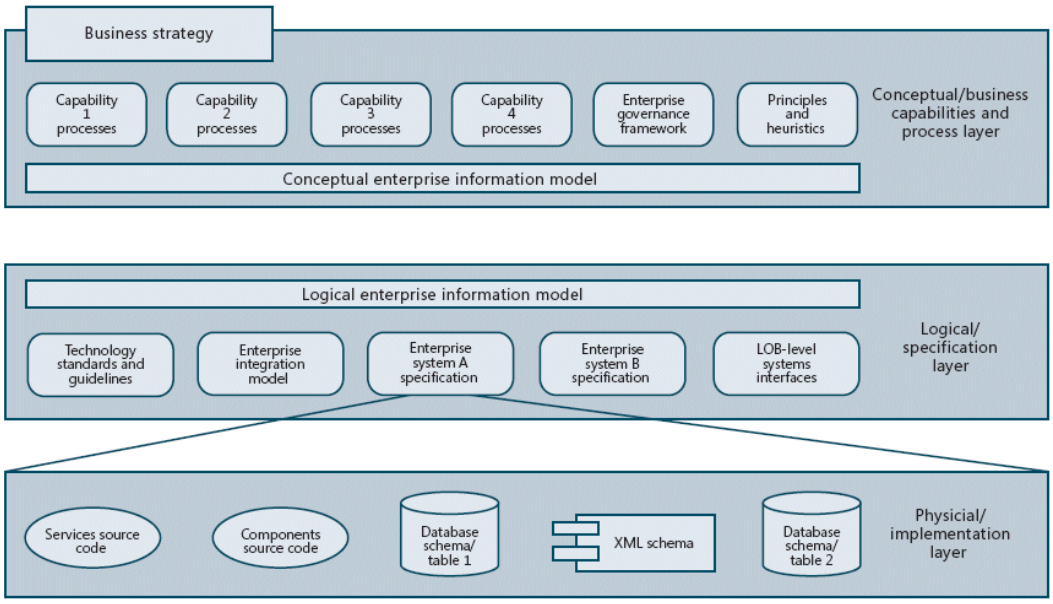

Figure 37 - Capability-based Information Architecture (Source: Architecture Journal)

[22] Juval Lowy of iDesign provides a good discussion for implementing Service Bus connectivity to the Internet in his article Working With The .NET Service Bus.

We will explore when to use the following approaches:

- Event-driven Enterprise Services Bus (and Microsoft Manufacturing Toolkit)
- Data Integration Architecture (EAI and ETL)

4.2.1 Event-driven Enterprise Services Bus and BizTalk Server

While .NET and Web services standards can be employed to event application and time series data, it becomes more difficult to "manage" based on the number of points and types of integration, both machine/application and people oriented workflow.

Our approach is to leverage a services bus for the publishing and subscription of data and applications for a "managed integration."

Process events, like out of range limit alarms, take many forms that will drive different activities. A functional imperative for many of our solutions is to enable cross-boundary workflow between applications, and people-oriented workflow, depending on the severity or trend of an event.

Events and workflows are managed and monitored through business activity monitoring. In most near real-time event processing scenarios, the BizTalk Server ESB solution is sufficiently scalable to process hundreds of small documents each second. For higher performance requirements, Microsoft StreamInsight Complex Event Processor can be used. StreamInsight has demonstrated performance exceeding 100K events/second.

The Microsoft Manufacturing Toolkit demonstrates the use of the Microsoft platform, including BizTalk Server, to build a publish/subscribe services-based architecture. The toolkit consists of guidance documentation and demonstrative code-samples.

A design principle is that time series data will be hosted in a real-time historian database. Calculated data from this source will be made available to an events data warehouse via a Web service through BizTalk Server. Options for event processing include:

- Instantiate an operational workflow
- Notify a subscribing application
- Notify an engineer for immediate attention

The overall reference architecture diagram (Figure 36), shows two CIM integration message busses: one for operations and one for the enterprise. The busses could be implemented as a single message bus so that there is a single version of the truth. However, for security and performance reasons, operations typically implement an isolated messaging architecture. As a result, only messages that specifically pertain to operations are passed (such as asset model updates when equipment is added or moved). These could be reflected as events, and passed as model update events, or passed as messages. The rest of the messaging traffic is typically outbound one-way traffic – from operations to the rest of the enterprise. This traffic could be

handled via events, via the bus connector, or via SQL Server Integration Services (SSIS) Extract, Transform and Load (ETL) integration, depending upon the form and volume of the data. In any of these cases, it is important to establish information architecture with well-defined data mastership so that a single version of the truth is maintained. Please refer to section 3.5.5 on the need to isolate the network operation center bus from the enterprise bus for security/performance reasons.

The reference architecture diagram reflects a single event bus enterprise wide. This bus is intended to be the single point for event subscribers. This implementation precludes the need to jump through the hoops to subscribe to multiple busses.

In practicality, implicit in the reference architecture is filtering and message distribution, both at the StreamInsight CEP stream management level, and at the operations to enterprise CIM message bus interconnect, to ensure appropriate distribution of events. The event handling strategy should be established enterprise wide to ensure subscribers need only connect to one bus, and that duplicate events are not distributed.

When events are driven from special purpose distributed control systems (DCS) applications, they may be passed along to a StreamInsight Complex Event Processing engine.

CIM provides an information model that should be the basis for utility message definitions and for master data. In practice, extensions to the CIM are necessary in most deployments. A key to successful integration will be the master data strategy. Microsoft M modeling, the M model repository, and the new Master Data Services (the Stratature product Microsoft purchased being released in SQL Server 2008 R2 release) can be leveraged to establish an enterprise-wide master data architecture.

4.2.2 Data Integration Architecture

A data integration architecture should be developed in concert with the master data strategy.

Data integration is fundamental to enabling deep analysis to drive business intelligence. Realistically, all the potential uses for integrated data in the smart energy ecosystem cannot be foreseen today.

For example, analysis of customer behavior in response to variable pricing programs may result in the need for data from the financial system, the meter data management system and distribution operations.

Therefore the new scenarios necessitate a data integration architecture that will enable these data consolidations, with these considerations:

- **Performance, ease of access, and security considerations** should drive the tradeoff between replication and an OLAP integration architecture.
- **De-normalized cube design** can ease reporting and analysis.

- Serious consideration should be given to building a **CIM-based unified data model using OLAP access**, rather than constructing an all-encompassing data warehouse. The latter poses serious maintenance and update issues.

The reference architecture diagram, Figure 38, shows an ETL pipe from operations data stores to enterprise data stores. In practice, this is typically implemented as one-way data integration, for supplying operational data to the rest of the enterprise.

The following considerations should be taken into account for the design of the data integration architecture:

- The primary objective is establishing **data mastership**, whether in the operations system or in other enterprise systems. A good example of such data mastership is the decision that the GIS/asset management system should be the data source for all distribution field equipment model updates.
- **Meter data** to support billing.
- **Operations data** such as breaker switching to drive condition based maintenance, etc.
- **Non-time series** will be hosted in the native operational data warehouse or accessed through SQL UDM. Data replication and creating additional DWs is not advised, but rather accessed from a Unified Cube SSAS.
- **Non-critical event data** will be passed along to an Events DW for trending, or modeling with special purpose modeling applications. Higher priority "events" will be passed through WF to Microsoft® Office SharePoint® for notification leveraging MOSS dashboard services such as Excel, Real Time OSIsoft Webparts, or Rich Client UX such as SilverLight or WPF.

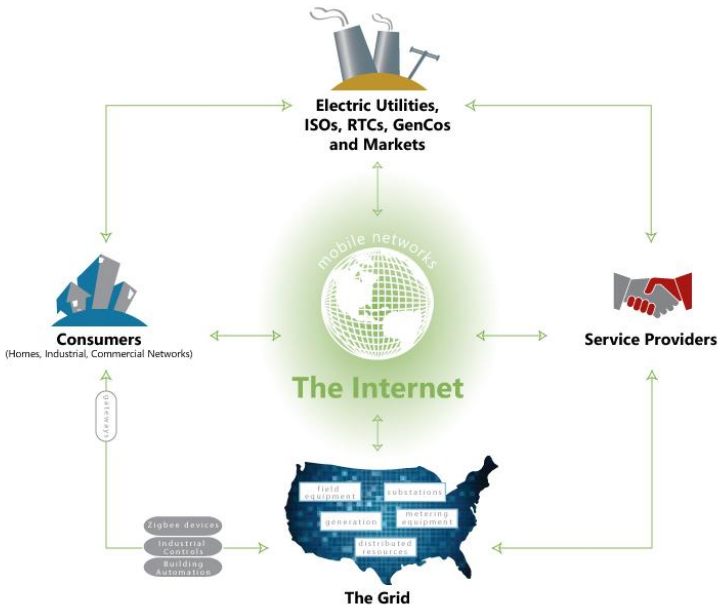

Figure 38 - Microsoft Smart Energy Ecosystem Reference Architecture

4.3 Collaboration Services

As previously described, the smart energy ecosystem will thrive if collaboration is adopted as a key tenet of its operation. Customers are becoming active participants in this new energy environment, creating the emergence of a wide range of new service providers. Many new services are already being provided using the software as a service (SaaS) model.

To further enable this dynamic, Microsoft offers some key technologies that provide a collaboration infrastructure, featuring:

- Azure, which focuses on supporting collaboration using cloud-based services, and
- SharePoint, which focuses on user collaboration.

4.3.1 Azure Services Platform

While Azure is technically an operating system in the cloud, and Azure Services Platform is technically a cloud computing environment, the reference architecture advises leveraging the new Microsoft Azure Services as a key enabler for cross enterprise process integration, data exchange and cloud-based collaboration.

The Azure Service Platform is an Internet-scale cloud services platform that is hosted by Microsoft data centers. The platform is central to the Microsoft software plus services(S+S) approach to providing rich computing environments, whether hosted on-premise or in a Microsoft data center. The S+S approach provides choice and flexibility in the development, operation, migration and management of applications, whether they exist on the Internet, or are hosted locally. Figure 39 illustrates the Azure Services Platform capabilities:

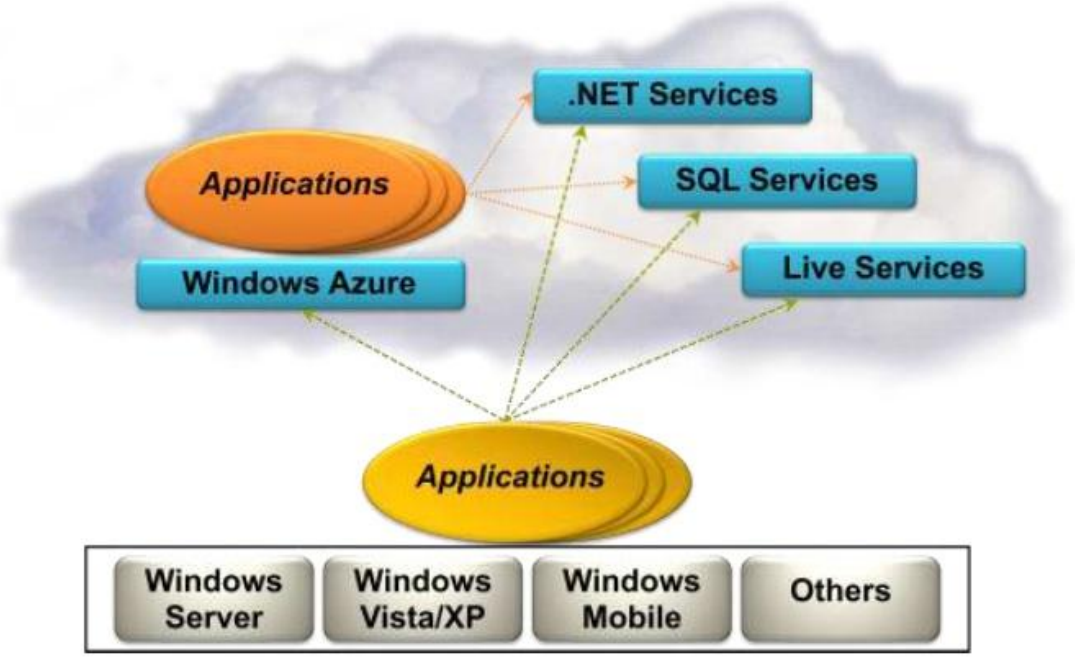

Figure 39 - Azure Service Platform Capabilities

The Azure Services Platform can be used to implement new applications or enhance existing applications, where applications can run in the cloud or on local systems. Components within the Azure Services Platform include:

- Windows Azure operating system that runs in the Cloud using Microsoft data centers
- Applications and services that run in the cloud on Windows Azure
- A service bus, part of .NET Services that provides a secure, standards-based messaging infrastructure
- Other cloud services, including .NET Services beyond the Service Bus, SQL Services and Live Services
- Local (on-premise) systems that may use operating systems such as Windows Server®, Windows Vista®, Windows XP, Windows Mobile®, and other non-Microsoft operating systems
- Applications that run on local systems that interact with Windows Azure and the other cloud services

Azure applications and services are developed using the .NET Framework, supporting a variety of managed code programming languages. Azure provides for standards-based interoperability using HTTP, SOAP, REST, PHP and XML.

Figure 40 illustrates an Azure Service configuration:

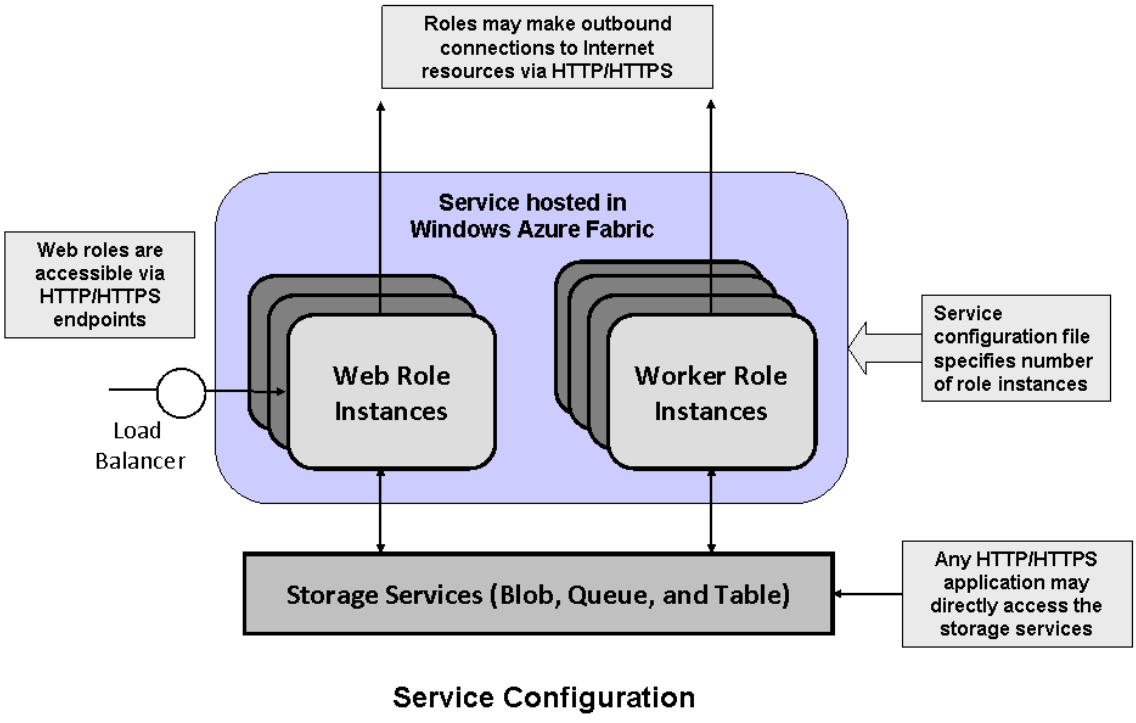

Figure 40 - Azure Services Platform (Source: David Chappell & Associates)

4.3.2 Microsoft Office SharePoint Server

Microsoft also enables collaboration through Microsoft Office SharePoint Server 2007, where the focus is collaboration between users and access to enterprise information resources.

Office SharePoint Sever 2007 is an integrated suite of capabilities that can help improve operational effectiveness.

Figure 41 - SharePoint Platform Services

SharePoint Server provides the following key capabilities:

- Team collaboration, where teams can work together, collaborate on and publish documents, maintain task lists, implement workflows and share information through the use of wikis and blogs
- Portals, where users can be connected to business critical resources
- Enterprise content management (ECM)
- Enterprise search, which can leverage a variety of repositories and formats
- Business process and forms, where workflow templates can be used to automate approval, review and archiving processes
- Business intelligence, where dashboards and reports can provide up to date information, improving insight and helping to improve decisions
- Web content management, where the goal is to put Web publishing into the hands of business users
- Social computing, where the goal is often to improve communication within a user community

SharePoint provides an ideal solution to the problem of content management for support of compliance and compliance reporting. There are also many examples where SharePoint is

currently used to support collaboration by teams, especially in those situations where an organization may have many subject areas of interest, each with corresponding interest groups, and given users may participate in a subset of those groups.

