White Paper

prepared for the

Electric Power Research Institute (EPRI)

Scoping Study and Survey of Electric Utility Industry Chief Information Officers (CIOs):

Trends, challenges, opportunities, and plans regarding future Information Technology Needs for the Electric Power Industry

By

Massoud Amin
Professor of Electrical and Computer Engineering
Honeywell/H. W. Sweatt Chair in Technological Leadership
Director, Center for the Development of Technological Leadership (CDTL)
University of Minnesota
Minneapolis, MN 55454 USA

EPRI Project Manager:
Clark W. Gellings
Vice President – Technology

5 November 2007

Introduction

During the last 10-15 years, several research programs at the Electric Power Research Institute (EPRI) have increasingly focused on incorporating sensors, electronic communications, and computational ability across all generation, transmission and distribution assets to enhance the value of electricity to society. Information Technology (IT) serves as a lynchpin in this system and keeps the network together.

However, we are concerned that the evolution in advanced IT may not be brisk enough to meet the needs of our customers. Figure 1 depicts the increased services expected in the near future due to tremendous amounts of data being generated. This “tsunami” of incoming data will change how utilities operate and maintain the grid. Naturally, among the issues to be explored is whether all this data needs to be centralized and how it may be reduced to information and managed or where it is stored.

Figure 1 illustrates the data that could be generated by a typical utility that decides to overlay a communications infrastructure on its power delivery system and begin to enhance the functionality of its system in stages from distribution automation through to full connectivity with customers.

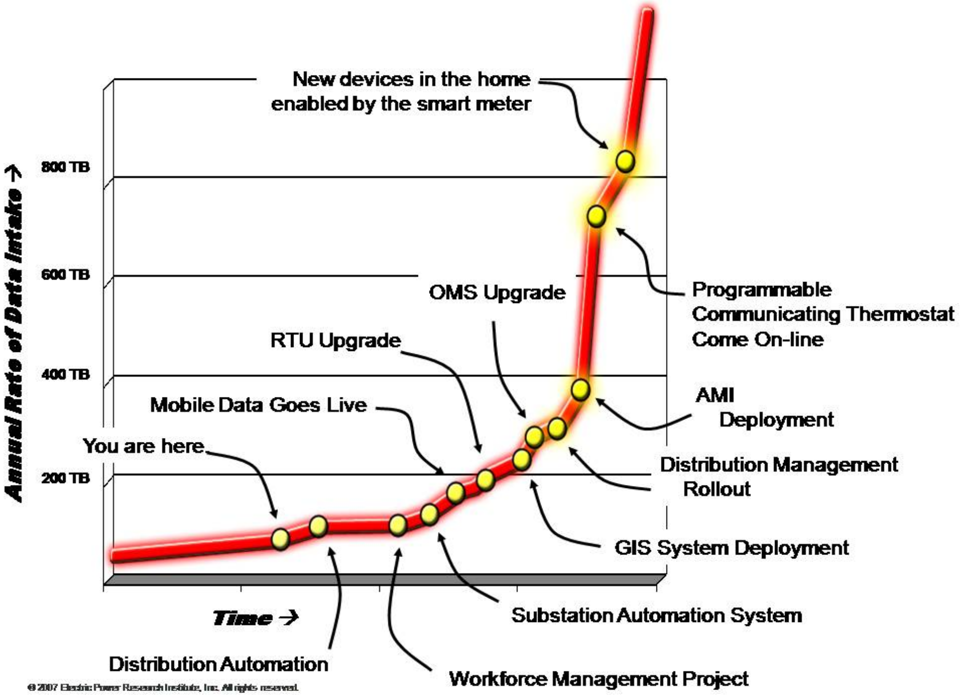

Figure 1: A tsunami of incoming data (Note: AMI in the diagram refers to advanced metering infrastructure)

To put Figure 1 in perspective, the US Library of Congress contains 20 terabytes (TB) of data; the British National Archive, which represents 1,000 years of British history, contains 600 TB; Google’s search engine crawler processes about 850 TB of information (that is the amount of raw data from the web). One TB equals 1,024 gigabytes (GB).

EPRI's leadership asked me to investigate whether there is an IT problem looming for the electric power industry and how EPRI can help the industry address these problems.

We contacted approximately 25 Chief Information Officers (CIOs) in the industry to determine trends and to assess future IT needs for the electric power industry. From September 15 through October 20, 2007, we had the privilege of interviewing 11 CIOs. I gratefully acknowledge the insightful feedback obtained from the following individuals: Mr. Steve Berberich (California ISO); Ms. Rebecca Blalock with Mr. Joe Massari, and Mr. Thomas Wilson (Southern Company); Mr. Chuck Bremer (Ameren Services); Mr. Andres Carvallo (Austin Energy); Ms. Patricia Graham (CenterPoint Energy Inc.); Mr. Joe Hamrock (AEP); Mr. Ron Hinsley (ERCOT); Mr. Alain Steven (PJM Interconnection, LLC); Mr. Chuck Tickles (Kansas City Power and Light); and Mr. Clark Gellings, Mr. Kevin Evans and Ms. Joyce Engberg (EPRI).

