Executive Summary

The electric power industry is one of the most crucial national infrastructure sectors. It encompasses sensitive potential targets and underlies the smooth operation of all other infrastructures. Despite widespread backup and continuity of operations resources and procedures, if the electric power sector were to suffer sustained outages, communications could be seriously disrupted, trains could stop running, planes could be grounded, and the economy could grind to a halt. Unlike other energy sources, electricity cannot be stockpiled, so power disruptions would have almost immediate effects.

The sector has always contained security vulnerabilities, but these vulnerabilities have been compounded by the introduction of new networking technologies, deregulation and structural changes in the industry. Additional vulnerabilities have been introduced by placing ever-more energy management and control systems online, opening them up to remote access and linking them to corporate networks. The outcome of these developments is that energy management systems (EMS) and supervisory control and data acquisition (SCADA) systems that manage and control transmission and delivery of electric power, and distributed control systems (DCS) and programmable logic controllers (PLCs) that control the production of electricity, are vulnerable to malicious attacks or other cyber impacts. Some operators have introduced effective security measures to address vulnerabilities in IT systems that link to control systems, but technologies are not available to secure the control systems themselves. Control system communication protocols also remain vulnerable. Penetration tests and vulnerability assessments conducted by Department of Energy (DOE) laboratories and security firms have demonstrated the cyber vulnerabilities of energy industry control systems and related information networks. As the same DCS, SCADA and PLC technologies and associated standards are used around the world, specialized knowledge about these systems is widely dispersed and available.

There have been dozens of cases where control systems – in the electric power, water, waste-water, oil, gas, and paper industries – have been intentionally or unintentionally impacted by electronic means, according to operators and industry experts. Moreover, online attackers are targeting power companies’ information systems that could be used as entranceways into the actual control systems. All this information clearly shows that the electric energy sector is vulnerable to cyber impacts, and indications are that terrorists, hostile nation-states or malicious computer hackers pose a threat to the sector.

It is unclear what consequences could ensue from a cyber attack against control systems in the electric energy sector. As has been shown by accidents or errors, causing small local or regional outages or disruptions is relatively easy to achieve and could undoubtedly be done by skilled cyber attackers. More coordinated attacks against regional power networks are also possible in light of current vulnerabilities, but would require a certain level of planning and specialized knowledge. Attacks that in some way disrupt the national power grid appear possible, but too little information is currently available to accurately assess the potential impact of cyber attacks on the national grid. Therefore, it is imperative to support and expand testing and research in this area.
Table of Contents

**Executive Summary**.......................................................................................................... 1

**Table of Contents** ..............................................................................................................2

**Introduction**....................................................................................................................... 3

**The Electric Energy Sector** ................................................................................................4

**Deregulation / Structural Changes in the Sector** ............................................................... 5

**Vulnerabilities** .................................................................................................................... 6

  - Management and Control Systems are Inherently Insecure ........................................... 6
  - Remote Access .................................................................................................................. 7
  - Proprietary Software ....................................................................................................... 7
  - Access Through Corporate Networks ............................................................................. 7
  - Control System Procedures ............................................................................................. 8
  - Communication Failures ................................................................................................. 8

**Threats** ................................................................................................................................... 10

  - Hostile nation-states ..................................................................................................... 11
  - Cyberterrorists .............................................................................................................. 11
  - Hackers .......................................................................................................................... 11
  - Insiders ........................................................................................................................... 12

**Potential Consequences** .................................................................................................... 12

**Protective Measures** ......................................................................................................... 13

**Conclusions** ....................................................................................................................... 16

**Additional Resources** ....................................................................................................... 17

  - Reports .......................................................................................................................... 17
  - Media Articles .............................................................................................................. 18
Introduction

This paper analyzes the vulnerabilities and threats facing the electric energy infrastructure, placing primary emphasis on the cyber vulnerabilities associated with control systems and related information systems and networks. Physical vulnerabilities and threats are touched upon briefly, but exceed the scope of this examination.

The analysis provides a general overview of the electric energy sector, describing key assets, systems and functions. The report provides an analysis of direct and indirect control system vulnerabilities, and offers examples of specific security flaws. Further, it explains how deregulation and subsequent structural changes in the industry have affected the vulnerability of control systems. Moreover, the paper offers fact-based analysis of potential threats to the sector and the likely consequences should an attack occur. It also suggests protective measures, ranging from industry regulations and best practices to specific security measures.

