Electricity Infrastructure Security

S. Massoud Amin
April 8, 2009

The articles and media reports on our nation's electric power grid "penetrated by spies"[1] bring back memories of the last seven years: In the aftermath of the tragic events of 9/11, when I became responsible for security R&D at EPRI, I received seemingly contradictory piles of reports/files that either claimed that "we are bullet proof" or "the sky is falling."

Without going through sensitive information in this email, it was neither extreme as the broad brush on the whole sector. The truth critically depended on the specifics of the organization's preparedness and security measures that had been put in place.

Background

The North American power network may be considered to be the largest and most complex machine in the world — its transmission lines connect all the electric generation and distribution on the continent. In that respect, it exemplifies many of the complexities of electric power infrastructure and how technological innovation combined with efficient markets and enabling policies can address them. This network represents an enormous investment, including over 15,000 generators in 10,000 power plants, and hundreds of thousands of miles of transmission lines and distribution networks.

The existing power-delivery system is vulnerable to natural disasters and intentional attack. Regarding the latter, a successful terrorist attempt to disrupt the power-delivery system could have adverse effects on national security, the economy, and the lives of every citizen. Secure and reliable operation of the system is fundamental to national and international economy, security and quality of life. Their very interconnectedness makes them more vulnerable to global disruption, initiated locally by material failure, natural calamities, intentional attack, or human error.

This not new-- both the importance and difficulty of protecting power systems have long been recognized. In 1990, the Office of Technology Assessment (OTA) of the U.S. Congress issued a detailed report, *Physical Vulnerability of the Electric System to Natural Disasters and Sabotage,* concluding: "Terrorists could emulate acts of sabotage in several other countries and destroy critical [power system] components, incapacitating large segments of a transmission network for months. Some of these components are vulnerable to saboteurs with explosives or just high-powered rifles." The report also documented the potential cost of widespread outages, estimating them to be in the range of $1 to $5/kWh of disrupted service, depending on the length of outage, the types of customers affected, and a variety of other factors. In the New York City outage of 1977, for example, damage from looting and arson alone totaled about $155 million—roughly half of the total cost.

During the twenty years since the OTA report, the situation has become even more complex. Accounting for all critical assets includes thousand of transformer, line reactors, series capacitors, and transmission lines. Protection of ALL the widely diverse and dispersed assets is impractical because there are so many assets involved. In addition, cyber, communication, and control layers add new benefits only *if architected correctly and securely*, and new challenges.

---

[1] Electricity Grid in U.S. Penetrated By Spies, by Siobhan Gorman**,** WSJ (Eastern edition). N.Y.: Apr 8, 2009, page A.1 (online at http://online.wsj.com/article/SB123914805204099085.html). In this particular case, the electricity industry immediately had a conference call with DHS and they determined that there were no events known to either that would have precipitated this WSJ article. The article may have been timed to correspond to the hearing yesterday of a bill that would have created a "Cyber Czar" in the White House. In the days ahead there will be related conference calls to further discuss frustrations at the lack of industry responsiveness.

Electricity Infrastructure: Interdependencies with Cyber and Digital Infrastructures[2]

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. Increased use of electronic automation raises significant issues regarding the adequacy of operational security, if security provisions are not built in

Security of cyber and communication networks 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, standalone communication 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.

In addition, some trends show that worldwide cyber attacks are on the rise; the number of documented attacks and intrusions has been rising very rapidly in recent years. Due to the increasingly sophisticated nature and speed of some malicious code, intrusions, and denial-of-service attacks, human response may be inadequate.

Any telecommunication link that is even partially outside the control of the organization that owns and operates power plants, SCADA systems, or EMSs represents a potentially insecure pathway into the business operations of the company as well as a threat to the grid itself. The interdependency analyses done by most companies in the last 10 years (starting with preparations for Y2K, and after the tragic events of 9/11) have identified these links and the system's vulnerability to their failures. Thus they provide an excellent reference point for a cyber-vulnerability analysis.

Like any complex dynamic infrastructure system, the electricity grid has many layers and is vulnerable to many different types of disturbances. 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 operation-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 secure 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.

I have presented non-sensitive material on this key issue for over a decade. Most recently on Thursday, 26 March, 2009, I spoke at the U.S. Congressional Research and Development [R&D] Caucus, on the Smart Grid briefing that ASME and IEEE-USA convened. I highlighted cyber security as one of the key challenges, and asked for the design of a smart grid would include "security built-in as part of its design and NOT glued on as afterthought," to solving the cyber security question (www.researchcaucus.org).

Regarding today's cyber threat reports, it is fundamental to separate "hype" from the truth; what concerns me about such reports is mainly one piece in an earlier article: "The response to the alert was mixed. An audit of 30 utility companies that received the alert showed only seven were in full compliance, although all of the audited companies had taken some precautions."

That is the reality that needs to be addressed.

---

[2] As we network our entire lifestyle, including critical infrastructures, the question of security becomes increasingly important, as it is also a matter of public good and economic security. Additional pertinent material is available from the sidebar at the left-hand column of http://umn.edu/~amin