During these interviews, we focused on the following four questions:

1. What is the potential impact and plan for increased volumes/frequency of incoming data, including tens of thousands of data points and advanced metering infrastructure[*] (AMI) data streams and their integration?

2. What is the changing CIO role and impact in this new IT world, including mergers and consolidations, cyber-security requirements, outsourcing, and workforce challenges?

3. What are the IT challenges that cut across systems and functions? For example, how data and IT networks act as the glue and nervous system map to connect financial systems to operations center to call/phone centers.

4. What are the anticipated IT investments to be made over the next five years? Does this represent an increase over current levels and what is your "no regrets" path to investing?

We have distilled the results of these conversations into this white paper and plan to conduct a workshop in 2008 to deliberate the issues identified. An integrated summary of insights and feedback from the colleagues we interviewed follows in question and answer format.

Questions & Answers (Q&A)

Question 1: What is the potential impact and plan for increased volumes/frequency of incoming data, including tens of thousands of data points and advanced metering infrastructure (AMI) data streams and their integration?

Answer: Two-way communication and advanced metering will generate tremendous amounts of data in the next three to five years. Many electric utilities currently do not handle these high volumes of real-time data. With this massive information explosion expected, we have a huge opportunity to transform the industry.

In fact, many CIOs interviewed have already deployed advanced meter reading (AMR) technology as part of their distribution automation. They are already collecting aggregated data from tens to hundreds of thousands of meters and several thousand alarm stations. Within the next year, AMR will be performed every 15 minutes, resulting in an average of tens of terabytes

[*] Note: The IT community uses the acronym AMI to refer to Alternative Mark Inversion.

of data per week at each organization. However, one CIO pointed out that AMR is not yet a full-fledged AMI. The industry needs to generate a distribution central system similar to the Distribution Energy Management System/Supervisory Control and Data Acquisition (EMS/SCADA) system, but with many more nodes and in a more cost-effective manner.

The real benefits of AMI depend on what it gets leveraged for, with the greatest benefits coming from two-way communication for local control, on demand *reads* and inspection, demand response (e.g., managing thermostats remotely), and integrating other renewable resources (including wind, solar, and biomass) with demand response into the system. Security for AMI will be critical – both physical security and data security through encryption. It is imperative that the industry maintain 100 percent uptime

Data warehousing will also become increasingly important. For example, organizations must decide how much data to retain for each customer every year. If AMI is deployed in just one area, the data will be available for wholesale and independent system operators (ISOs) and regional transmission organizations (RTOs) with shorter time intervals (e.g., 7-day, 12-day and 24-day settlements) with a lower number of data points. However, organizations will need to address storing two to three sets of redundant data.

In addition, organizations must consider market transactions and locational marginal pricing (low-frequency two-way communication mostly generated through the internet), security dispatch (high-frequency data in terabytes of size), and real-time data handling and alarms (which may occur in 5-minute versus 15-minute intervals). These factors will require secure collection and real-time analysis. Data aggregation and storage (which requires additional hardware, servers, memory, etc.) are all shared problems and will place increased stress on the servers, organizations and stakeholders.

While control centers are not currently affected by AMI data streams or data “tsunamis,” there are opportunities in demand response. Organizations should consider how control centers will be integrated into ISOs and where AMI data streams will connect to. Additional challenges at ISOs and RTOs include the following:

- monitoring systems that include different levels of sensors and data collection/ data management systems
- synchronization through control centers
- determining when load has been controlled or otherwise reduced (demand response)
- location of control centers and the resultant communication delays if they are located tens or hundreds of miles away
- accommodating phasor measurement units (PMUs) with three second measurements that have much higher frequencies than remote terminal units (RTUs) done through data concentrators
- handling real-time data that will be utilized for state estimation, contingency analysis, fast simulation, and modeling and visualization (note: enterprise applications are much broader than that and will be pursued programmatically)
- enabling elastic demand and connecting all consumers in the real-time market

In addition, the Federal Energy Regulatory Commission (FERC) has been pushing demand response. To be really useful, a house’s “black box” should sense the price, which will greatly increase data communication needs. Optimistically, in 10-15 years the market could be cleared in seconds (depending on the technology and communication backbone). Realistically, it may take one minute.

All colleagues referenced the potential of emerging smart applications. These include embedded PCs located next to relays, meters used as both information and electricity gateways into homes, communicating with appliances (with built-in security and privacy), and other related advanced applications. In addition, all field personnel will have access to load, maintenance data, GIS and outage management information.

The potential increase in volume and frequency of incoming data and the associated processing and integration points will necessitate migrating to a state-of-the-art (SOA) enterprise systems framework accompanied by the decomposition of traditional legacy applications into services. Unfortunately, this will need to be done on a large scale, and utilities will need to migrate into this new infrastructure quickly.

Question 2: What is the changing CIO role and impact in this new IT world, including mergers and consolidations, cyber-security requirements, outsourcing, and workforce challenges?