Authors of this report:

Eric Goetz (egoetz@ists.dartmouth.edu)
Research Analyst, IRIA

Input and assistance received from George Bakos, Eric Byres, Trey Gannon, Robert Gray, Dion Stempfley, and Joseph Weiss.
The Electric Energy Sector

The national power grid is highly interconnected and dynamic, consisting of over 3,200 public and private utilities, rural cooperatives and trading companies. It is sub-divided into regional grids. The sector is further split into generation, transmission, delivery and customer service systems, supplemented with an energy trading system. “The goal of the modern-day power systems is to generate and deliver electric energy to customers as reliably, economically, and safely as possible while maintaining the important operating parameters (voltage, frequency, and phase angles) within permissible limits.”

At the provider level, companies have EMS and SCADA systems, as well as DCSs and PLCs to monitor and control various aspects of power generation, transmission and delivery. These management and control systems are key to the functioning of the electric energy sector. They house the utility’s systems’ databases, the operational applications and displays, and the power system report-generation function. They are used to collect the electric system data from the field, initiate alarms to operations personnel, and issue control commands to substation, plant controllers and field devices. A SCADA system typically consists of a master computer, one or more remote data-gathering and control units, up to 100,000 data collection points in the field, and a mixture of standard and/or custom software used to monitor and control remote field data elements. SCADA systems can transmit analog or digital system status information and are also used to remotely issue operational control signals, such as opening or closing switches on the power transmission and distribution grid.

The electric energy sector is comprised of myriad assets, which can be summarized under the following main headings:

- **Generation Plants** – the electric energy sector has a variety of generating facilities that draw energy from different sources. Hydroelectric power, fossil fuels and nuclear energy are utilized in different percentages around the country. Most regions, or large energy providers, offer a mixture of these generating plants.

- **Transmission Lines** – these lines are used to transport electric power from the generation plants to transmission and distribution substations at voltages from 69,000 to 765,000 volts.

- **Transmission and Distribution Substations** – these play a key role in the sector as they are used to convert energy from the high voltages used during transmission to lower voltages required for delivery.

- **Local and Regional Control Centers** – these control centers house an energy provider’s energy management and control systems. They monitor control data from remote terminal units (RTUs) and substation SCADA systems to ensure that the power system is functioning properly. Control centers also dispatch remote control messages – either by operators or automatically - to power plants and

---

1 For a map of North American Electric Reliability Council (NERC) regions and subregions see [http://www.eia.doe.gov/cneaf/electricity/chg_str_fuel/html/fig02.html](http://www.eia.doe.gov/cneaf/electricity/chg_str_fuel/html/fig02.html)

substations, and other points of the generation or transmission system to regulate the production and flow of power.

- **Remote Terminal Units (RTUs) / Intelligent Electronic Devices (IEDs)** – RTUs collect data from sensors in the field and convey them to EMS and SCADA systems. IEDs are devices incorporating one or more processors with the capability to receive or send data/control from or to an external source (e.g. electronic multifunctioning meters, digital relays, and controllers). These devices are used to implement control and management commands remotely. Newer versions are often IP (Internet Protocol) –enabled, meaning that they can be placed on the Internet.

- **Communications Links** – Energy firms make use of a variety of communication methods, including fiber optic cables, wireless technologies, radio, microwave and satellite links, and the Internet to link assets and disseminate management and control commands. Most energy companies have dedicated communications links to management and control systems, but commercial communications networks, like the wireline telephone systems, are also utilized.

### Deregulation / Structural Changes in the Sector

A flurry of legislation in the 1990s has led to a significant measure of deregulation in the electric energy sector. These new laws resulted in structural changes in the power sector that introduced additional cyber vulnerabilities by opening up the system to insiders and external entities.

Before deregulation, power companies were vertically integrated regional monopolies with state agencies regulating prices to ensure a guaranteed rate of return. Single companies handled all aspects of the energy business. Deregulation has forced some energy sector monopolies to split up into power generation, transmission, delivery and revenue collection/customer service branches, and has allowed new players to enter the market. Generated energy must be purchased in the open market, and the required spinning reserves have dropped from 20-30% to 10-15%. Automated control systems now exist for generation, transmission and delivery.