One example would be for an enterprise architecture, where architects might collaborate to define different aspects of the architecture. The specifications often take the form of Microsoft Office documents, UML and design artifacts. Developers might then have read-only access to the architecture, and thus be able to raise concerns. The developers may also have different subject areas related to software designs and the posting of design artifacts for sharing with other groups.

One notable user of SharePoint is the UCA International Users Group, which is the parent users group for many smart grid related efforts including IEC TC57 standards working groups.

The following customer-facing Web pages offer several examples of the use of SharePoint:

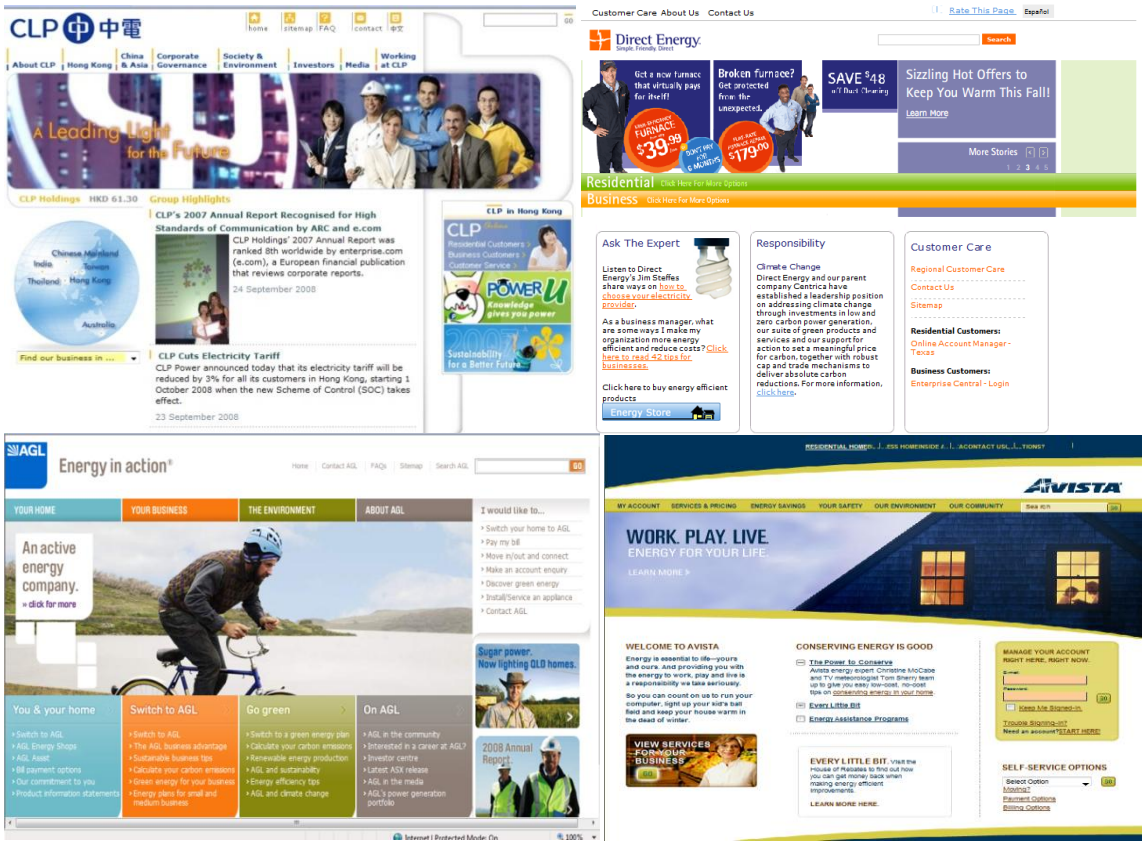

Figure 42 - Microsoft SharePoint based Customer Facing Web Portals

The reference architecture recommends Microsoft Office SharePoint Server as a core capability for information distribution – both internal and external to an organization. Security, RBAC, IRM, workflows, and a rich set of tools for construction and distribution of enterprise content make SharePoint a core element in the reference architecture.

4.4 Process Integration

Process integration refers to the integration of processes within an organization as well as integration of processes that may span multiple organizations.

The Microsoft SERA recognizes the following scenarios for process integration:

- Process integration is entirely with an organization
- Process integration may involve B2B data links to other organizations
- Process integration may involve many devices inside and outside any enterprise
- Process integration may involve the use of cloud services
- Process integration is multi-organization, where cloud-based messaging and orchestration are needed

In order to enable process integration, these varied scenarios translate to the need for:

- An enterprise service bus, for on-premise integration
- An inter-enterprise service bus, for B2B or multi-organization integration
- An extra-enterprise service bus, for integration that may involve devices or customers.

Where the 'intra' enterprise role of the ESB can be served by BizTalk Server, the needs of 'inter' and 'extra' enterprise integration can be served by the Internet-based Azure .NET Service Bus. Figure 43 illustrates such an architecture, where on-premise ESBs, clients and other services can be integrated using the service bus.

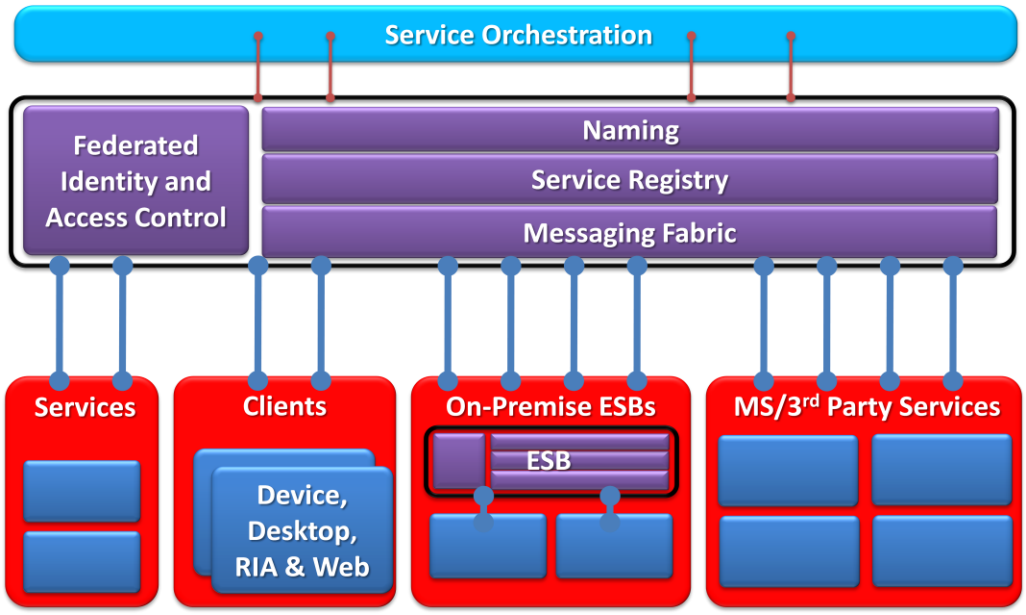

Figure 43 - Service Bus Integration

4.4.1 Service Bus

As shown in Figure 44 below, the Microsoft .NET Service Bus is a part of the Azure Services Platform. It provides a secure, standards-based messaging fabric to securely connect applications across the Internet.

The reference architecture recognizes that the emergence of new players in the smart energy ecosystem, new devices and new business models will lead to implementations that employ Internet-based application message exchange as an effective integration solution. The .NET service bus relies on the .NET Access Control Service for controlling access to solutions through a claims-based security model. The naming system on the service bus allows endpoints to be uniquely identified using host independent, hierarchical URIs. The service bus registry is used for publication and discovery of service endpoint references within a solution.

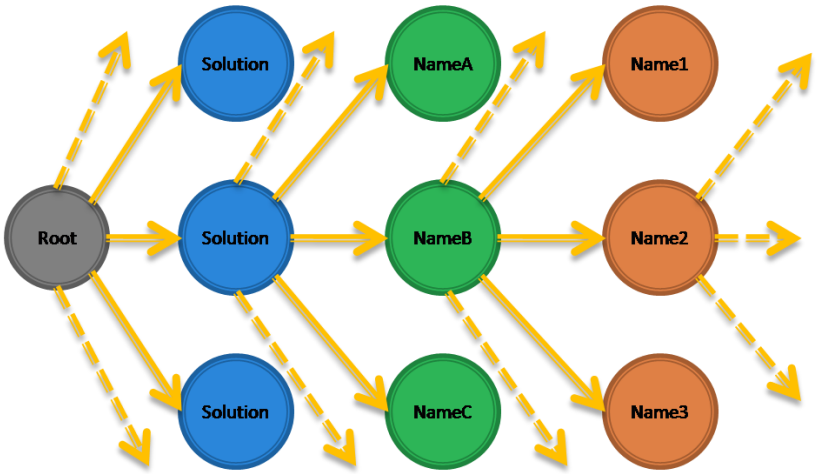

Figure 44 - .NET Service Bus Naming System

The primary programming model on the service bus is the Windows Communication Foundation (WCF). Connections are created using TCP or HTTP. The messaging fabric within Service Bus supports standard protocols including those defined by Web service specifications and REST, as well as access from non-.NET platforms.

Figure 45 illustrates the secure publish/subscribe messaging provided by service bus, using both unicast and multicast protocols.

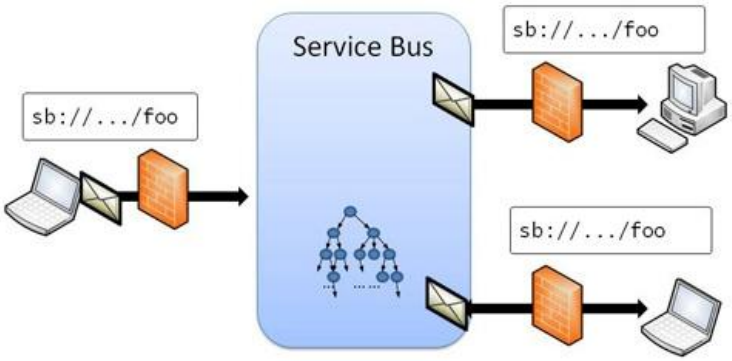

Figure 45 - Publish/Subscribe through Service Bus

Figure 46 shows that connections between processes can be either relayed by the service bus, or direct between the processes. A hybrid connection model lets this be negotiated once the initial connection is made through the service bus.

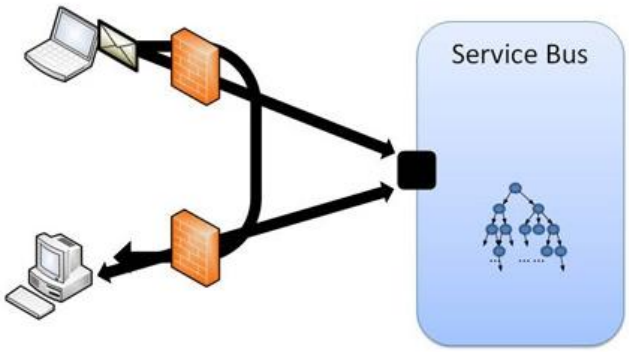

Figure 46 - Connections through Service Bus

The Microsoft .NET Workflow Service is another one of the core service offerings found within the Azure .NET Services. The .NET Workflow Service supports cloud-based workflows that model service interactions through the .NET Service Bus and HTTP messaging. This service extends Windows Workflow Foundation (WF) to the cloud.

4.4.2 BizTalk Server

BizTalk Server is Microsoft's offering for process integration as it provides the means to seamlessly connect systems within and across organizations.

BizTalk includes more than 25 multi-platform adapters and a robust messaging infrastructure. In addition to integration functionality, BizTalk provides:

- Strong durable messaging designed to never lose messages
- A rules engine BRE
- EDI connectivity
- Business activity monitoring (BAM)

- RFID device management and event based communication
- ESB guidance

BizTalk is a mature product – the latest version is BizTalk Server 2009. BizTalk Server 2009 allows organizations[23] to:

- Simplify and automate interoperability to reduce costs and errors
- Gain critical insights on business processes and performance
- Shield processes from change impacts
- Promote agility and manageability
- Integrate to eliminate redundancy
- Automate business interactions with partners

Figure 47 describes the basic message flow within BizTalk Server:

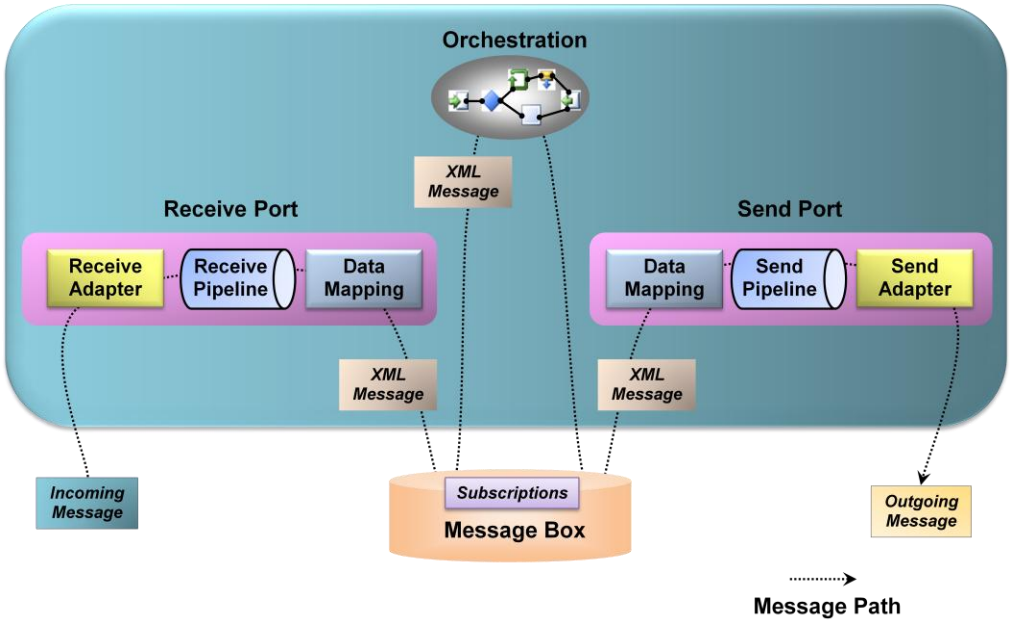

Figure 47 - BizTalk Basic Message Flow (Source: Chappell & Associates)

Figure 47 illustrates that once a message from a source is received by an adapter of a receive port, a message may be validated and converted into an internal format for delivery to the message box. Once delivered to the message box, the message may be read by an orchestration. As the result of an orchestration, another message may be produced and be delivered to the message box. Using subscriptions, messages from the message box are delivered to a send port, where they may be transformed and delivered to a target. An example of this would be for meter readings, where a legacy metering system may be able to provide data using MultiSpeak

[23] A whitepaper is available that provides an introduction to BizTalk Server 2009.

or MV90 formats, but the target system may need the data to be transformed to an IEC 61968-9 format.

Figure 48 provides a broader view of business process management:

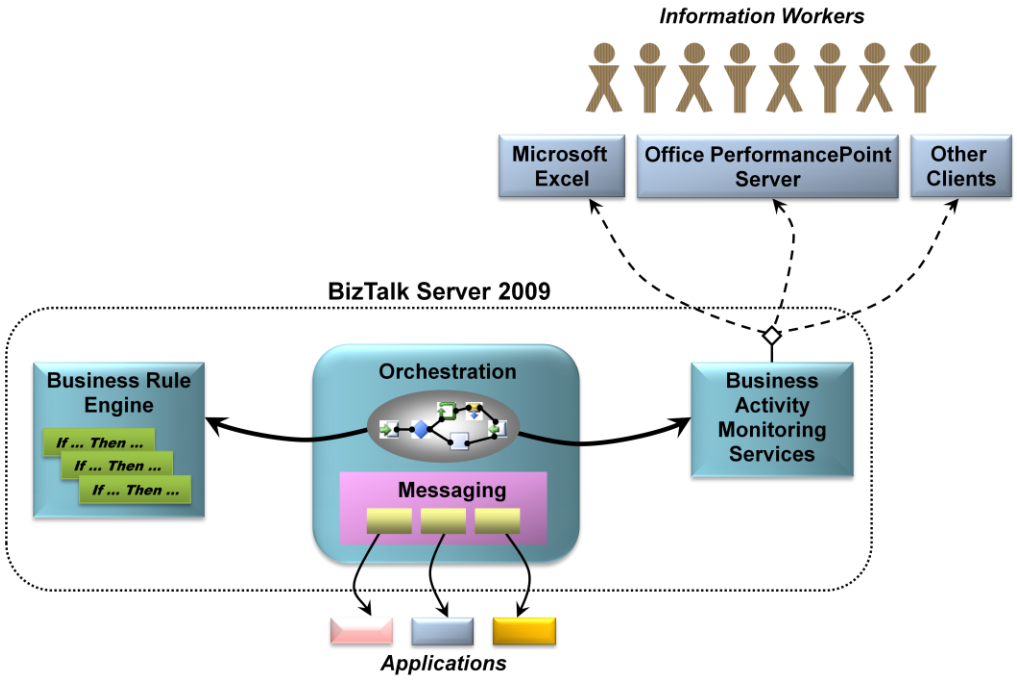

Figure 48 - Business Process Management (Source: Chappell & Associates)

Figure 48 demonstrates how the BizTalk orchestrations can leverage business rule engine (BRE) and business activity monitoring (BAM) services. Information posted to BAM services can be accessed by users through tools such as Excel and Office SharePoint Server BI, as well as other application components. Windows Communication Foundation (WCF) and Windows Workflow Foundation (WF) can be used to develop applications that can access BAM data.

