



North American  
Electric  
Reliability  
Council

## MANAGING THE RELIABILITY RISKS OF INFORMATION TECHNOLOGY DEPENDENCIES

~~~~~

# WHAT THE NORTH AMERICAN ELECTRIC RELIABILITY COUNCIL CAN DO

---

The electric industry is at a crossroads. The industry's electricity supply and delivery systems infrastructure is recognized as the most reliable in the world, in large part due to the voluntary adoption and implementation of reliability rules by the North American Electric Reliability Council (NERC). The recent introduction of wholesale and retail electricity competition and increasing public demand for electricity led utilities to re-evaluate whether this exceptional record of reliability can continue absent a mandatory compliance scheme and new technological investments in electric supply and delivery systems. The industry's response to these and other challenges inevitably promises to increase its already heavy reliance on information technology (IT). Therefore, it is appropriate that NERC recognize IT and physical infrastructure security as equally important to ensuring the reliability of the electricity systems of North America.

### THE ELECTRIC BUSINESS IS BECOMING ELECTRONIC COMMERCE

Managing electric utility operations has never been more challenging. Deregulation has significantly enlarged the wholesale market for generation, and

open access transmission has facilitated the transfer of electricity over greater distances. These changes come at a time when many parts of the North-American transmission system are already operating near their operating limits.

In response to these trends, electric utilities are increasing their already substantial dependence on IT systems. Today, many of the approximately 3,200 electric utilities serving North America depend on IT networks such as supervisory control and data acquisition (SCADA) systems to manage their generation, transmission, and distribution systems. These systems are linked to centralized control centers and business management systems, many of which are also connected to systems outside the utility. Computers play a key role in helping utilities collect information from many thousands of data collection points and issue the control commands needed to maintain reliable, uninterrupted electric service.

Meanwhile, utilities' participation in open markets, as mandated by deregulation, is vastly compounding the size

# What Is Changing?

|                               |   |                                 |
|-------------------------------|---|---------------------------------|
| Manned Facilities Operations  | ➔ | Unmanned Facilities             |
| Remote Monitoring             | ➔ | Automated Monitoring/Control    |
| Local Markets                 | ➔ | Open, Regional/National Markets |
| Local Customer Services       | ➔ | Consolidated Call Centers       |
| Customer Billing Information  | ➔ | Customer Services Information   |
| Heterogeneous Technology      | ➔ | Standardized/Homogeneous        |
| Traditional Electric Services | ➔ | On-line Businesses/E-Commerce   |

and complexity of the electric industry's IT infrastructure. Technologies such as the Internet, virtual private networks, and other types of dedicated networks have been a chief enabler of the exponential growth in wholesale electricity transactions that has occurred over the last few years. Functions, such as pricing, scheduling, bidding, metering, capacity limit notification, utilization and allocation, and settlement, as well as control of generation, transmission, distribution, and demand on the grid itself, are carried out over IT networks. Power marketers, manipulating physical and virtual assets and conducting arbitrage to maximize financial gain, are relying on Internet-based applications such as the Open Access Same-time Information System (OASIS) for access to information and markets.

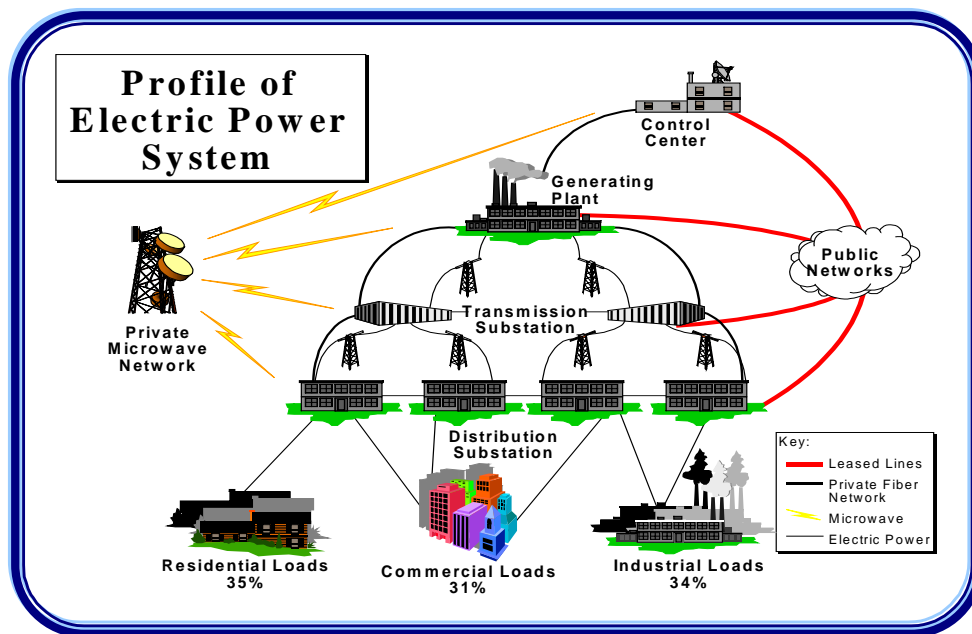
To differentiate themselves in the face of increasing competition, utilities also are using IT in new ways that add value for the customer. Many utilities invested in highly sophisticated, information-intensive, consolidated customer call centers and dispatch centers. Utilities are allowing their employees to access more customer data from a

single computer platform. Customers are being billed, paying bills, and examining their account histories electronically. Like it or not, the electricity business is becoming electronic commerce.