Answer: Real-time IT used to be separate from the IT that managed back office and corporate networks. With the implementation of IT-type components and data transmission across the electric grid, the role of the CIO and the electric technology operations officer will combine. Organizational transformation will prove to be a natural outcome of moving to an intelligent grid.

CIOs roles are changing as the system is increasingly “marketized.” CIOs need to evaluate emerging technology trends and focus on how they can best be integrated into the organization to meet business goals. CIOs are closer to the “ground” and are more familiar with the real-time requirements of the industry. However, they must remain disciplined and not react to technological hype.

Many CIOs are relegating their technical roles to their operational organization and are focusing more on business strategies, analysis and due diligence. CIOs already have much of these “soft” skills, but do require more business skills. CIOs are not just technologists, but are also business people. More CIOs are directly reporting to CEOs. As such, they are often involved in assessing mergers and acquisitions along with other strategic responsibilities. In addition, CIOs need to partner with COOs to work on interoperability across the industry.

Organizations are finding it hard to retain talented CIOs. The job market offers many opportunities, especially as baby boomers retire. Organizations are challenged with matching their workforce with fluctuating demand. This may require different compensation structures, especially as organization need to retain expertise in new areas while maintaining legacy systems.

CIOs interviewed expressed concerns about the following business issues:

- out-sourcing or off-shoring mission critical or operationally sensitive areas due to security concerns (can utilities protect their interest via contractual terms?)
- effectively sourcing IT and protecting intellectual property
- managing a supply chain that is spread over hundreds or even thousands of miles, which requires multiple authentication points and encryption
- addressing cyber security (beyond just hackers and other mischief makers), including

encrypting the device layer, tagging data as sensitive, engineering resilience into the network, etc.

- the influences of the North American Electric Reliability Corporation (NERC) and the development of reliability rules
- dealing with compliance and governance issues in a holistic way as they impact gas, electricity, business and customer relations
- the implications of state and federal regulators and legislators, who are increasingly reaching into operations
- the changing culture within utilities, who need to provide instantaneous response to their consumers (not “rate payers”) as quality of goods and services become increasingly compared across the industry

Question 3: What IT challenges cut across systems and functions? For example, how data and IT networks act as the glue and nervous system map to connect financial systems to operations center to call/phone centers.

Answer: Connections into financial systems such as Enterprise Resource Planning (ERP) systems like Oracle, People Soft or SAP have been in place for years. However, organizations require much more connectivity and are transitioning to a full service-oriented enterprise-wide architecture. IT needs to connect processes from disparate systems and harmonize the performance layer. The often millions of data points that come in must be automated and integrated. For example, generators that use dozens of different databases from isolated applications can instead use common data. Organizations have also started to deploy more firewalls and data filtering between operations.

Many colleagues indicated that we are a data rich industry but sometimes information poor. CIOs need to introduce technology that addresses specific business needs and processes instead of deploying overkill solutions that are not required. While technology is certainly prevalent in the market, internal business processes are not necessarily mature enough for efficient implementation of that technology.

Organizations have a continuing and growing desire to analyze their available data and act accordingly. A key objective is building business intelligence around data. The vision is to build the “smart grid.” Organizations need to start with the software, map out their system, and know where their assets are (e.g., Java or .NET). A smart grid provides look-ahead foresight capability and predictions that can forestall problems.

In addition to analyzing data, organizations will need to understand data management from both a corporate and federal perspective. The FERC code of conduct call for effective data segregation and segregation of duties within multiple entitites. These governance and policy requirements may be an excellent opportunity for EPRI and Edison Electric Institute (EEI) collaboration, the National Rural Electric Cooperation (NRECA), and the American Public Power Association (APPA).

Question 4: What are the anticipated IT investments to be made over the next five years? Does this represent an increase over current levels and what is your "no regrets" path to investing?

Answer: Probable investments over the next five years will continue to focus on reducing complexity, increasing sustainability, and driving reusability. In order to implement intelligent/smart grids, organizations must effectively solve end-to-end event correlation of IT and non-IT assets. The "no regrets" path to investing is by integrating business requirements in advance of designing technical solutions.

An extreme example comes from California, which approved $2.2 billion in funding for PG&E to add 5.1 million smart meters by 2011. This will result in operating savings of $160 million per year and reduce demand by 448 MW. Customer bills are anticipated to increase $0.49–$0.99 per month for the first five years and decrease annually thereafter.

For change to be accepted, all IT investments must be performance oriented and based on business results. IT expenditures can be difficult to explain and have political implications. A costly architecture refresh can be justified if clear business cases are made. Some non-IT executives in the industry are confused by the difference between real-time IT and back-office IT systems. They see only one IT system and do not understand the very different characteristics and challenges each has. These executives need to be educated that real-time data usability is key for the industry.