In an even broader context, BizTalk Server can be used for business to business (B2B) integration, as shown in Figure 49:

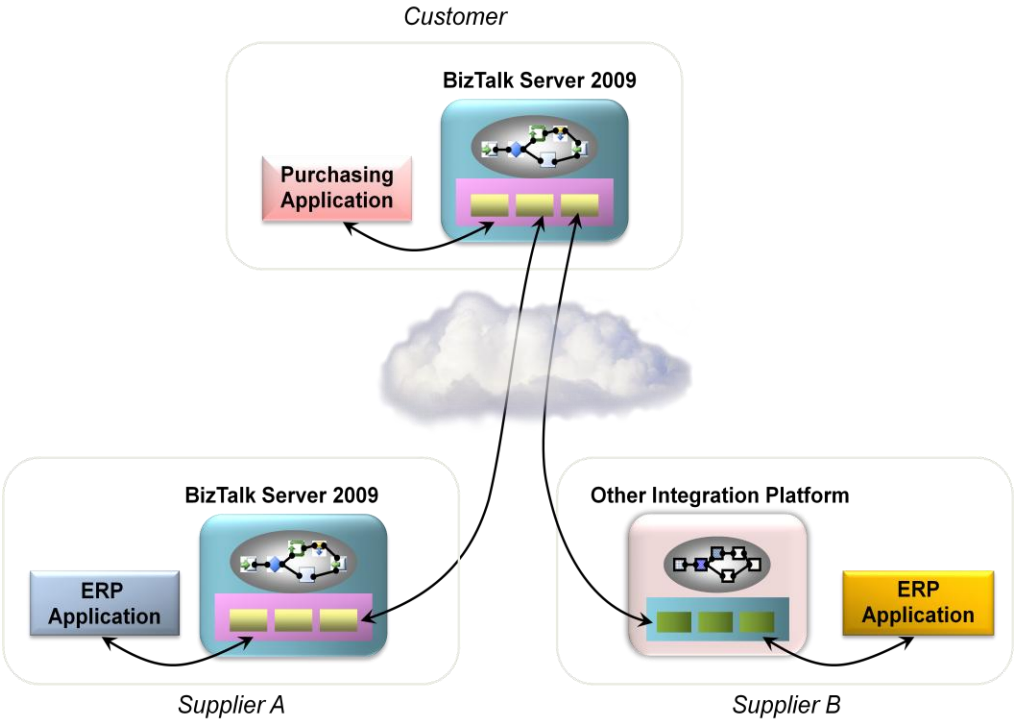

Figure 49 - Business-to-Business Integration Using BizTalk Server (Source: Chappell & Associates)

This shows that, when a business process spans multiple organizations, orchestration can manage communication between multiple systems – the ones internal and external to the organization. That orchestration means the flow of tasks creating a seamless experience for very distributed processes. These capabilities are commonly needed in energy markets and procurement as well as for integration between utilities and service providers. The registration and management of demand response programs is one example of this, where service providers identify, register and manage resource participation demand response programs that are managed by a utility or ISO.

4.5 Databases and Data Warehouses

Microsoft SQL Server is a database management and analysis system that is well suited to provide the needs related to databases which may be implemented as data warehouses, data marts, production databases and operational data stores within the smart energy ecosystem.

All of these capabilities are notable because the information management needs within the smart energy ecosystem will continue to grow in breadth, depth, granularity and usage.

Beyond those basic uses, SQL Server also provides the foundation for the Microsoft business intelligence platform and serves as a key integration component.

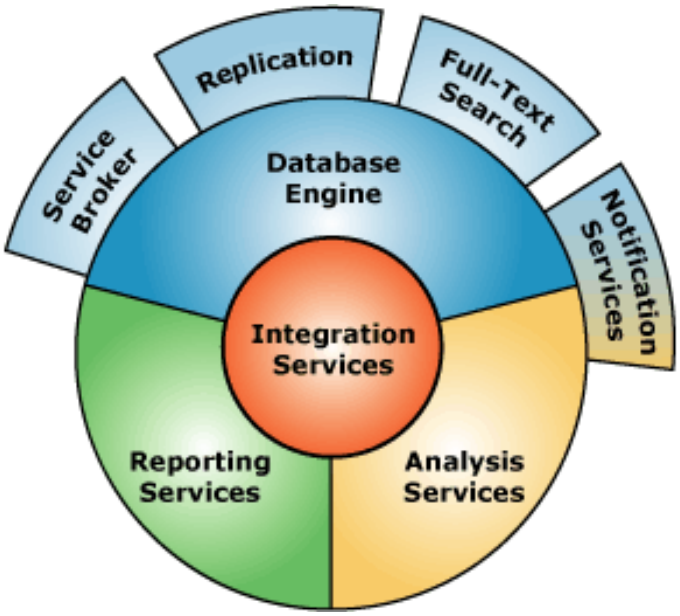

Figure 50 - SQL Server 2008 Key Components

Within SQL Server 2008, the key components include:

- Relational database engine
- Management Studio
- Analysis services
- Integration services
- Replication
- Reporting Services
- Service Broker

SQL Server is built around a core SQL-compliant database engine that addresses the persistence, access, security, processing and transactional needs for the wide range of applications that exist within the smart energy ecosystem. SQL Server is optimized for both online transactional processing (OLTP) and online analytical processing (OLAP). The SQL Server Management Studio provides the capabilities needed to create, edit and manage database objects in a graphical environment.

The analysis services within SQL Server directly address the specific needs of multidimensional data and data mining. These services provide the ability to design, create and manage multidimensional structures that contain information aggregated from multiple data sources, as needed primarily for the implementation of data warehouses and data marts. Also provided are features and tools needed for data mining, such as industry-standard data mining algorithms, support for data mining models and support for complex prediction queries.

The SQL Server Integration Services (SSIS) is a platform for building enterprise-level data integration and data transformation solutions. These services provide a rich and robust set of capabilities

needed for the extract, transform and load (ETL) integration patterns as described in the Reference Architecture as used to populate a data warehouse.

The replication mechanisms provided by SQL Server address key needs related to availability and scalability. Within the smart energy ecosystem, replication is typically employed for purposes of availability, disaster recovery and scalability. For availability, data can be replicated from a master instance to backup instances located remotely at sites serving as backups for network operations centers. In the case of scalability, data from a SQL Server instance (e.g. a data warehouse or data mart) can be replicated to a number of instances so that query workload can be load balanced across multiple instances.

The reporting services in SQL Server provide a wide range of tools and services for the creation, deployment and management of reports.

4.6 Business Intelligence

Business intelligence (BI) is the use of technologies to help organizations make better decisions.

These benefits are usually realized through consolidating, aggregating and analyzing data. The focus of BI and SOA are sometimes seen as being in conflict, where the data needed for BI is often scattered between services and hidden behind contracts.

As a result, Microsoft's BI solution takes a pragmatic approach to data access and leverages many different alternatives to aggregate data, as well as easy solutions to get data from a variety of applications and products so that access to key performance data does not compromise the SOA.

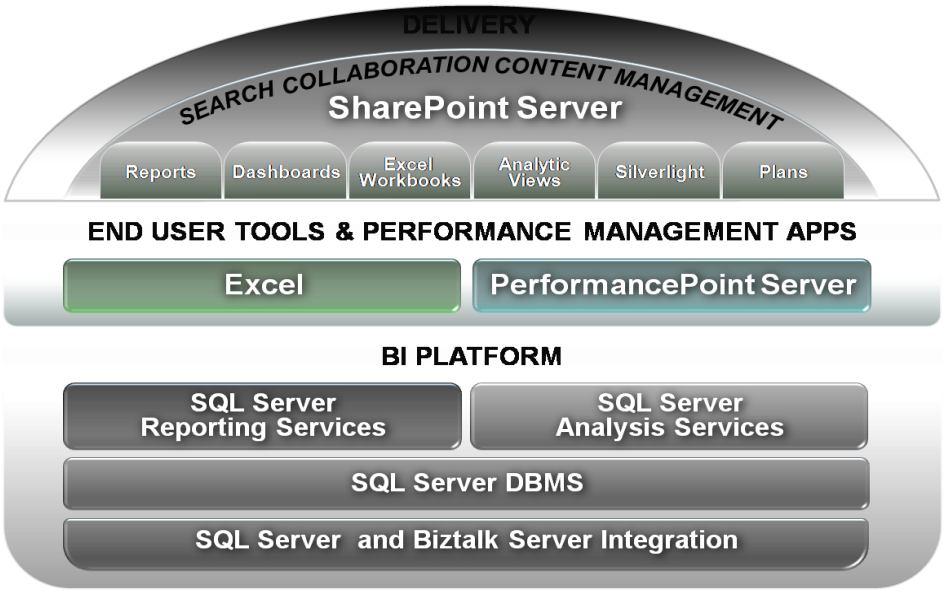

Figure 51 - SQL Server and Business Intelligence

Business intelligence is supported using the following Microsoft products:

- Office Excel Services
- SharePoint Server Business Intelligence, which provides functionality needed for performance management including scorecards, dashboards, management reporting, analytics, planning, budgeting, forecasting, and consolidation.
- SQL Server DBMS
- SQL Server Reporting Services
- SQL Server Analysis Services (SSAS), with Data Mining and Data Warehousing capabilities
- SQL Server Integration Services (SSIS), which provides ETL, aggregation and calculation capabilities
- BizTalk Server

4.7 Complex Event Processing

Complex event processing (CEP) solution can be implemented and configured using a variety of Microsoft and third party products. The Microsoft CEP platform is built upon SQL Server 2008 and allows software developers to create complex and innovative CEP solutions along two scenarios:

1. Building packaged event-driven applications for low latency processing
2. Developing custom event-driven applications for business and the Web with high throughput, low latency needs

The SERA recognizes the need to a high performance event handling service at the "edge" of the smart energy ecosystem computing environment.

Figure 52 shows a diagram of the Microsoft StreamInsight CEP engine:

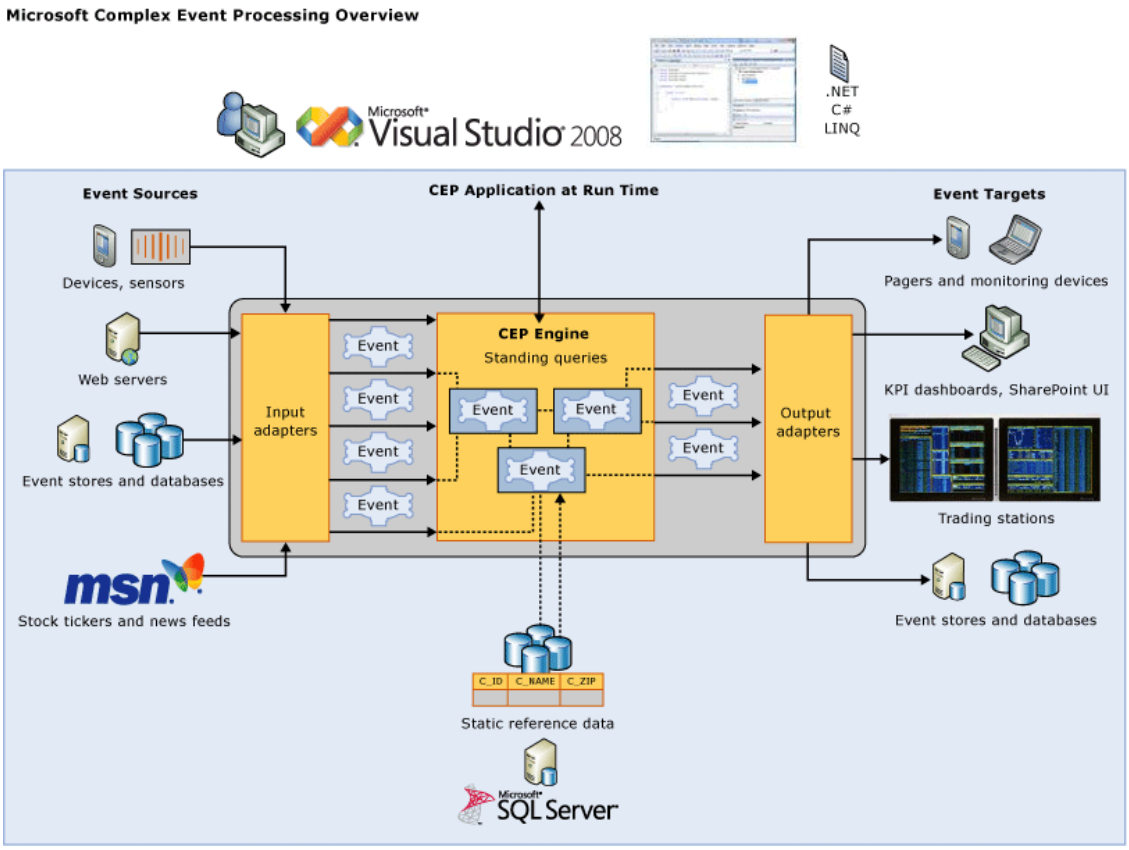

Figure 52 - Microsoft CEP Platform

StreamInsight has demonstrated performance exceeding 100K events/second. This enables the following important capabilities for the reference architecture:

- Unpack message streams and identify state changes over time
- Process real-time events
- Analyze event streams and create composite events
- Filter event streams and route events
- Invoke Web services and trigger business process

4.8 Mobility

Mobile devices are becoming increasingly important to utilities, service providers and customers as they are being used for an increasingly wider range of uses:

- Mobile technologies help reduce the time it takes to perform time-intensive and repetitive tasks, like equipment installation and repair, crew management and redeployment, meter reading, outage identification and repair.
- Mobile solutions enable collaboration through the sharing of data that has been historically unavailable in the field, such as drawings, schematics, blueprints and equipment repair

records. The availability of solutions to help field worker collaboration with improved information transfer will ease the impacts of the aging workforce phenomenon and also help to significantly reduce time to repair thereby reducing customer downtime and improving customer satisfaction.

Microsoft provides technologies that significantly accelerate deployment and management, whether the target platform is embedded, mobile or PC:

- Microsoft provides the Windows Mobile platform for the development of mobile devices.
- Visual Studio and the Windows Mobile Software Development Kit (SDK) make it possible to develop both native C++ applications and C# or VB managed code applications for mobile devices.[24]
- The managed languages in particular have extensive support for database access and for the .NET Compact Framework. The .NET Compact Framework is a subset of the .NET Framework, but it does afford a developer the ability to work in essentially the same development environment and tools.
- Applications that have been designed to use a relational data store can leverage the Microsoft SQL Server CE compact relational database that runs on smart devices.

4.9 Management and Security

This section describes the Microsoft products that support management and security needs.

In Figure 53, where the problem space has many layers, each of the products described addresses one or more layers of the problem.

[24] A brief note on terminology: Microsoft now calls devices with integrated phone and touch screen Windows Mobile Professional devices, and devices without a touch screen Windows Mobile Standard devices. Developers should ensure they have the correct SDK for their target mobility application.