## **The Emerging Operational Risks of IT Dependencies**

In this competitive business environment, electric utilities may feel pressured to minimize investments in areas such as information systems security to keep costs low. However, the explosive increase in the number and interconnectedness of the electricity industry's IT systems exposes utilities to more threats and different kinds and levels of business risks that needs to be carefully managed.

Utilities' operational systems currently may present vulnerabilities that, if exploited, could disrupt the flow of electricity to a large number of customers. Links between utilities' control center systems and their corporate information systems, other utilities, power pools, control areas, vendor support services, and remote maintenance and administration ports offer electronic



intruders multiple points through which to gain access to utility networks. A knowledgeable intruder, aided by publicly available “hacker” tools, could issue false commands to a utility’s energy control systems causing system operators to receive incorrect system status information or causing disturbances on the electricity supply and delivery systems.

The industry is well-prepared to deal with several isolated disruptions. However, a coordinated attempt to penetrate several critical information systems simultaneously may overwhelm industry resources and result in severe outages.<sup>1</sup> Given the heavy dependence of other critical infrastructures (e.g., banking and finance, transportation) on reliable electricity supplies, the degradation of electric system reliability could result in significantly adverse consequences for our national security and economic well being.

Breaches of the confidentiality, integrity, and availability of systems and data used in generation and transmission capacity trading could be equally

harmful, causing market distortions and prompting government intervention or regulation. Regardless of whether these or related occurrences affect the actual generation of electricity and its delivery to the customer, they clearly would foster a public perception of a decline in electric service reliability.

In addition, disruption of the underlying computer and telecommunications systems that support an electric utility’s operations could rupture carefully nurtured customer relationships and public confidence. By corrupting customer service databases, a sophisticated hacker could hamper the timeliness and accuracy of customer billing processes, or obtain sensitive customer information. Consolidation efforts may make customer call centers more vulnerable to denial of service attacks, which can sever important communications between utilities and their customers. Increased regulatory scrutiny, financial penalties, lawsuits, and public embarrassment could ensue, reducing confidence in the industry as a whole.

<sup>1</sup> David Jones and Ronald Skelton, “The Next Generation Threat to Grid Reliability – Data Security,” *IEEE Spectrum* (June 1999): 46–48.

# WHAT CAN NERC AND ITS MEMBERS DO?

As the focal point for the electric industry's reliability and infrastructure protection activities, NERC members have the unique responsibility to meet the new challenges to electric reliability posed by an increased dependence on IT systems. Specifically, NERC can:

- Encourage electric industry support to review current regional and local electronic and physical critical infrastructure protection security measures and implement additional measures, as needed
- Encourage an industrywide policy of sharing security-related experiences and practices to maintain customer and public confidence in the electric industry and to help reduce security-related costs
- Suggest that members ask operations managers within their organizations for regular reports on IT system reliability and security issues
- Encourage members to build on the industry's information sharing process for physical incidents by sharing information about threats to, and vulnerabilities of, its IT systems.

---

Note: This document was developed under the direction and with the participation of electric industry representatives of the Critical Infrastructure Protection Forum of the North American Electric Reliability Council (NERC), supported by staff from the Critical Infrastructure Assurance Office, U. S. Department of Commerce and staff from the U. S. Department of Energy.