As markets are changing, the requirements on ISOs and RTOs are also changing, and they are under increased governmental pressures to lower their fees. With IT coming in as the biggest item on an RTO's budget, FERC has been under tremendous pressure to reduce IT costs through standardization. They have been criticized for the overall cost of RTOs and questioned about their benefits. Some CIOs are striving to maintain a constant budget by reducing maintenance costs. This helps offset inflationary pressures and creates headroom for adding value-added business. Other CIOs predict that IT spending can go up if initiatives are directly tied to business cases.

IT budgets also need to address increased data storage needs, which will grow into the petabytes, a unit of storage equal to one quadrillion bytes (1000^5 or 10^{15}). Organizations can currently use virtual servers until they can address data center constraints. Quad processors and IBM's new P-platform and storage platforms will help alleviate some of the pressures in the short term.

Other trends CIOs must consider when budgeting include:

- growing investment in security applications and testing
- increasing analytics to transform data into knowledge
- dealing with ERP systems that may be going away
- increasing mobile access to the communications environment for easy access by field workers and executives
- granting call centers real-time access to service levels, payments, outages, etc.
- enabling real-time networks (in seconds) and faster markets (less than a day, executed at any time) to handle increased data and two-way communications linked to the market/business
- accommodating the unknown level of investment by ABB and other vendors in AMI
- increased spending needs for distribution automation and load management systems

In summary,

- **Blockers and barriers to IT investments** are non–technical and stem from policy/politics. Because they are constrained by budgets and cost, IT investments must justify a certain level of return on investment (ROI).

- **Accelerators** include the need to be responsive to the customer and to help reduce energy consumption. In some regions, policy/politics may require integrating renewable distributed resources.

EPRI's Role

The CIOs we interviewed highly encouraged an active role for EPRI. Their suggestions included the following:

- Work with the meter vendors to put a HyperText Transfer Protocol (HTTP) stack on their meters rather than continuing with proprietary protocols. This would then enable access to meter activities over the public Internet through a broadband connection, thus minimizing the communication infrastructure build-out currently needed to support AMI activities.
- Develop a mechanism for open source and standards-based technology. Develop algorithms and software for data mangement and compression.
- Help stakeholders design best practices.
- Create a smart grid and advise on best practices for integrating new technologies. For example, if a million hybrids are connected to the grid, what IT infrastructure is needed, how do we meter and monetize grid use, etc.? Also, develop global international standards for the smart grid all the way from the home to communication needs architecture with PMUs.
- Work with stakeholders to determine security options (wireless, fiber, PLC, etc.) for AMI and how it will be defined for thousands of entry points. Utilities have the ability to build backbones for these, but security will remain a challenge.
- Assist with demand response/direct load control technologies for integrating incoming data (at five minute intervals).
- Create tools/forums for CIOs that will help them address budget constants.
- Help develop a common information model (CIM) so that systems handling very high volumes and frequency of data will communicate securely and seamlessly. This will require a middleware layer to pass data heterogeneously.
- Develops pilot programs using emerging technologies (e.g., virtual training platforms).
- Develop IT courses in non-IT executives.
- Increase partnership roles that address sustainability trends (e.g., partnering with IBM's Green IT Initiative). Similarly, partner with NERC, the Nuclear Energy Institute (NEI), and the Nuclear Regulatory Commission (NRC) in the nuclear sector.
- Investigate incentives for collaboration across industry players.

Appendix:

Information Technology in the Electric Utility Industry

Information technology (IT), as defined by the Information Technology Association of America (ITAA), is "the study, design, development, implementation, support or management of computer-based information systems, particularly software applications and computer hardware." IT deals with the use of electronic computers and computer software to convert, store, protect, process, transmit and retrieve information, securely. (Source: Wikipedia)

Recently it has become popular to broaden the term to explicitly include the field of electronic communication so that the abbreviation ICT (Information and Communications Technology) is more frequently used. In this paper, we use the term IT.

The term information technology encompasses many aspects of computing and technology, and the term is more recognizable than ever before. IT includes a variety of disciplines that range from installing applications to designing complex computer networks and information databases. Functions that may be included are:

- Data management
- Computer networking
- Computer engineering
- Software design
- Management information systems
- Systems management or system administration

Data management comprises all the disciplines related to managing data as a valuable resource. The official definition provided by the Data Management Association (DAMA) is that "Data Resource Management is the development and executive of architectures, policies, practices and procedures that properly manage the full data lifecycle needs of an enterprise."

Data management includes analysis, modeling, warehousing, transfer, quality assurance, security and architecture.

Demand Response refers to programs which employ communications with customers so as to either directly control their use of electricity or to send price signals which may cause consumers to alter their demand based on savings they could anticipate.

Computer networking is the engineering discipline concerned with communication between computer systems or devices. Networking, routers, routing protocols, and networking over the public Internet have their specifications defined as part of the Internet Standards Process.

Communicating computer systems constitute a computer network, and these networks generally involve at least two devices capable of being networked, with at least one usually being a computer. The devices can be separated by some distance. Computer networking is often considered part of telecommunications, computer science, information technology, and computer engineering.