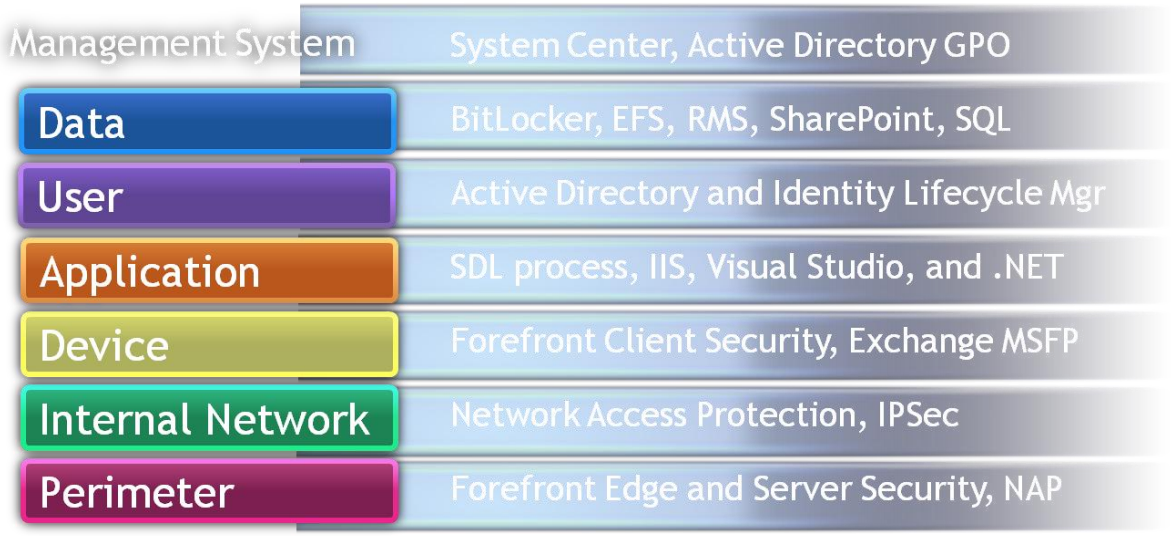

Figure 53 - Management and Security Layers

The combined products work toward the "end-to-end trust" vision, which enables a comprehensive approach to the entire scope of security for the smart energy ecosystem.

4.10 System Center

System Center solutions help information technology (IT) pros manage the physical and virtual IT environments across data centers, client computers and devices. Using these integrated and automated management solutions, IT organizations can be more productive service providers to their businesses.

Microsoft® System Center solutions play a central role in Microsoft's vision for helping IT organizations benefit from self-managing, dynamic systems. System Center solutions capture and aggregate knowledge about the infrastructure, policies, processes and best practices so that IT professionals can optimize IT structures to reduce costs, improve application availability and enhance service delivery.

In the smart energy ecosystem, System Center can take on much of the burden for management of devices as the devices scale out and the demands for more active configuration management emerge. For example, implementing MOM (Microsoft Operations Manager) packs or equivalent device status services can enable a comprehensive view of all the utility assets in a single tool. The captured asset information provides a foundation for insights driving condition based monitoring and for dynamic asset configuration management.

By aiming to enable self-managing, dynamic systems, System Center solutions close the gap between development, operations and IT—connecting people, processes and tools—by evaluating dependencies and optimizing business process performance from deep inside the operating system, applications, and composite services and workflows.

System Center Configuration Manager comprehensively assesses, deploys, and updates servers, client computers, and devices—across physical, virtual, distributed, and mobile environments. Optimized for Windows and extensible, it is the best choice for gaining enhanced insight into, and control over, IT systems. Tools provided by the Configuration Manager include:

- Asset Intelligence
- Software Update Management
- Desired Configuration Management
- Software Distribution
- Operating Systems Deployment

System Center Operations Manager is the end-to-end service-management product that is the best choice for Windows because it works seamlessly with Microsoft software and applications, helping organizations increase efficiency while enabling greater control of the IT environment. Microsoft and Microsoft Partners provide a wide variety of management packs.

Microsoft also provides an IT Compliance Management Guide that shows how to shift governance, risk and compliance (GRC) efforts from people to technology. Its configuration guidance can be used to help efficiently address your organization's GRC objectives. This accelerator helps the utility better understand how an IT process framework can help you implement GRC controls in your Microsoft infrastructure.

Microsoft also provides a case study related to streamlining regulatory compliance. Microsoft information technology (Microsoft IT which manages all IT for the company) uses a holistic approach to address the ever-increasing complexity of regulatory compliance. This continually evolving system combines IT support for different regulatory frameworks into a single overarching process, and uses standardized tools to test similar controls. By combining tools and using a clearly defined role-based accountability model, Microsoft IT streamlines business processes, reduces duplication of effort, and makes IT professionals more operationally efficient.

4.11 End to End Trust

End to End Trust is Microsoft's vision for a safer, more trusted Internet – a vision that should extend to the network at the heart of the smart energy ecosystem.

There are three primary elements to creating greater trust on the Internet:

1. **Creation of a trusted stack** where security is rooted in hardware and where each element in the stack (hardware, software, data and people) can be authenticated in appropriate circumstances.
2. **Managing claims relating to identity attributes**, with the creation of a system that allows people to pass identity claims (sometimes a full name perhaps, but at other times just an

attribute such as proof of age or citizenship). This system must also address the issues of authentication, authorization, access and audit.

3. **Good alignment of technological, social, political and economic forces** so that there is real progress towards a safer, more trusted Internet. The goal is to put users in control of their computing environments, increasing security and privacy, and preserving other cherished values such as anonymity and freedom of speech.

The SERA therefore recommends the following practices for security implementation:

- Encrypt data at rest
- Encrypt and sign communications
- Sign all service implementations
- Encrypt and wrap data in motion with transport layer security (TLS)
- Minimize storage and mapping of personally identifiable information (PII)
- Leverage the SDL for all software and services

4.11.1 Rights Management Services

Microsoft Active Directory Rights Management Services (AD RMS) in Windows Server 2008 helps safeguard digital information from unauthorized use—both online and offline, inside and outside of the firewall. In conjunction with AD RMS–enabled applications, AD RMS augments an organization's security strategy by protecting information through persistent usage policies. These policies remain with the information—whether documents, spreadsheets, presentations, or e-mail messages—no matter where it goes or how it is stored.

- Eliminate unauthorized viewing and distribution of sensitive corporate data.
- Improve compliance with internal and external regulations by lowering the risk of data leaks.
- Reduce the risk of intellectual property loss, which can result in a compromised ability to compete.

4.11.2 BitLocker

Windows BitLocker™ Drive Encryption (BitLocker) is a security feature in the Windows Vista, Windows Server 2008 and Windows® 7 operating systems that can provide protection for the operating system on your computer and data stored on the operating system volume.

In Windows Server 2008, BitLocker protection can be extended to volumes used for data storage as well.

BitLocker performs two functions:

- Encrypts all data stored on the Windows operating system volume (and configured data volumes). This includes the Windows operating system, hibernation and paging files, applications, and data used by applications.

- Is configured by default to use a trusted platform module (TPM) to help ensure the integrity of early startup components (those used in the earlier stages of the startup process), and "locks" any BitLocker-protected volumes so that they remain protected even if the computer is tampered with when the operating system is not running.

4.11.3 Active Directory Domain Services

Active Directory Domain Services (ADDS), formerly known as Active Directory Services, is the central location for configuration information, authentication requests and information about all of the objects that are stored within your forest.

Using Active Directory, you can efficiently manage users, computers, groups, printers, applications and other directory-enabled objects from one secure, centralized location.

As more and more devices are added to the smart energy ecosystem, efficient management of the devices will be a necessity or security will be compromised due to the sheer complexity of ongoing management.

- Auditing. Changes made to Active Directory (AD) objects can be recorded so that you know what was changed on the object, as well as the previous and current values for the changed attributes.
- Fine-Grained Passwords. Password policies can be configured for distinct groups within the domain. No longer does every account have to use the same password policy within the domain.
- Read-Only Domain Controller. A domain controller with a read-only version of the Active Directory database can be deployed in environments where the security of the domain controller cannot be guaranteed, such as branch offices where the physical security of the domain controller is in question, or domain controllers that host additional roles, requiring other users to log on and maintain the server. The use of Read-Only Domain Controllers (RODCs) prevents changes made at branch locations from potentially polluting or corrupting your AD forest via replication. RODCs also eliminate the need to use a staging site for branch office domain controllers, or to send installation media and a domain administrator to the branch location.

In addition to ADDS, Active Directory Federation Services (ADFS) can be used to manage the secure sharing of identity information between trusted business partners via federation across an extranet.

4.11.4 Identity Lifecycle Manager

Microsoft Identity Lifecycle Manager (ILM) 2007 provides an integrated and comprehensive solution for managing the entire lifecycle of user identities and their associated credentials. It provides identity synchronization, certificate and password management, and user provisioning

in a single solution that works across Microsoft Windows and other organizational systems. As a result, IT organizations can define and automate the processes used to manage identities from creation to retirement. ILM provides the following benefits:

- Boosts efficiency by integrating with existing infrastructures to automate and centralize identity lifecycle processes and tools that were historically disparate and manual.
- Improves operational efficiency by gaining a single view of a user across multiple systems.
- Incorporates strong authentication tools seamlessly with end-to-end lifecycle management of smart cards and digital certificates.
- Reduces integration and customization costs by providing a single foundation for all core identity lifecycle management.
- Improves security and compliance with the ability to enforce and track identities across the enterprise.
- Reduces help desk costs by providing people with self-help tools to manage routine tasks, such as changing passwords or resetting smart card PINs.

4.11.5 Secure Development Lifecycle

Software vendors must also endeavor to address security threats or risk becoming the weak link targeted for attack.

Microsoft works closely with its partners to identify and develop domain specific solutions. This close working relationship represents great value for customers by leveraging the Microsoft platform.

All software, including partner solutions, should embrace a Secure Development Lifecycle to meet the security and reliability expectations for the Smart Energy Ecosystem.

Security is a core requirement for software vendors because they are driven by market forces, including the need to protect critical infrastructures and to build and preserve widespread trust in computing. All software vendors face the major challenge of creating more secure software that requires less updating through patches and less burdensome security management.

For the software industry, the key to meeting today's demand for improved security is to implement repeatable processes that reliably deliver measurably improved security. Therefore, software vendors must transition to a more stringent software development process that focuses, to a greater extent, on security. Such a process is intended to minimize the number of security vulnerabilities extant in the design, coding, and documentation and to detect and remove those vulnerabilities as early in the development lifecycle process as possible. The need for such a process is greatest for enterprise and consumer software that is likely to be used:

- To process inputs received from the Internet
- To control critical systems likely to be attacked

- To process personally identifiable information

Microsoft's experience with making real-world software secure has led to a set of high-level principles for this process. The overall security perspective reflects Microsoft's end-to-end trust vision for a safer Internet.

Microsoft refers to these high-level real world principles as SD^3+C, which signifies "Secure by Design, Secure by Default, Secure in Deployment, and Communications." These principles are part of the Microsoft Security Development Lifecycle (SDL) and are defined as follows:

- **Secure by Design**: the software should be architected, designed, and implemented so as to protect itself and the information it processes, and to resist attacks.
- **Secure by Default**: in the real world, software will not achieve perfect security, so designers should assume that security flaws would be present. To minimize the harm that occurs when attackers target these remaining flaws, software's default state should promote security. For example, software should run with the least necessary privilege, and services and features that are not widely needed should be disabled by default or accessible only to a small population of users.
- **Secure in Deployment**: Tools and guidance should accompany software to help end users and/or administrators use it securely. Additionally, updates should be easy to deploy.
- **Communications**: software developers should be prepared for the discovery of product vulnerabilities and should communicate openly and responsibly with end users and/or administrators to help them take protective action (such as patching or deploying workarounds).

Figure 54 - Microsoft Security Development Lifecycle

While each element of SD^3+C imposes requirements on the development process, the first two elements—secure by design and secure by default—provide the most security benefit. Secure by design mandates processes intended to prevent the introduction of vulnerabilities in the first place, while secure by default requires that the default exposure of the software—its "attack surface" be minimized.

The SDL Optimization Model shown in Figure 55 has been designed to facilitate gradual, consistent and cost-effective implementation of the SDL and reduce customer risk.

Figure 55 - SDL Optimization Model

The SDL Optimization Model is structured around five capability areas that roughly correspond to the phases within the software development lifecycle:

1. Training, policy, and organizational capabilities
2. Requirements and design
3. Implementation
4. Verification
5. Release and response

4.11.6 Device Security

Microsoft Forefront delivers end-to-end security and access to information through an integrated line of protection, access and identity management products.

Forefront Security products deliver protection, access, and management solutions, built around user identity and integrated with a highly secure, interoperable platform. Our solutions help to deliver a more contextual and user-centric security solution aligned to the needs of our customers.

Microsoft is working to achieve the goal of business ready security based on three fundamental tenets:

1. **Integrate and extend across the enterprise**
   - Deeply integrates with the identity infrastructure and across the stack
   - Support for heterogeneous environments
   - On-premises and hosted solutions for seamless connectivity
   - Open standards and protocols based identity and security platform

2. **Help protect everywhere, access anywhere**
   - Defense in-depth across multiple layers to help protect across endpoints, servers and network
   - Secure identity-based access products help connect the mobile workforce virtually anywhere

- Identity-aware protection help organizations secure information and enable policy-based access

3. **Simplify the experience, manage compliance**

- Enable centralized management of the environment and gain critical visibility into the state of the infrastructure
- Help improve security and compliance through identity tracking and enforcement throughout the enterprise
- Provide policy management features and reporting to enable auditing and compliance

4.11.7 Network Access Protection

Network Access Protection (NAP) is a policy enforcement platform built into the Windows Vista, Windows 7, and Windows Server 2008 operating systems.

NAP is an extension to Internet Protocol Security (IPsec)[25] primarily for use with mobile computing devices that helps administrators more effectively protect network assets by helping to enforce compliance with system health requirements. IT administrators can create customized health policies with NAP to validate computer security posture before allowing access or communication, automatically update compliant computers to enable ongoing compliance, and optionally confine noncompliant computers to a restricted network until they become compliant.

In terms of the smart energy ecosystem, this capability can be applied to help ensure new grid connected devices conform to the appropriate policies, or restrict their access, thus adding to the overall ecosystem security.

NAP includes an application programming interface (API) set for developers and vendors to create complete solutions for health policy validation, network access limitation, and ongoing health compliance. To validate access to a network based on system health, NAP provides the following areas of functionality:

- **Health policy validation** determines whether the computers are compliant with health policy requirements.
- **Network access limitation** limits access for noncompliant computers.

[25] **Internet Protocol Security** (**IPsec**) is a protocol suite for securing Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a data stream. IPsec also includes protocols for establishing mutual authentication between agents at the beginning of the session and negotiation of cryptographic keys to be used during the session. IPsec can be used to protect data flows between a pair of hosts (e.g. computer users or servers), between a pair of security gateways (e.g. routers or firewalls), or between a security gateway and a host. Wikipedia.org

- **Automatic remediation** provides necessary updates to allow a noncompliant computer to become compliant.
- **Ongoing compliance** automatically updates compliant computers so that they adhere to ongoing changes in health policy requirements.

4.11.8 IPsec

Internet Protocol security (IPsec) is a framework of open standards for protecting communications over Internet Protocol (IP) networks through the use of cryptographic security services.

IPsec supports:

- Network-level peer authentication
- Data origin authentication
- Data integrity
- Data confidentiality (encryption)
- Replay protection

The Microsoft implementation of IPsec is based on standards developed by the Internet Engineering Task Force (IETF) IPsec working group.

IPsec is supported by:

- Microsoft Windows 7
- Windows Vista
- Windows Server 2008
- Windows Server 2003
- Windows XP
- Windows 2000

IPsec is integrated with Active Directory Domain Services (AD DS).

IPsec policies can be assigned through Group Policy, which allows IPsec settings to be configured at the domain, site, organizational unit, or security group level.

4.11.9 Perimeter

Microsoft Forefront Threat Management Gateway (TMG) is an extensible platform that integrates firewall and cache features, and routes requests and responses between the Internet and client computers.

Forefront TMG integrates firewall and cache features to secure networks and improve their performance. Forefront TMG provides filtering to block access to specific sites, and uses

network address translation (NAT) and other methods to enable secure access between an intranet and the Internet.