A computer network is any set of computers or devices connected to each other. Examples of networks are the Internet, or a small home local area network (LAN) with two computers connected with standard networking cables connecting to a network interface card in each computer. All modem aspects of the Public Switched Telephone Network (PSTN) are computer-controlled, and telephony increasingly runs over the Internet Protocol, although not necessarily the public Internet.

According to the Institute of Electrical and Electronics Engineers (IEEE) Computer Society, **computer engineering** is a discipline that combines elements of both electrical engineering and computer science. Computer engineers are typically electrical engineers that have abandoned power engineering courses in favor of training in the areas of software design and hardware-software integration. Computer engineers are involved in many aspects of computing, from the design of individual microprocessors, personal computers, and supercomputers, to circuit design.

Software design is a process of problem-solving and planning for a software solution. After the purpose and specifications of software is determined, software developers will design or employ designers to develop a plan for a solution. It includes low-level component and algorithm implementation issues as well as the architectural view.

Management Information Systems (MIS) is a general name for the discipline covering the application of people, technologies, and procedures – collectively called information systems – to solve business problems. MIS are distinct from regular information systems in that they are used to analyze other information systems applied in operational activities in the organization.

System management refers to enterprise-wide administration of distributed computer systems. Systems management is strongly influenced by network management initiatives in telecommunications. System management may involve a variety of activities ranging from hardware and software management to system security, storage management, and utilization monitoring.

In what follows we provide a brief tutorial on some of the key enabling technologies:

Storage capacity: As of October 2007, one terabyte of storage may be purchased for $422 USD.[1] Storage capacity has changed dramatically since the 1950s. Anecdotally, while working in St. Louis during 1985-97, a colleague described watching as workers painfully muscled additional kilobytes worth of storage (they reckoned it was under 200kb) through the doorway and down the stairs into the computer room in the basement! IBM delivered its first hard drive on September 13th, 1956. The RAMAC (also known as 'Random Access Method of Accounting and Control') was the size of two refrigerators and weighed a ton. It required a separate air compressor to protect the heads, had pizza-sized platters and was able to store a then whopping 5 megabytes of data. The RAMAC was available to *lease* for $35,000 USD, the equivalent of $254,275 in today's dollars.

25 years later, the first hard drive for personal computers was invented. Using the MFM encoding method, it held a 40MB capacity and 625 KBps data transfer rate. A later version of the

[1] NextTag Comparison Shopping: www.nextag.com/terabyte-drive/search-html

ST506 interface switched to the RLL encoding method, allowing for increased storage capacity and processing speed.

IBM made technological history on August 12, 1981, with the launch of their first personal computer - the IBM 5150. At a cost of $1,565, the 5150 had just 16KB of memory. As recently as the late 1980s, 100MB of hard disk space was considered ample.

When asked about the limitations of the early PC, Tom Standage, the Economist magazine's business editor says: "It's hard to imagine what people used to do with computers in those days because by modern standards they really couldn't do anything."

As a result of these major breakthroughs, the industry has grown from several thousand disk drives per year in the 1950s to over 260 million drives per year in 2003. During this period, the cost of magnetic disk storage has decreased from $2,057 per megabyte in the 1960s to $.005 today.[2]

Additionally, advances in another form of storage, non-volatile memory (NVM), impact the digital camera and other device development. The demand for NVM devices is growing in parallel with the expansion of digital computing and processing beyond desktop computer systems into a greater range of consumer electronics, communications, automotive and industrial products. These products include mobile phones, still and video digital cameras, personal digital assistants (PDAs), portable digital music players, digital video recorders, set-top boxes, telecommunications routers and switches, digital televisions and other electronic systems. Industry analysts estimate that the total Flash memory market including stand-alone and embedded components accounted for over $26 billion in sales in 2006 and is expected to reach $64 billion in 2011.[3]

Network capacity: In September 1940 George Stibitz used a teletype machine to send instructions for a problem set from his Model K at Dartmouth College in New Hampshire to his Complex Number Calculator in New York and received results back by the same means. Linking output systems like teletypes to computers was an interest at the Advanced Research Projects Agency (ARPA) when, in 1962, J.C.R. Licklider was hired and developed a working group he called the "Intergalactic Network", a precursor to the ARPANet.

In 1964, researchers at Dartmouth developed the Dartmouth Time Sharing System for distributed users of large computer systems. The same year, at MIT, a research group supported by General Electric and Bell Labs used a computer (DEC's PDP-8) to route and manage telephone connections.

Throughout the 1960s Leonard Kleinrock, Paul Baran and Donald Davies independently conceptualized and developed network systems which used datagrams or packets that could be used in a packet switched network between computer systems.

The first widely used PSTN switch that used true computer control was the Western Electric 1ESS switch, introduced in 1965.

In 1969 the University of California at Los Angeles, SRI (in Stanford), University of California at Santa Barbara, and the University of Utah were connected as the beginning of the ARPANet

[2] Kroll Ontrack, 2006
[3] Saifun Semiconductors, Dec., 2006

network using 50 kbit/s circuits. Commercial services using X.25, an alternative architecture to the TCP/IP suite, were deployed in 1972.

Computer networks and the technologies needed to connect and communicate through and between them, continue to drive computer hardware, software, and peripherals industries. This expansion is mirrored by growth in the numbers and types of users of networks from the researcher to the home user.

Today, computer networks are the core of modern communication. This boom in communications would not have been possible without the progressively advancing network.

Historically, Local Area Networks (LANs) have featured much higher speeds than Wide Area Networks (WANs). This is not necessarily the case when the WAN technology appears as Metro Ethernet, implemented over optical transmission systems.

The largest and best example of a WAN is the Internet, which is the largest network in the world. The PSTN (Public Switched Telephone Network) also is an extremely large network that is converging to use Internet technologies, although not necessarily through the public Internet.

A Wide Area Network involves communication through the use of a wide range of different technologies. These technologies include Point-to-Point WANs such as Point-to-Point Protocol (PPP) and High-Level Data Link Control (HLDC), Frame Relay, ATM (Asynchronous Transfer Mode) and Sonet (Synchronous Optical Network). The difference between the WAN technologies is based on the switching capabilities they perform and the speed at which sending and receiving bits of information (data) occur.

In order for communication to take place between computers, mediums must be used. These mediums include Protocols, Physical Routers and Ethernet, etc. This is covered by Open Systems Interconnection which comprises all the processes that make information transport possible.

Ethernet is a physical and data link layer technology for local area networks (LANs). Ethernet was invented by engineer Robert Metcalfe. When first widely deployed in the 1980s, Ethernet supported a maximum theoretical data rate of 10 megabits per second (Mbps). Later, Fast Ethernet standards increased this maximum data rate to 100 Mbps. Today, Gigabit Ethernet technology further extends peak performance up to 1000 Mbps.

Higher level network protocols like Internet Protocol (IP) use Ethernet as their transmission medium. Data travels over Ethernet inside protocol units called frames.

The run length of individual Ethernet cables is limited to roughly 100 meters, but Ethernet can be bridged to easily network entire schools or office buildings.

Fast Ethernet supports a maximum data rate of 100 Mbps. It is so named because original Ethernet technology supported only 10 Mbps. Fast Ethernet began to be widely deployed in the mid-1990s as the need for greater LAN performance became critical to universities and businesses.

A key element of Fast Ethernet's success was its ability to coexist with existing network installations. Many network adapters support both traditional and Fast Ethernet. These so-called "10/100" adapters can usually sense the speed of the line automatically and adjust accordingly. Just as Fast Ethernet improved on traditional Ethernet, Gigabit Ethernet improves on Fast Ethernet, offering rates up to 1000 Mbps instead of 100 Mbps.

Gigabit Ethernet is an extension to the family of Ethernet computer networking and communication standards. The Gigabit Ethernet standard supports a theoretical maximum data rate of 1000 Mbps. At one time, it was believed that achieving Gigabit speeds with Ethernet required fiber optic or other special cables. However, Gigabit Ethernet can be implemented on ordinary twisted pair copper cable (specifically, the CAT5e and CAT6 cabling standards).[4]

Operational Systems Digital Network Control

IT has and will play a critical role in ensuring the reliable transmission and distribution of electricity. Electricity's share of total energy in the world is expected to continue to grow, as more efficient and intelligent processes are introduced, such AMR and AMI data streams, demand response, wide-area sensing and management systems for improved performance.

In this sense, the electrical infrastructure is becoming increasingly intertwined with the IT infrastructure that supports it. The technologies support the operational control of electrical networks, ranging from energy management systems (EMS) to remote field devices. Critical systems include those described below.

Energy Management System (EMS): The objective of the EMS is to manage production, purchase, transmission, distribution and sale of electrical energy in the power system at a minimal cost with respect to safety and reliability. Management of the real-time operation of an electric power system is a complex task requiring interaction of human operators, computer systems, communications networks, and real-time data-gathering devices in power plants and substations. An EMS consists of computers, display devices, software, communication channels and remote terminal units that are connected to Remote Terminal Units (RTUs), control actuators, and transducers in power plants and substations. The main tasks it performs have to do with generator control and scheduling, network analysis and operator training. Control of generation requires that the EMS maintain system frequency and tie line flows while economically dispatching each generating unit. Management of the transmission network requires that the EMS monitor up to thousands of telemetered values, estimate the electrical state of the network and inform the operator of the best strategy to handle potential outages that could result in an overload or voltage limit violation. EMSs can have real time two-way communication links between substations, power plants, independent system operators, and other utility EMSs. There are two types of EMS systems. One may control a region or control an area and interface with the bulk power system. Another can be applied at the distribution level (DEMS) – Distribution Energy Management System. The term EMS is also used to refer to building control systems. Building EMSs may be connected to utility systems in the future – potentially through AMI.