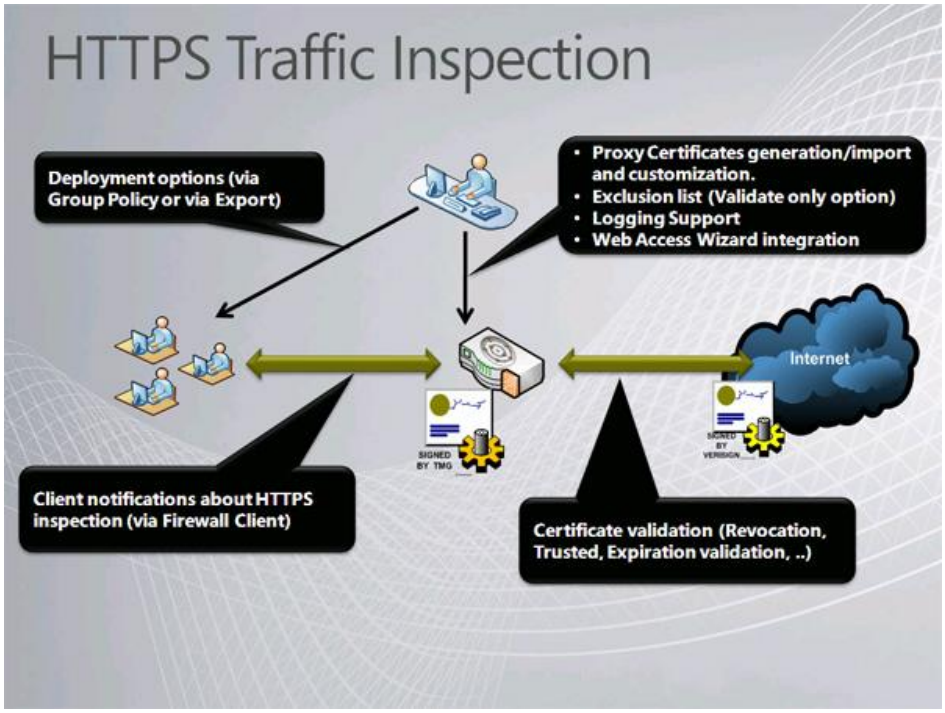

Figure 56 - Forefront Threat Management Gateway HTTPS Traffic Inspection

Forefront TMG is an extensible platform that provides security, hardware redundancy and load balancing, efficient use of network resources by means of sophisticated caching mechanisms, and administration tools. Forefront TMG features are extensible by developers and configuration tasks can be automated. Forefront TMG runs on computers using Microsoft Windows Server 2008 and relies on the features and functionality of the WS 2008 operating system.

Forefront TMG includes several technologies:

- Microsoft Firewall service
- A Web proxy
- Secure network address translation (SecureNAT)
- Advanced caching capabilities, including RAM caching and use of the Cache Array Routing Protocol (CARP)
- Dynamic Internet Protocol (IP) packet filtering
- Virtual private networking (VPN)
- Alerting

Included in the tools section below are the SDL Security Threat Modeling Tool, and the Security Intelligence Reporting Tool which complement a TMG implementation and operation.

4.11.10 Secure Operations

Secure Operation is every bit as critical as a SDL. If proper secure operational guidelines are not followed, the secure design, development and deployment efforts may be severely or completely compromised.

NERC CIPS 2-9 provide guidance for the high voltage transmission system. Due to the inherent integration and interoperation being driven by the new business processes of the smart energy ecosystem, it will be paramount that consistent operational security best practices are followed. Proper training, qualification and operation should be included in the utility operational security program and the architecture must enable execution and reporting on these programs. Microsoft supports the evolving security landscape for system operations across the entire smart energy ecosystem.

4.12 Platform

The smart energy ecosystem requires a wide range of computing resources.

Starting from the smallest devices of the ecosystem and working up to the larger parts of systems presented in the reference architecture we can see the following:

- Smart devices that are constructed using embedded operating systems, such as the Microsoft .Net Micro Framework, Windows CE, or Windows Embedded.
- Mobile handheld devices that leverage mobile operating systems such as Windows Mobile and the .NET Micro Framework.
- Portable computers (e.g. laptops and notebooks) that leverage operating systems such as Windows Vista or Windows 7.
- User desktop platforms, such as those using Windows 7, Windows Vista or Windows XP, noting that user desktops may also be outside the enterprise, as are the cases for customers with their own personal computers or employees working remotely.
- Departmental and enterprise servers, such as those that use versions Windows Server, such as Windows Server 2008.
- Cloud-based servers, where the physical platforms are deployed within a Microsoft data center.

Common to all of these platforms is connectivity via a network. Most platforms currently use one or more 32- or 64-bit processors. Where smart devices may have small memory footprints and low power consumption, the other end of the spectrum includes enterprise servers with 32GB memory, multiple processors and high power consumption.

4.13 Virtualization

Virtualization is another important platform technology for the smart energy ecosystem.

Within settings such as an ISO or utility, there are a diverse set of applications that need to be deployed. Each application deployment may require many processors to adequately support users, simulations and analysis, as well as to provide for needs beyond normal operations, such as development, testing and training. And each application has specific needs related to operating systems, memory and processors, where the needs will likely change over time.

Virtualization can take on many dimensions that need to be allowed and managed, including:

- Server
- Desktop
- Storage
- Application
- Presentation
- Network

Without virtualization, it is common practice to oversize the deployment footprint for an application to address potential future needs and minimize risk. It can become a daunting task to manage the hardware for these deployments, to say nothing of the issues of cost, space, power and cooling requirements.

By contrast, virtualization provides the means for resources to be optimized on an enterprise basis, as opposed to a per application basis.

Virtualization is used to:

- Provide a virtual infrastructure that can be configured to optimize the utilization of the underlying physical infrastructure.
- Apply to servers, desktops and applications.
- Optimize the utilization of computing infrastructure and improve business continuity.
- Apply across a wide spectrum of ways, from servers in the data center to desktops.

4.13.1 Hyper-V

Server consolidation is a significant new trend in IT infrastructure, for the optimization of physical servers.

Hyper-V and System Center Virtual Machine Manager, as well as the other Microsoft virtualization technologies, all help enable broad server consolidation use cases, as shown in Figure 54.

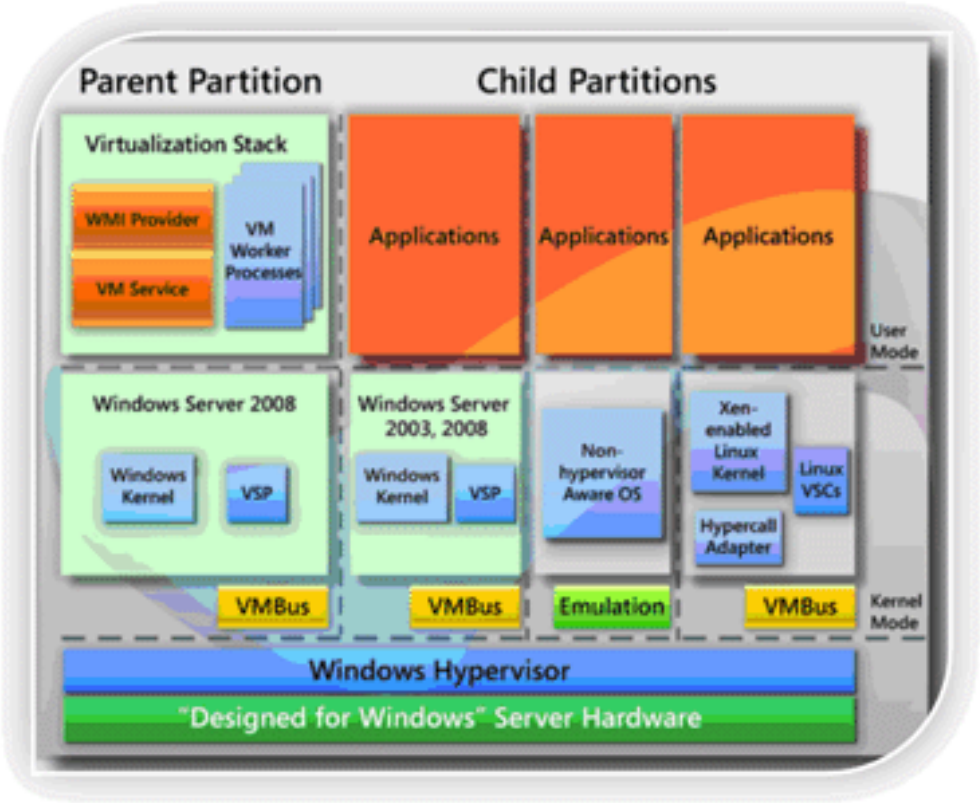

Figure 57 - Hyper-V Visualization Stack

Microsoft Hyper-V provides software infrastructure and management tools that are used to create and manage a virtualized server computing environment.

Using Windows Server 2008 Hyper-V, a variety of guest operating systems – including Windows Server, Windows XP, Vista and Linux versions – can be used. Hyper-V can be used to make a virtual machine highly available through the use of Failover Clustering.

Other key features include:

- Ability to export and import a Virtual Machine (VM) from one host to another
- Live migration
- Encryption of the server, so that data cannot be stolen even if disks are stolen
- Live backup of running VMs
- Wide range of hardware supported
- Wide range of storage supported, including direct and network attached storage and the use of storage area networks
- Snapshots of VMs can be taken
- Up to 32GB of physical memory can be used
- 32 and 64 bit VMs
- Up to 4 virtual processors per VM.

4.13.2 Microsoft Desktop Virtualization

Depending on user requirements, Microsoft has several different options for desktop virtualization.

- The most common desktop virtualization is Terminal Services, a server side solution where clients connect to the server via a Microsoft Remote Desktop Protocol.
- Enterprise Desktop Virtualization is for client-hosted Virtual Machines (VMs).
- Microsoft also provides Application Virtualization, Presentation Virtualization, and Profile Virtualization to further separate logical processing from the physical infrastructure.

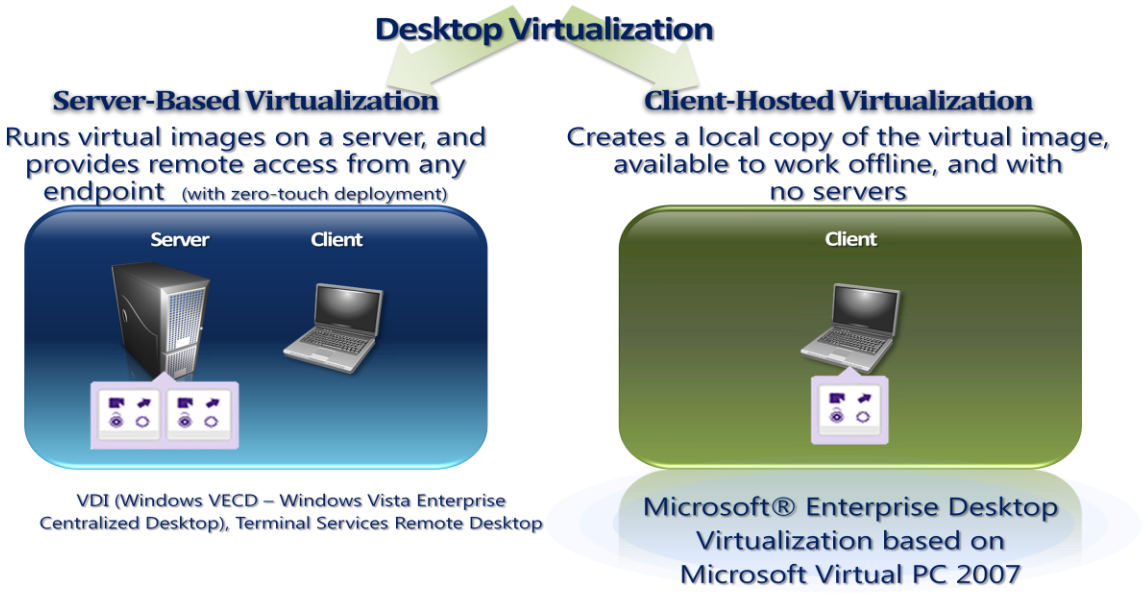

Figure 58 - Desktop Virtualization

4.13.3 Remote Desktop Services

Remote Desktop Services (RDS) is the new name that includes Terminal Services and reflects the expanded role in Windows Server 2008 R2 so that you can run the desktop or applications in the datacenter while your users can be anywhere. RDS enables a full-fidelity desktop or application experience and efficiently connects remote workers from managed or unmanaged devices. RDS helps keep critical intellectual property secure and simplify regulatory compliance by moving applications and data from the user's access device to the data center.

Remote Desktop Services provides a single set of infrastructure for presentation virtualization and virtual desktop infrastructure (VDI). RDS provides a centralized desktop delivery architecture.

Presentation virtualization (formerly Terminal Services) provides the ability to centrally manage an application while serving up application interaction to a remote user. However, this approach has typically involved a separate Terminal Server for each application which can result in servers being underutilized. Microsoft Application Virtualization for Terminal Services solves this issue, enabling server consolidation, better profile management and acceleration of application deployment.

4.13.4 Microsoft Application Virtualization

Application virtualization is at the heart of Microsoft Application Virtualization (App-V).

As shown in Figure 56, App-V enables applications to run on client machines without being installed on them. App-V creates a package of a single application, and these application instances stored on the server are streamed to the PC where they run in their own virtualized Windows environment, isolated from other applications.

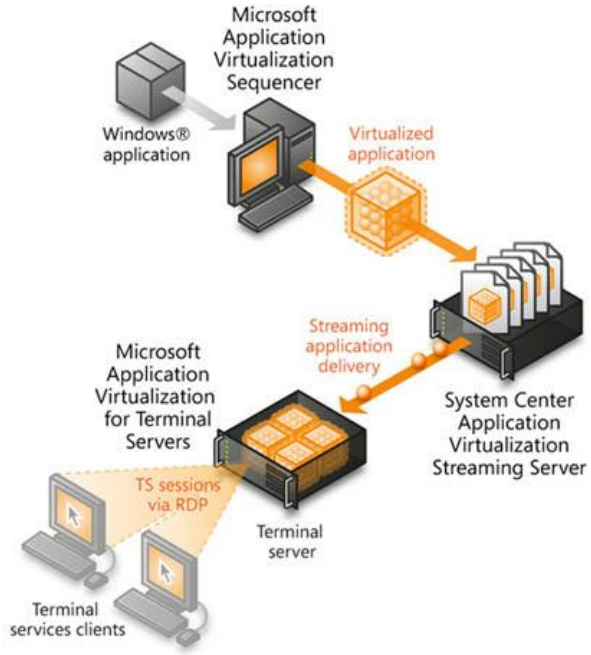

Figure 59 - Application Virtualization

App-V has many advantages:

- It eliminates much of the tedious application management tasks, which can result in significantly accelerating deployment of capabilities to end users and as well as enable very large scale deployments.

- Centralized management and delivery of applications significantly reduces the effort to migrate client side PC OS as well.
- App-V decouples applications from the operating system and enables them to run as network services.

These capabilities will allow faster evolution of the smart energy ecosystem resulting from faster and easier deployment of new application versions, and from broader deployment to many more machines once the platform constraint is eliminated.

Figure 60 illustrates how Application Virtualization Sequencer can scale out of new features and functionality can be achieved with much less effort than in the past, where each computing platform had to be individually configured.

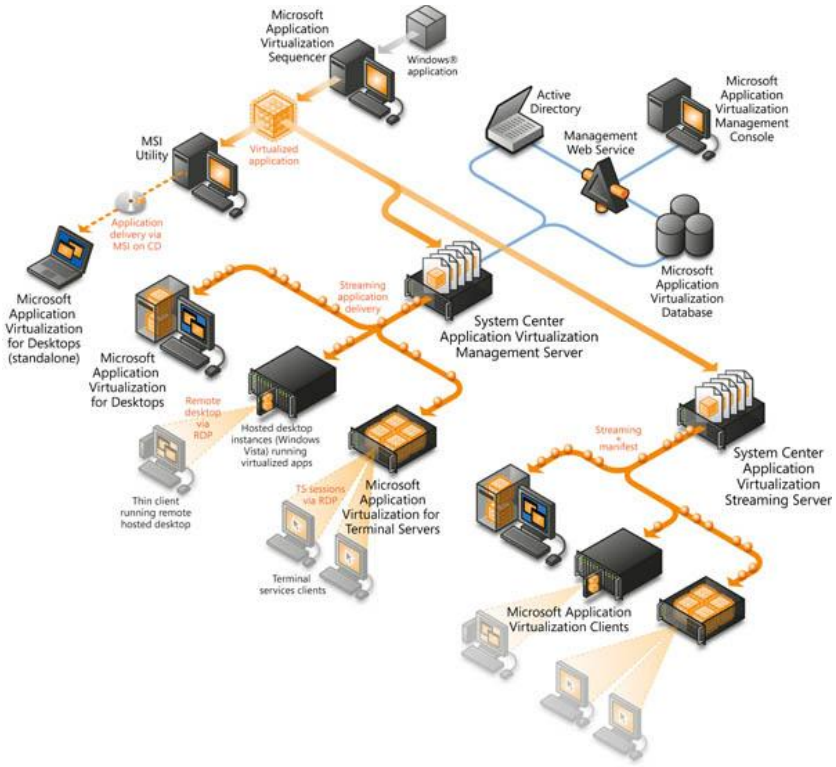

Figure 60 - App V Scale Out

Application virtualization can be used in conjunction with other virtualization technologies—network, storage, machine—to create a fully virtual IT environment where computing resources can be dynamically allocated in real-time based on real-time needs.