Supervisory Control and Data Acquisition (SCADA) System: A SCADA system supports operator control of remote (or local) equipment, such as opening or closing a breaker. A SCADA system provides three critical functions in the operation of an electric power system: data acquisition, supervisory control, and alarm display and control. It consists of one or more computers with appropriate applications software connected by a communications system to a number of RTUs placed at various locations to collect data, perform intelligent control of electrical system devices and report results back to an EMS. SCADAs can also be used for

[4] Wikipedia, 2007

similar applications in natural gas pipeline transmission and distribution applications. A SCADA can have real time communication links with one or EMSs and hundreds of substations.

Remote Terminal Unit (RTU): RTUs are special purpose microprocessor-based computers that contain analog to digital converters (ADC) and digital to analog converters (DAC), digital inputs for status and digital output for control. There are transmission substation RTUs and distribution automation (DA) RTUs. Transmission substation RTUs are deployed at substation and generation facilities where a large number of status and control points are required. DA RTUs are used to control air switches and var compensation capacitor banks (that support voltage) on utility poles, control pad-mounted switches, monitor and automate feeders, monitor and control underground networks and for various uses in smaller distribution substations. RTUs can be configured and interrogated using telecommunication technologies. They can have hundreds of real time communication links with other substations, EMS, and power plants.

Programmable Logic Controller (PLC): PLCs have been used extensively in manufacturing and process industries for many years and are now being used to implement relay and control systems in substations. PLCs have extended I/O systems similar to transmission substation RTUs. The control outputs can be controlled by software residing in the PLC and via remote commands from a SCADA system. The PLC user can make changes in the software without making any major hardware or software changes. In some applications, PLCs with RTU reporting capability may have advantages over conventional RTUs. PLCs are also used in many power plant and refinery applications. They were originally designed for use in discrete applications like coal handling. They are now being used in continuous control applications such as feedwater control. PLCs can have many real time communication links inside and outside substations or plants.

Protective Relays: Protective relays are designed to respond to system faults short circuits. When faults occur, the relays must signal the appropriate circuit breakers to trip and isolate the faulted equipment. Distribution system relaying must coordinate with fuses and reclosures for faults while ignoring cold-load pickup, capacitor bank switching and transformer energization. Transmission line relaying must locate and isolate a fault with sufficient speed to preserve stability, reduce fault damage and minimize the impact on the power system. Certain types of “smart” protective relays can be configured and interrogated using telecommunication technologies.

Automated Meter Reading: Automated meter reading (AMR) is designed to upload residential and/or commercial gas and/or electric meter data. This data can then be automatically downloaded to a PC or other device and transmitted to a central collection point. With this technology, one-way, real-time communication links exist outside the utility infrastructure.

Advanced Metering Infrastructure: Advanced metering infrastructure (AMI) is AMR on steroids. It utilizes two-way communications at wide band width to allow signals to be sent to the consumer to provide information and allow load control and price response.

Plant Distributed Control Systems (DCSs): Plant Distributed Control Systems are plant-wide control systems that can be used for control and/or data acquisition. The input/output (I/O) count can be as high as 20,000 data points or higher. Often, the DCS is used as the plant data highway for communication to/from intelligent field devices, other control systems such as PLCs, RTUs, and even the corporate data network for Enterprise Resource Planning (ERP) applications. The

DCS traditionally has used a proprietary operating system. Newer versions are moving toward open systems such as Windows NT, Sun Solaris, etc. DCS technology has been developed with operating efficiency and user configurability as drivers, rather than system security. Additionally, technologies have been developed that allow remote access, usually via PC, to view and potentially reconfigure the operating parameters.

Field Devices: Examples of field devices are process instrumentation such as pressure and temperature sensor and chemical analyzers. Other standard types of field devices include electric actuators. Intelligent field devices include electronics to enable field configuration, upload of calibration data, etc. These devices can be configured off-line. They also can have real time communication links between plant control systems, maintenance management systems, stand-alone PCs, and other devices inside and outside the facility.

Recognizing the increased interdependence between IT and electricity infrastructures, along with technical and business opportunities, electric power utilities typically own and operate at least parts of their own telecommunications systems which often consist of backbone fiber optic or microwave connecting major substations, with spurs to smaller sites.

The energy industry has historically operated closed, tightly controlled networks. Deregulation and the resulting commercial influences have placed new information sharing demands on the energy industry. Traditional external entities like suppliers, consumers, regulators and even competitors now must have access to segments of the network. The definition of the network must be expanded to include the external wide area network connections for these external entities. This greatly increases the security risk to other functional segments of the internal network that must be protected from external connections. This is true whether a private network or the Internet is used to support the external wide area network.

The external entities already have connections to the Internet and as such the Internet can provide the backbone for the External Wide Area Network. Duplicating this backbone to create a private network requires not only large up front start up costs, but also ongoing maintenance costs and potentially higher individual transaction costs than using the Internet.

Information systems and on-line data processing tools such as the Open Access Same-time Information System (OASIS), which is now in operation over the Internet; and Transfer Capability Evaluation (TRACE) software, which determines the total transfer capability for each transmission path posted on the OASIS network, while taking into account thermal, voltage, and interface limits.

Increased use of electronic automation raises issues regarding adequacy of operational security: (1) reduced personnel at remote sites makes them more vulnerable to hostile threats; (2) interconnection of automation and control systems with public data networks makes them accessible to individuals and organizations, from any world-wide location using an inexpensive computer and a modem; (3) use of networked electronic systems for metering, scheduling, trading or e-commerce imposes numerous financial risks.

Utility telecommunications often include several media and diversified communications networks which in part provide redundancy; these range from dedicated fiber optic cables, digital & analog microwave, and Very Small Aperture Terminal (VSAT) satellite to power line carrier technology as well as the use of multiple address radio, spread spectrum radio, trunked mobile radio, and cellular digital packet data. Security of the cyber and communication networks now used by businesses is fundamental to the reliable operation of the grid; as power systems rely more heavily on computerized communications and control, system security has become increasingly dependent on protecting the integrity of the associated information systems. Part of the problem is that existing control systems, which were originally designed for use with proprietary, stand-alone communications networks, were later connected to the Internet (because of its productivity advantages and lower costs), but without adding the technology needed to make them secure. Communication of critical business information and controlled sharing of that information are essential parts of all business operations and processes.

As the competitive market and the impact of IT grow, information security will become more important. Energy-related industries will have to balance what appear to be mutually exclusive goals of operating system flexibility with the need for security. Key electric energy operational systems depend on real-time communication links both internal and external to the enterprise. The functional diversity of these organizations has resulted in a need for these key systems to be designed with a focus on open systems that are user configurable to enable integration with other systems both internal and external to the enterprise. In many cases, these systems can be reconfigured for security using telecommunication technologies and in nearly all cases the systems dynamically exchange data in real time. Power plant DCS systems produce information necessary for dispatch and control. This requires real-time information flow between the power plant and the utility’s control center, system dispatch center, regulatory authorities, etc. A power plant operating as part of a large wholesale power network may have links to an independent system operator, a power pool, etc. As the generation business moves more and more into market-driven competitive operation, both data integrity and confidentiality will become major concerns for the operating organizations.

Any telecommunication link which is even partially outside the control of the organization owning and operating power plants, SCADA systems or EMSs represents a potentially insecure pathway into business operations and to the grid itself. The interdependency analyses done by most companies during Y2K preparations have both identified these links and the systems vulnerability to their failures. Thus they provide an excellent reference point for a cyber-vulnerability analysis.

While strong centralized control is essential to reliable operations, this requires multiple, high-data-rate, two-way communication links, a powerful central computing facility, and an elaborate operations control center, all of which are especially vulnerable when they are needed most — during serious system stresses or power disruptions. For deeper protection, intelligent distributed control is also required, which would enable parts of the network to remain operational and even automatically reconfigure in the event of local failures or threats of failure.

Distributed control capability is becoming available in next-generation integrated sensors that are equipped with two-way communication capability and support “intelligent agent” functions — not just sensing, but data assessment, adaptive learning, decision making, and actuation as well. The development of Intelligent Electronic Devices (IEDs) that combine sensors, telecommunication units, computers, and actuators will allow highly automated adjustments to be made at many points on the system and protect substantially against cascading failures. The use of distributed intelligent agents also opens the door to the development of a self-healing power grid that responds adaptively to counteract disturbances at the site of their occurrence.

Intelligent sensors will be capable of gathering a wide range of operating data, including time-stamped measurements of voltage, current, frequency, phase angle, and harmonics. This information, which provides input for distributed control, can also be integrated into a real-time system-wide database and coupled to analysis tools that perform dynamic monitoring, state estimation, disturbance analysis, and contingency assessment for the grid as a whole. Unfortunately, simulation-based techniques and mathematical models are presently unable to accurately portray the behavior of interactive networks, whose dynamics can be highly nonlinear. Fine-tuning existing models with real-world input from distributed sensors may offer improvements, but substantial progress will require the formulation of new models.

SCADA and EMS system operations are critically dependent on the telecommunication links that gather data from geographically dispersed sources and transmit operational and control instructions to geographically dispersed facilities. In the North American grid these telecommunications links run the gamut from hardwired private networks to multi-network systems using a combination of private and public networks for both data acquisition and control. Not all of the networks are hardwired. Microwave and satellite communications links are common alternatives in areas where topography and/or distance make wireless more cost effective. At first glance it would seem that a private, hardwired network which is totally within the control of the owner organization is a secure system. However even hardwired private networks will be linked to networks outside the control of the company. Typical outside data sources are bulk power customers, major retail customers, bulk power providers, power pools, independent system operating entities, etc. These connections can offer a multitude of paths into the SCADA and EMS systems. Without proper security design and management, each link is a potential security risk.

Challenges include how to handle network disruptions and delays and manage orbits from the satellite. A major source of complexity is the interdependence of the telecommunication networks and the power grid. Issues range from the highest command and control level to the individual power stations and substations at the middle level, and then to the devices and power equipment at the lowest level.