App-V enables applications to run without the need to visit a desktop, laptop, or terminal server. Applications are no longer installed on the client—and there is minimal impact on the host operating system or other applications. App-V virtualizes per user, per application instance, as well as key application components. As a result, application conflicts and the need for regression testing are dramatically reduced.

Applications are rapidly delivered, when needed, to laptops, desktops and terminal servers via Dynamic Streaming Delivery. In most cases, only a small percentage of the application is needed to launch the application. Additional components are delivered when transparently requested by the application. This results in faster delivery of the application when needed. App-V streaming also integrates directly into System Center for a unified management strategy.

Centralized, policy-based management supports virtual application deployments, patches, updates, and terminations more easily via policies, and administered through the App-V console or via your ESD system. App-V reduces the complexities inherent in enterprise application management and enables IT administrators to reduce challenges and transform their computing environment into a dynamic, services-oriented infrastructure.

4.13.5 Microsoft Enterprise Desktop Virtualization

Microsoft Enterprise Desktop Virtualization (MED-V) is a desktop virtualization technology targeted at simplifying desktop management.

MED-V is an OS image that uses Virtual PC desktop VM Monitor to host and run instances of Windows desktop OS. Users interact with the VM running on the local PC and administrators can configure the MED-V so that users are unaware their application is running in a VM. MED-V gives users a standard environment – running in a VM – that can easily be moved to a new PC, as shown in Figure 61.

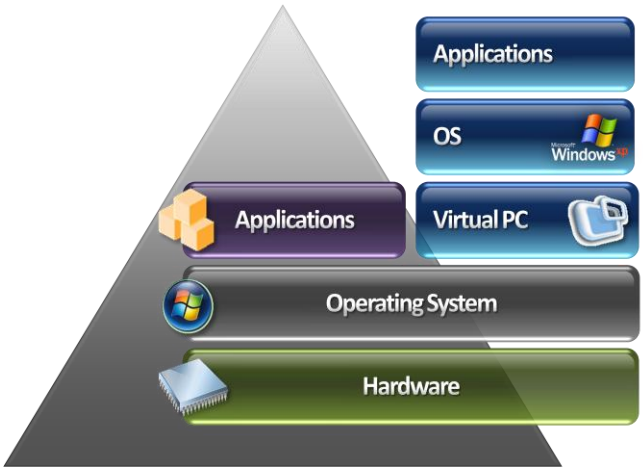

Figure 61 - Microsoft Enterprise Desktop Virtualization

MED-V can be used to run different versions of an OS concurrently, a capability that can help administrators manage OS upgrades.

For example, MED-V can run Windows Vista or Windows 7 directly on the PC, and run Windows XP in the VM. This lets PCs run legacy applications configured for older versions of an OS while taking advantage of new capabilities of a new OS or applications on the same desktop.

MED-V is simpler than a Virtual PC in that it can hide from the end user the fact that applications are running in a VM. Applications can be started from the Windows Start Menu, just as if they were running in the base operating system, or from host icons on the desktop. Or application borders can be colored to denote that the app is running in a VM.

VMs typically require large downloads. MED-V uses incremental data transfers to cut down on network traffic – both for initial download and for updates. The transfer technology examines local hard drives and only transfers those files that are not already on the drive or are different, thus reducing transfer volume. For updates, either for an application update of a patch, only the blocks of the VHD which have changed are transferred.

Figure 62 illustrates how administrators can use AD to assign VMs to authenticated users by creating a "workspace" and using it to configure a VM and the policy for how the VM runs in the Virtual PC (VPC)[26].

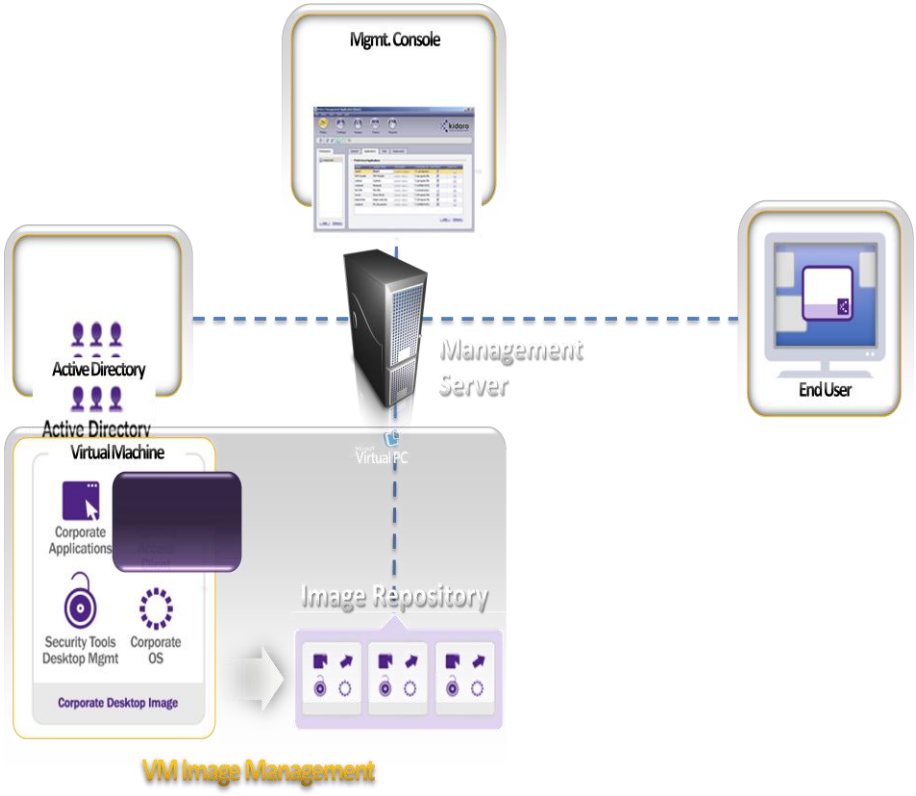

Figure 62 - VM Management

[26] **Microsoft Virtual PC** (renamed **Windows Virtual PC** for the Windows 7 release) is a virtualization program for Microsoft Windows operating systems, and an emulation program for Mac OS X on PowerPC-based systems. The software was originally developed by Connectix, and was subsequently acquired by Microsoft. Wikipedia.org

The execution of the VM is managed on the PC by the MED-V client, in compliancy with the policy. MED-V VMs can be deployed via System Center Configuration Manager or via Internet Information Services (IIS) and do not require user installation. Once configured on the PC, MED-V VMs can be executed offline.

4.13.6 Microsoft Desktop Optimization Pack

MED-V and App-V are delivered as part of the Microsoft Desktop Optimization Pack (MDOP) which is a set of PC management technologies:

- Microsoft Application Virtualization turns applications into centrally managed services that are never installed, never conflict and are streamed on-demand
- Microsoft Asset Inventory Service translates software service into business intelligence and instantly depicts a complete portfolio of the desktop software
- Microsoft Diagnostics and Recovery Toolset reduces downtime and accelerates desktop repair, recovery, and troubleshooting of unbootable Windows-based Systems
- Microsoft Advanced Group Policy Management provides governance and control over group policy through robust change management and role-based administration tools
- Microsoft System Center Desktop Error Monitoring enables proactive problem management by analyzing and reporting on application and system crashes
- Microsoft Enterprise Desktop Virtualization enhances deployment and management of Virtual PC images on a Windows Desktop while also providing a seamless user experience on a Virtual PC environment independent of the local desktop configuration and operating system

4.14 Tools

This section describes the tools used for design development, deployment and management of the smart energy ecosystem.

The breadth, depth and consistency of tools can offer both significant economies and technical advantages across the entire scope of the smart energy ecosystem, whether developing smart home devices using .NET Micro Framework, or developing the most complex next generation energy management system applications.

4.14.1 Visual Studio

Microsoft Visual Studio (VS) is a complete suite of tools for building server, desktop and Web-based applications, enterprise solutions and cloud-based services. Visual Studio is an interactive development environment (IDE) that has a graphical user interface and environment that helps to minimize development efforts.

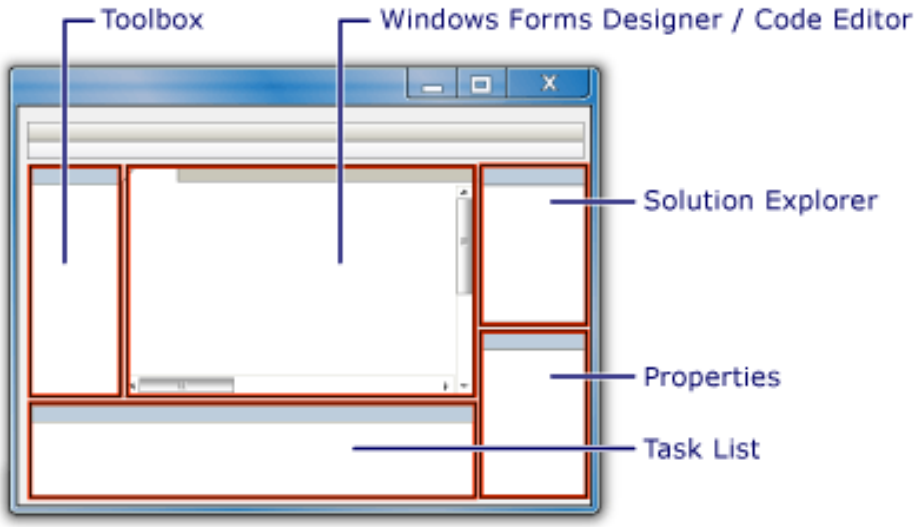

Figure 63 - Visual Studio IDE

Typically, the IDE is used to design forms and edit code. Within this IDE, IntelliSense provides an array of features that make language references easy to access. Visual Studio enables development using a variety of programming languages, including:

- Visual Basic
- C#
- C++
- Jscript
- ASP.Net

Visual Studio can be used to develop applications empowered by the capabilities provided by the .NET Framework and .NET Micro Framework, where code can be compiled for execution using the Common Language Runtime (CLR). However, it can also be used to develop other targets such as reports, orchestrations, RIAs or workflows. Indeed, Visual Studio features a wide variety of SDKs. Visual Studio also provides for source code control and support of development teams through the Visual Studio Team System.

4.14.2 Azure

Azure services are implemented using the Windows Azure SDK for Microsoft Visual Studio.

The Azure Services Developer Portal is an administrative tool for managing, deploying and monitoring services hosted within Azure. Cloud services are developed locally using the Developer Fabric and Development Storage with Visual Studio.

Figure 64 describes a process for moving from development to production.

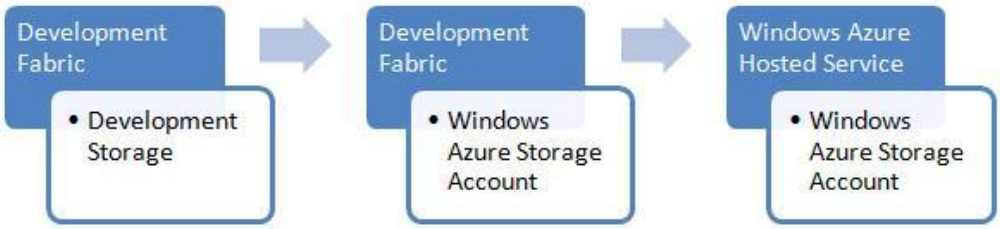

Figure 64 - Azure Deployment Workflow

The Azure Services Developer Portal requires the developer to login to an account using a Live ID. From there, there are a number of wizards that facilitate deployment and management.

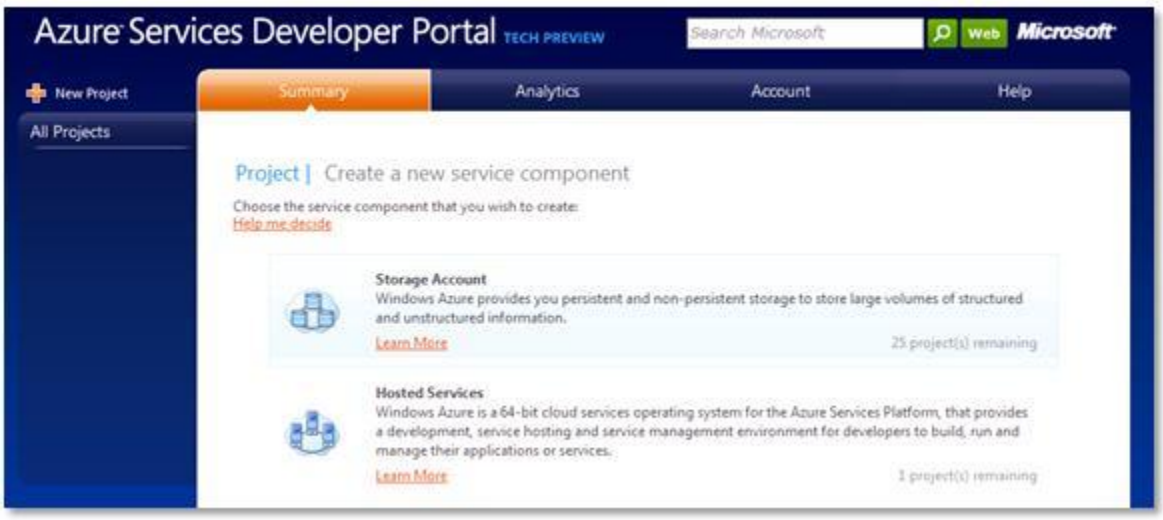

Figure 65 - Azure Services Developer Portal

Within Visual Studio, the 'publish' feature is used to package and publish a cloud service product. Within the portal interface, it can then be uploaded and deployed.

4.14.3 Silverlight

Microsoft Silverlight is a cross-browser, cross-platform implementation of the .NET Framework for building and delivering the next generation of media experiences and rich Internet applications (RIA) for the Web.

Silverlight is an important technology for the smart energy ecosystem, as it provides for location agnostic user interfaces.

Silverlight unifies the capabilities of the server, the Web, and the desktop, of managed code and dynamic languages, of declarative and traditional programming, and the power of Windows Presentation Foundation (WPF). The Silverlight Tools for Visual Studio 2008 provide features for

creating applications in Silverlight that may use either the managed API or JavaScript API programming models.

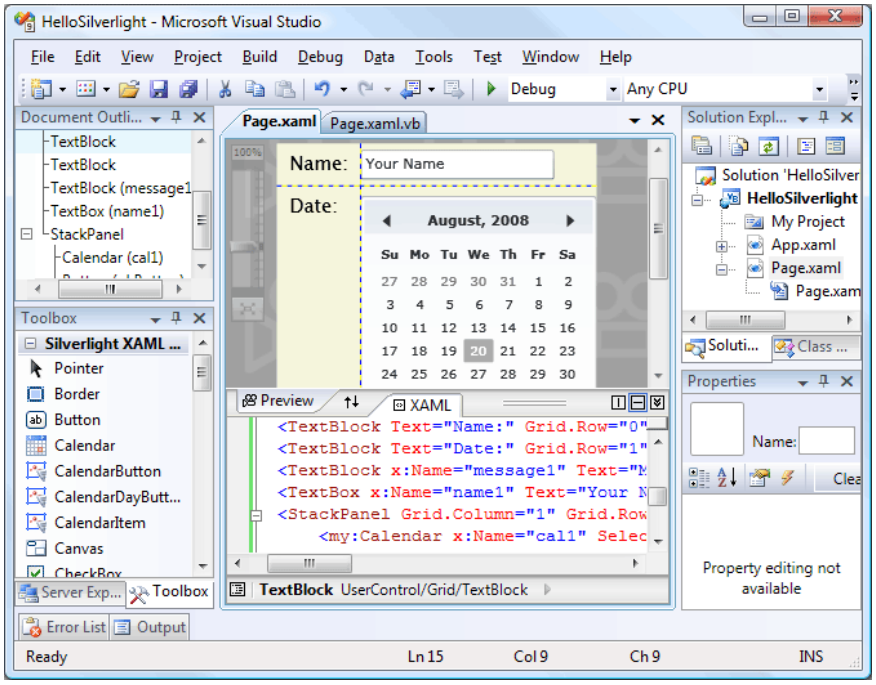

Figure 66 - Silverlight Designer

Figure 67 describes Silverlight 3.0 architecture, highlighting new features provided in version 2.

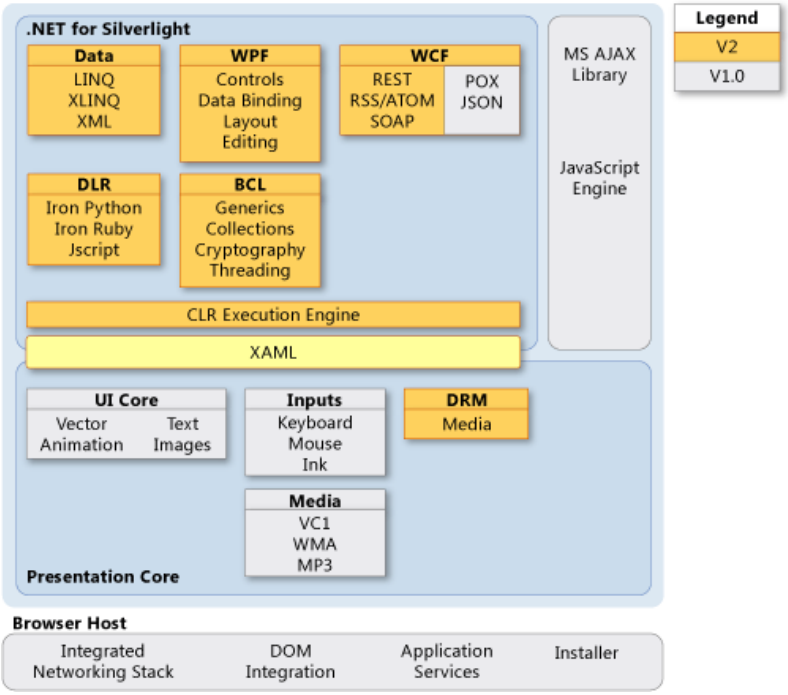

Figure 67 - Microsoft Silverlight Architecture

The core functionality provides by a browser plug-in that renders a user interface using XAML and exposes its internal Document Object Model (DOM) and event programming model in a way that is scriptable via JavaScript in addition to support for the use of a managed API. The managed API is based upon a subset of the .NET Framework. Access to remote services is enabled through the Windows Communication Foundation (WCF).

4.14.4 BizTalk System Design Environment

BizTalk solutions are implemented using BizTalk Project System Design Environment. This environment is built upon the Visual Studio development platform, permitting development of:

- Orchestrations
- Pipelines
- Business Rules
- Web Services
- Maps
- Adapters
- Business Activity Monitoring
- Human Workflows
- ESB

There are also a number of posters available related to a variety of aspects of BizTalk Server, including configuration, database infrastructure and BAM.

The BizTalk Orchestration Designer provides the capabilities needed to define process orchestrations. The orchestrations are used by BizTalk Server 2009 to orchestrate message exchanges between a set of applications.

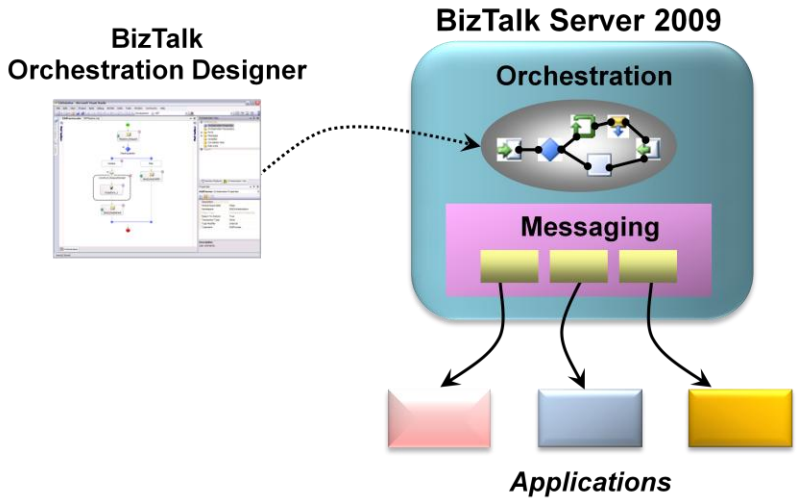

Figure 68 - BizTalk Orchestration Designer (Source: Chappell & Associates)

Figure 69 shows how BizTalk orchestrations are defined graphically, using drag and drop of components from a BizTalk Orchestration palate.

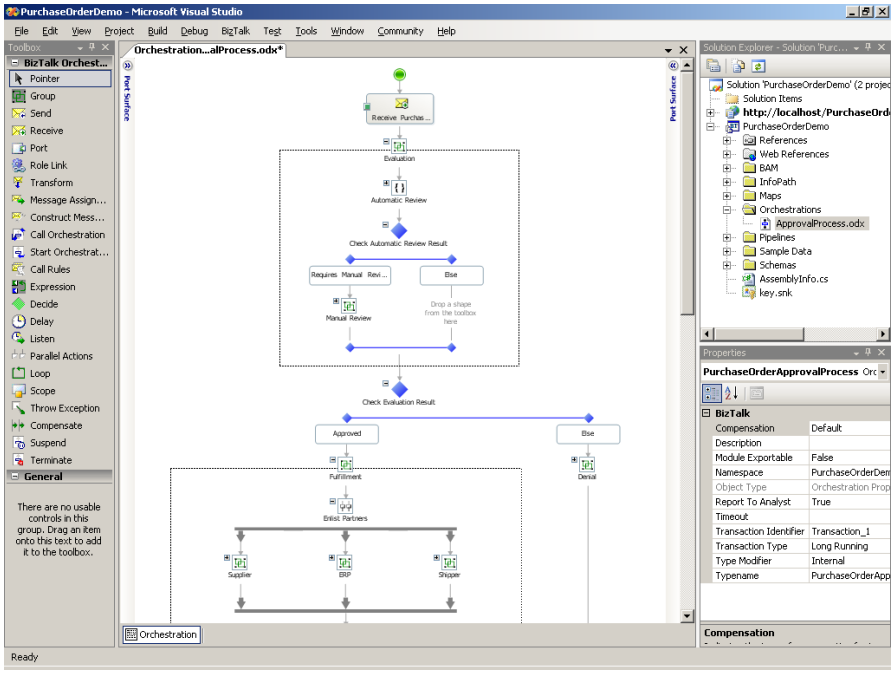

Figure 69 - Process Orchestration Design

Message structures within BizTalk are defined using XML Schemas. These can be created using the BizTalk Editor. Figure 70 illustrates the BizTalk Editor layout:

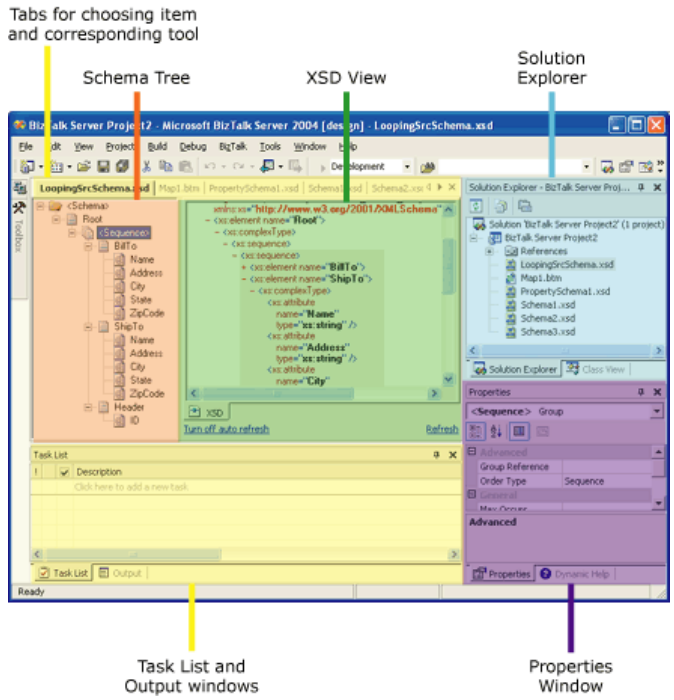

Figure 70 - BizTalk Editor

Within integrations, there is typically need to map inputs from a source into the output needs for a target. This is done using the BizTalk Mapper as shown in Figure 71.

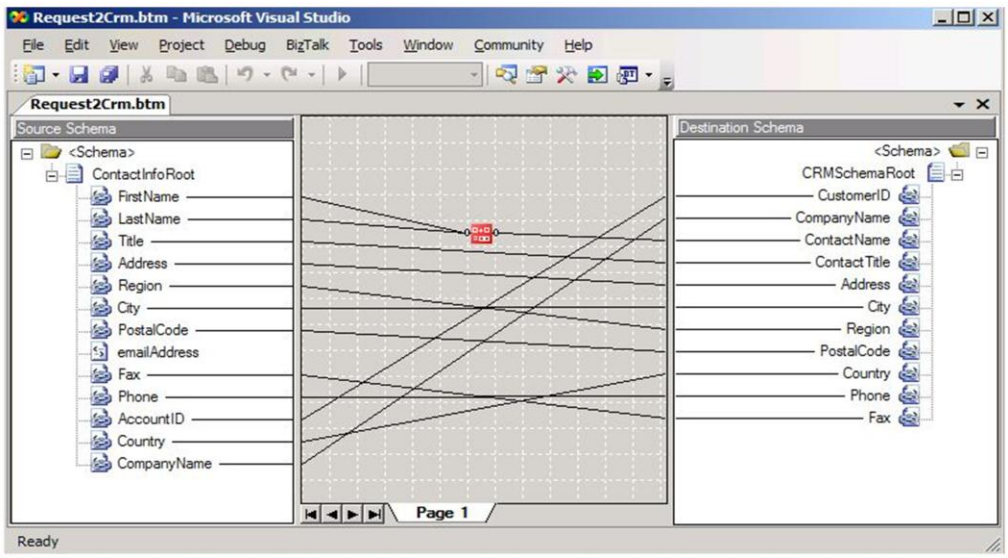

Figure 71 - BizTalk Mapper

The Microsoft BizTalk ESB Toolkit is a part of BizTalk Server 2009 that provides architectural guidance, patterns and a collection of BizTalk Server and .NET Framework components to simplify the development of an Enterprise Service Bus (ESB) on the Microsoft platform and to allow Microsoft customers to extend their own messaging and integration solutions.

Development scenarios common to ESB include:

- Itinerary-based routing
- Dynamic resolution and routing
- Dynamic transformations
- Exception management

This toolkit includes a number of ESB support components that are used for ESB implementations.

4.14.5 SQL Server Management Studio

SQL Server Management Studio is used by database developers and administrators for development and management of any components of the database engine.

SQL Server Management Studio combines a broad group of graphical tools with a number of rich script editors to provide access to SQL Server to developers and administrators of all skill levels. This is a primary tool for the support of a wide range of data-intensive applications including:

- Model management
- Meter data management

- Asset management
- Data warehouses

4.14.6 Business Intelligence Development Studio

Business Intelligence Development Studio is Microsoft Visual Studio 2008 with additional project types that are specific to SQL Server business intelligence.

Business Intelligence Development Studio is the primary environment used to develop business solutions that include Analysis Services, Integration Services, and Reporting Services projects.

Each project type supplies templates for creating the objects required for business intelligence solutions, and provides a variety of designers, tools and wizards to work with the objects, as shown in Figure 72.

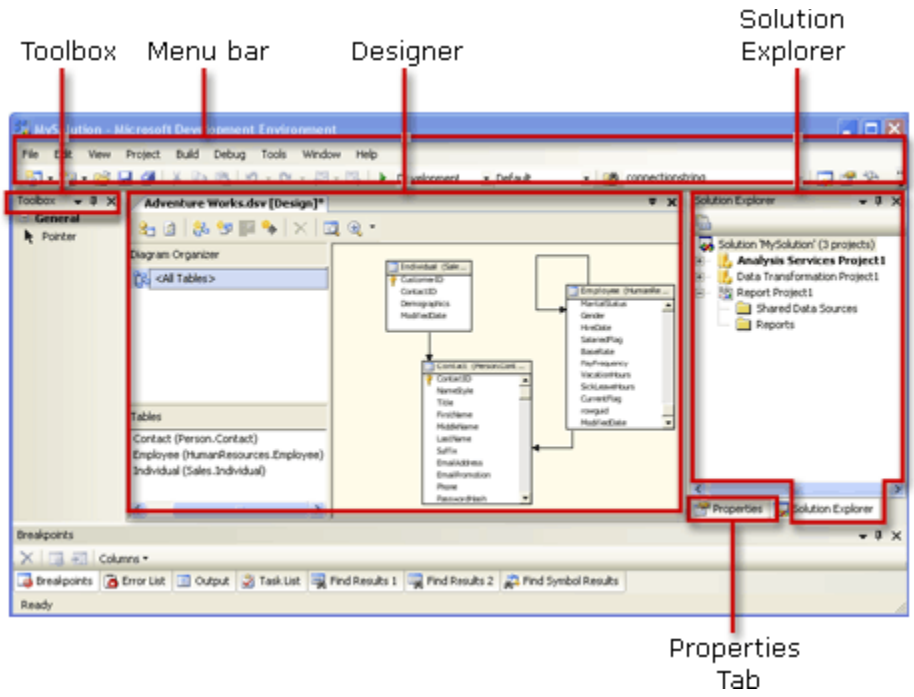

Figure 72 - Business Intelligence Development Studio

The SSIS Designer is a graphical tool that is part of the Business Intelligence Development Studio. The SSIS Designer includes a number of wizards that can be used for:

- SQL Server import and export
- Integration services connections
- Package installation
- Package configuration

4.14.7 Visio

Microsoft Visio is a drawing and diagramming platform that is used to visualize, explore and communicate complex information.

Visio is part of the Microsoft Office Suite.

Part of the power of Visio is its extensibility through the use of add-ins, where its capabilities are extended through both Microsoft and third party products to support a wide range of both technical and non-technical users.

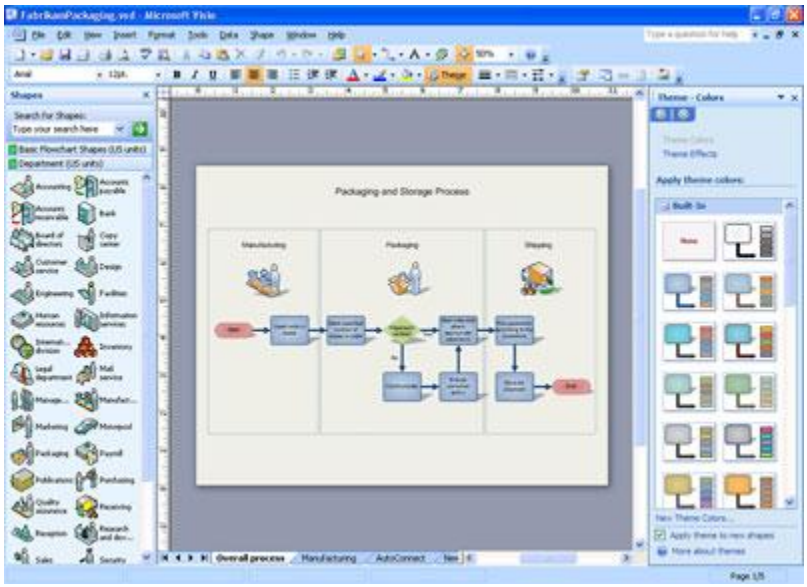

Figure 73 - Office Visio 2007

From the perspective of the smart energy ecosystem, Visio users would primarily include:

- Business analysts
- System architects
- Data architects
- Software architects
- Software engineers
- Programmers
- Developers
- Project managers

A common thread for many of these users is the definition of architectures and business processes through the use of UML. Visio conveniently supports a variety of UML diagram types.

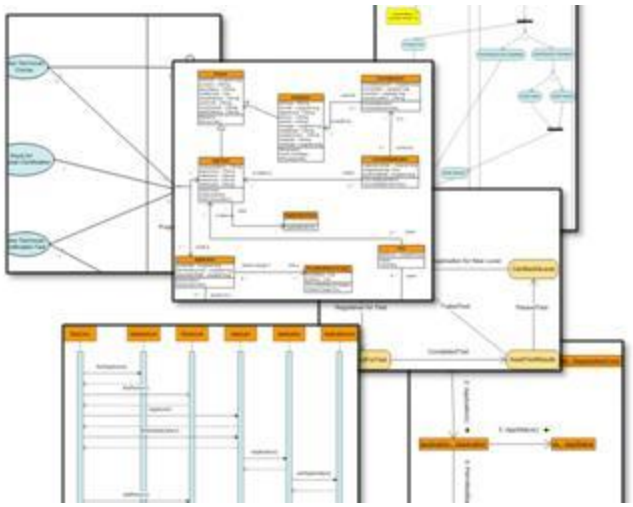

Figure 74 - UML using Visio

Some of the types of diagramming and visualizations supported by Visio 2007 include:

- Use cases
- System architectures
- Data flows
- Workflows
- Database design, and reverse engineering
- Process flows
- Web site designs
- User interfaces

Other sophisticated Visio capabilities include the ability to both reverse engineer and generate database schemas. It is also possible to connect data to diagrams and link data to shapes using the Data Link functionality. A data refresh feature can be used to automatically update data in diagrams. A Software Development Kit is available that allows Visio capabilities to be extended using a variety of programming languages.

4.14.8 Microsoft Modeling Tools

The Microsoft Modeling tool codenamed “M” is a new technology revealed recently at the Microsoft Professional Developers Conference.

“M” is part of the new Oslo set of Microsoft modeling technologies that include:

- A storage runtime (the code name “Oslo” repository, built on SQL Server 2008) that is highly optimized to provide your data schemas and instances with system-provided best SQL Server practices for scalability, availability, security, versioning, change tracking and localization.

- A configurable visual tool (Microsoft code name “Quadrant”) that enables you and your customers to interact with the data schemas and instances in exactly the way that is clearest to you and to them. That is, instead of having to look at data in terms of tables and rows, “Quadrant” allows every user to configure its views to naturally reveal the full richness of the higher-level relationships within that data.
- A language (Microsoft code name “M”) with features that enable you to model (or describe) your data structures, data instances and data environment (such as storage, security, and versioning) in an interoperable way. It also offers simple yet powerful services to create new languages or transformations that are even more specific to the critical needs of your domain. This allows .NET Framework runtimes and applications to execute more of the described intent of the developer or architect while removing much of the coding and recoding necessary to enable it.

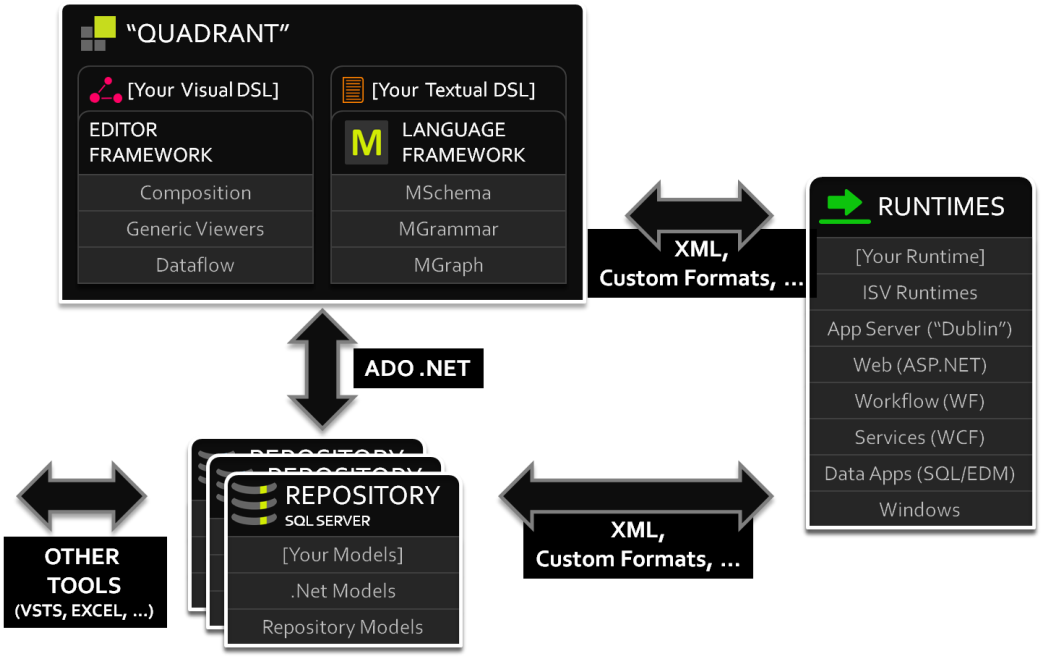

Figure 75 - “Oslo” Architecture

The development of CIM-based applications using model driven interfaces will be vital to the evolution of the smart energy ecosystem.

“M” provides the capability to: define data structures or schemas and store them into a repository. “M” models can be created using Visual Studio 2008 or later versions. The Visual Studio project build creates two files: one compiled image that can be loaded into the “Oslo” repository, and the other T-SQL script that can be loaded directly into a SQL Server 2008 Database. Once the model is in the “Oslo” repository database, applications can read and update model instances to drive application behavior or analyze the model by directly querying the model instance data.

The “Oslo” repository is implemented as a Microsoft SQL Server 2008 database, which provides a solid foundation for data storage for “Oslo” technologies and applications. SQL Server 2008 supports databases that are highly scalable, available and secure. SQL Server 2008 features include clustering, database mirroring, resource governor, backup-and-restore, replication, reporting services, change data capture and change tracking.

The use of SQL Server as the M schema repository has a very beneficial benefit for managing models in a utility. SSIS can be used to create new version of the repository, and applications subsequently moved to the new version. The SQL Server 2008 Change Data Capture feature can be used to track all updates to repository tables, thus helping to provide a historical record of model and schema updates.

As earlier stated, modeling in the smart energy ecosystem can be a challenging task, especially at the distribution level where systems can comprise literally millions of devices. Defining equipment in an Asset Management System, defining and updating the operational Distribution Management System (DMS) and Outage Management System (OMS), and defining and updating other systems throughout the enterprise such as the condition based maintenance system, can be time consuming and error prone. Directly mapping “M” schemas to SQL allows easy use of SQL as the base for populations of instances of the “M” schema.

”M” models can also be exposed from Visual Studio into C# assemblies in the CLR domain. This enables Visual Studio and “M” to be the basis of standards based message content definition. This also allows for running queries over the “M” image in the repository.

“M” Grammar and “Quadrant” are two additional elements of the “Oslo” architecture worth noting:

- **“M” Grammar** allows for the creation of languages specific to a domain – such as the electric utilities arena. An example of where this might be applicable is the creation of behaviors or processes around objects defined in the CIM.
- **Quadrant** is a graphical modeling tool that can be used in conjunction to “M” textual editing to easily traverse information models and schemas.

4.14.9 SDL Threat Modeling Tool

Complementing SDL and Forefront TMG is the SDL Threat Modeling Tool, the first threat modeling tool not designed solely for security experts.

SDL TMT makes threat modeling easier for all developers by providing guidance on creating and analyzing threat models.

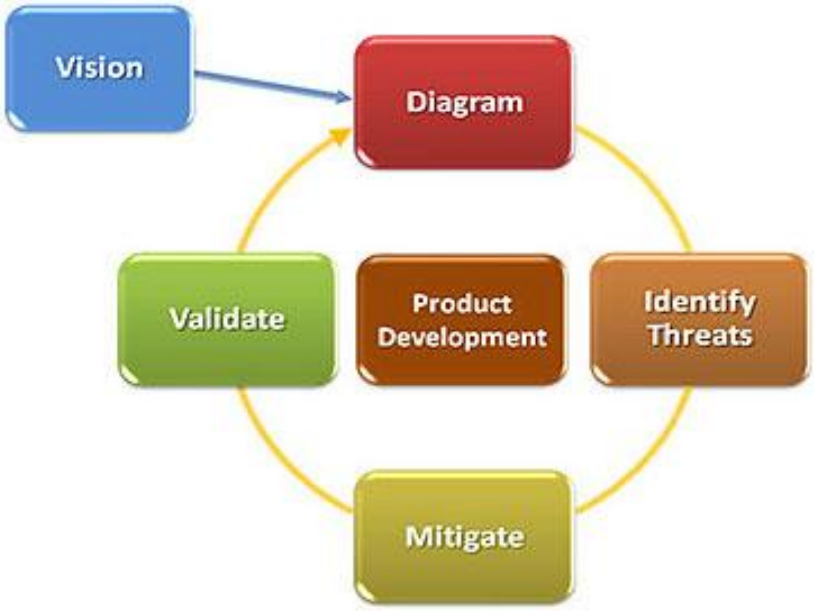

Figure 76 - The SDL Threat Modeling Process

The SDL Threat Modeling Tool enables any developer or software architect to:

- Communicate about the security design of their systems.
- Analyze those designs for potential security issues using a proven methodology.
- Suggest and manage mitigations for security issues.

4.14.10 Security Intelligence Report

Microsoft's Security Intelligence Report (SIR) provides an in-depth perspective on the changing threat landscape including software vulnerability disclosures and exploits, malicious software (malware), and potentially unwanted software.

Conclusion

Microsoft has endeavored to provide the view in this document of a reference architecture that articulates Microsoft's vision for the smart energy ecosystem, and to describe the Microsoft and in some cases, partner technologies which can be used to realize this vision. Microsoft recognizes that achieving this vision is a journey, and that few (if any) utilities have the luxury to implement this architecture in a Greenfield deployment. Further, partners are still developing their offerings to align with the tenants of the guidance of the reference architecture, so solutions will be forthcoming but may not exist today to fully implement this vision. To that end, utilities will need to establish a plan to migrate their infrastructure and solutions to align with the reference architecture.

Quickly some key questions arise: "How do I build the reference architecture plan, and how do I establish the priority of the steps along the plan?" Microsoft has worked closely with research organizations to address this question. An Infrastructure Optimization Model is proposed for use by Microsoft, partners and utilities alike to establish a baseline for a utility organization and to help define the plan to transition the organization. Figure 77 shows the progression for the IO Model.

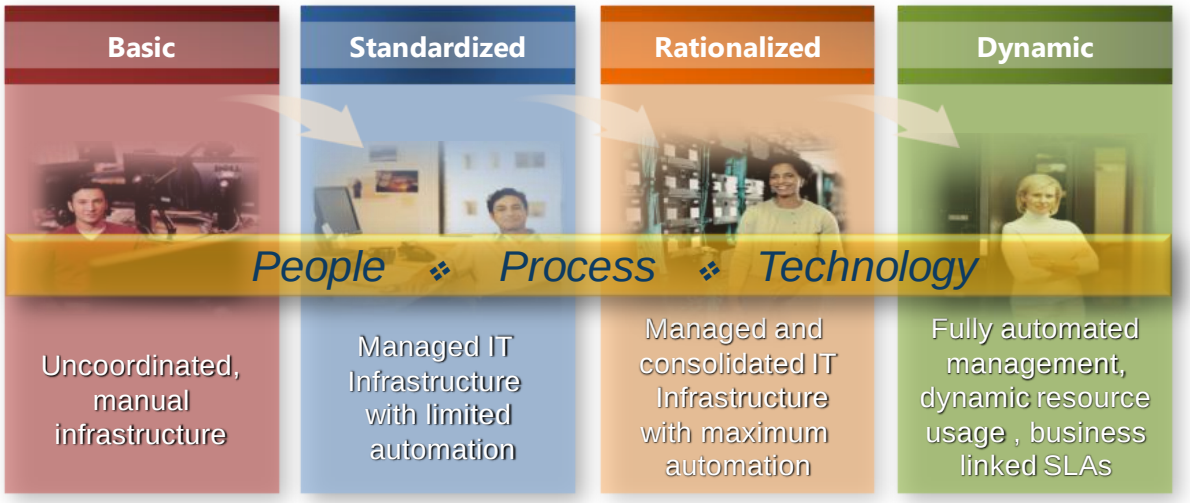

Figure 77 - Infrastructure Optimization Model

Fully implemented, the reference architecture provides guidance to enable achievement of the highest level of optimization: "Dynamic." However, the reference architecture recognizes that a building block approach must be established to make efficient and meaningful progress toward the stated vision. The Microsoft IO Model prescribes that fundamental capabilities be put in place as a foundation, before attempting to ascend to the higher levels of Dynamic infrastructure..

Figure 78 shows the capabilities directly addressed by the IO Model.

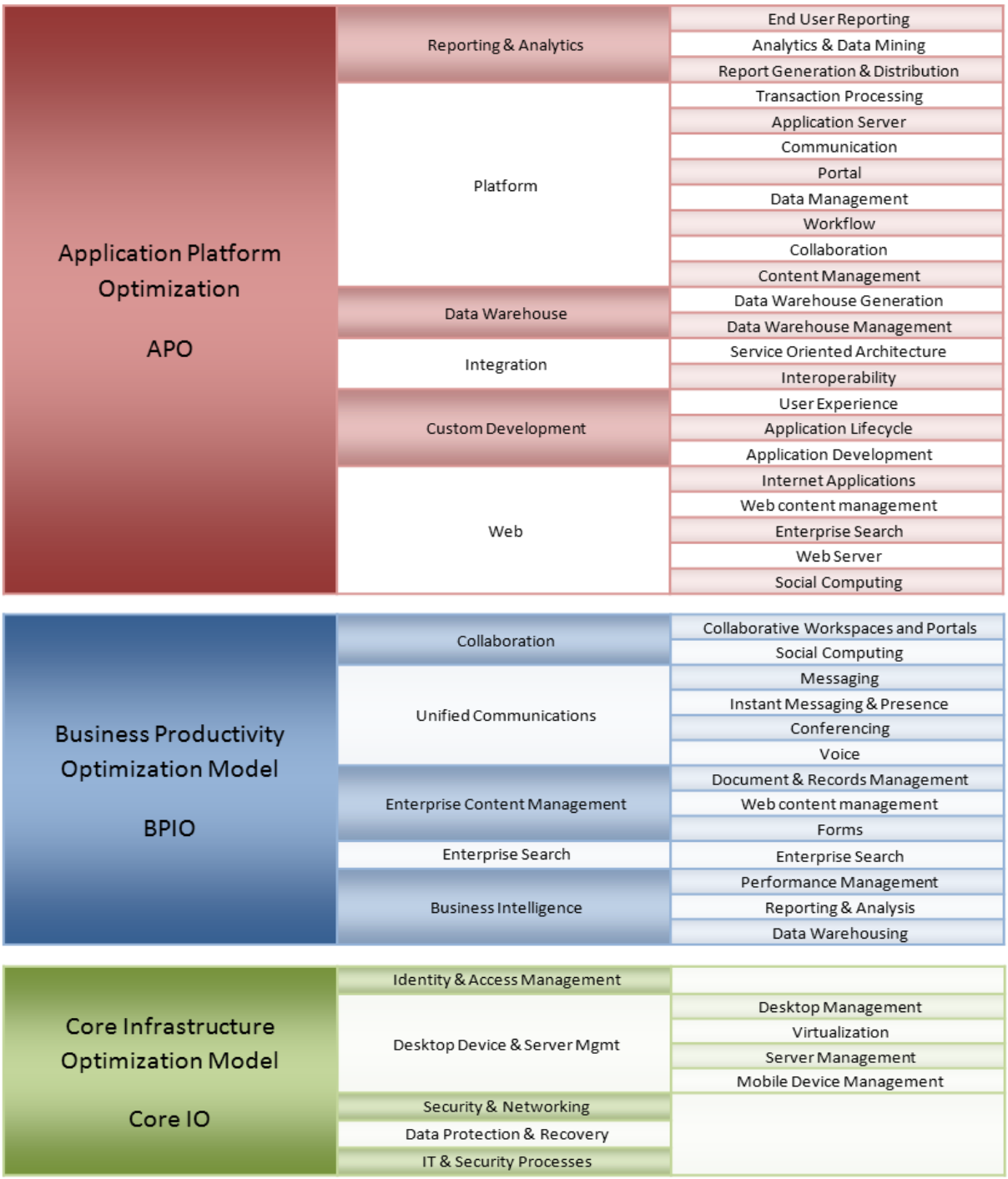

Figure 78 - Microsoft IO Model Capabilities

Note that the capabilities are grouped into three categories:

- Core Infrastructure Optimization
- Business Productivity Optimization
- Applications Platform Optimization

The detailed capabilities identified for each of these three categories state the “what” needs to be achieved for a utility to progress toward the dynamic optimized state. The reference architecture articulates the “how” solutions and infrastructure should be architected and deployed to enable achievement of the vision.

The transition of the power and utilities business to the new smart energy ecosystem may well be the most significant change to shape the industry since its inception. New processes such as end use loads dynamically participating in the ecosystem in a meaningful way, and new data requirements such as the 2,880 fold increase moving from 1 customer billing sample per month to 15 minute samples for a 30-day month, will significantly change the landscape. Smart metering, automotive electric propulsion, renewable generation, new communications, new business models and a host of new industry players will all shape the future. The outlook can be a daunting challenge for anyone in the power and utilities computing arena.

Microsoft believes that the SERA proposed within this document and the Microsoft Infrastructure Optimization Model provides the best avenue to navigate not only these challenges, but to establish a position of agility to navigate the challenges that are unforeseen today.

Microsoft and its partners’ complete set of solutions can be found on its Utilities Web site, www.Microsoft.com/Utilities.