Market consolidation and flexible energy trading has resulted in the introduction of more vulnerabilities. To cut costs, knowledgeable employees are being released and remaining employees are forced to take on additional responsibilities. In some cases, control system operators are no longer on-site or need access when not on-site, leading to a need for more remote access to these systems and more links between control systems and corporate networks. Further, deregulation and expansion into new lines of business often requires the integration of legacy systems from different organizations. This presents new information security challenges.

---

3 The 1992 Energy Policy Act (EPAC) and the 1996 Electric Consumers’ Power to Choose Act were crucial legislative milestones in the deregulation of the electric power sector.
Vulnerabilities

The physical vulnerabilities that exist in the electric energy industry have been dealt with elsewhere and exceed the scope of this examination. Instead, this report focuses on the cyber vulnerabilities of control systems and related information systems and networks. A number of misconceptions still shape the perception of vulnerability in the sector. Contrary to some beliefs, control systems are vulnerable to cyber attacks – both directly and indirectly through security flaws in related information systems and networks. Some operators have put security measures in place in the past few years to address known IT flaws, but the control systems themselves remain vulnerable. The following are the general areas of greatest concern:

Management and Control Systems are Inherently Insecure

Control systems were not developed with security in mind. Real-time operating systems have no encryption and little authentication; most control systems have no intrusion detection capabilities, and control system communication protocols (ICCP/CIM/DNP3/Modbus/Profibus) have been designed to be open.4 Implementing security on these systems could result in unacceptable service degradation. For example, encrypting communications to real-time systems might cause unacceptable delays. Further, existing hardware devices might not have the memory or processor capabilities to support encryption, and existing communications infrastructures may not have the bandwidth to support link level encryption. Security tools have not been developed for addressing control systems, thereby minimizing the cyber protection of control systems. A key cyber security problem for control systems is the lack of secure real-time operating systems at the control processor level.5

---

4 Some implementations of anomaly and sand trap type IDS systems have been deployed in SCADA environments, but sophisticated signature-based IDSs are currently not possible because actual attacks to model the IDS against are not being monitored.

5 It should be noted that even if a secure real-time operating system at the control processor level were developed, the applications and protocols that are written on top of the OS would remain vulnerable. Similarly, if the applications and protocols were secured, but a security subsystem with a protected security kernel were still lacking, control systems would remain at risk. Both areas need to be secured with appropriate procedures and technologies.
Remote Access
Control systems used to be isolated so there was minimal need for cyber security. This is no longer the case. For business reasons, control systems increasingly use remote access for operators, vendors and other entities (e.g. other utility control centers, regional power pools, independent system operators etc). Remote access includes a variety of direct or indirect links to RTUs, substations, power plants, and control centers. Remote links to control systems are not encrypted and have minimal electronic authentication capabilities. Additionally, control system equipment suppliers often install a remote access capability without the responsible utility security authority being aware. This could include suppliers providing their own firewalls for their VPN connections.

Proprietary Software
Energy management and control systems used to utilize proprietary operating systems. The operator interface for newer systems is often Windows- or Unix-based, thereby introducing known vulnerabilities for attackers to exploit. Much of the new SCADA software runs on Microsoft Windows operating systems (OSs). Flaws in these systems, which are plentiful, expose the SCADA software to attacks. Other platforms like Unix and real-time OSs, such as QNX, RTX or VxWorks, are still commonly used, but do not include security policies in their kernels. The general trend for energy management and control systems is a move away from proprietary software at the man-machine interface to commercial off-the-shelf solutions.

Access Through Corporate Networks
Control systems are advertently or inadvertently being linked to corporate networks to provide business units with real-time operational data or to speed up or automate other processes, such as customer service, power and outage management, and supply procurement. Corporate networks remain highly vulnerable to intrusions and systems compromises at the application or network levels. There are often multiple connections between corporate networks and control centers, or directly to management and control systems and devices. Administrators and operators are often not aware of these links, and there is sometimes little or no security to protect them. Following the traditional information warfare model, an attacker with time and resources could use a minor vulnerability in the corporate network to expand the attack until he was able to take control of energy management or control systems. With access to the corporate network, the attacker could gather information about the network, harvest passwords and test vulnerable control systems links without being detected, especially since there are few power plants or substations with firewalls or IDS. The bottom line is that if an attacker is...

6 There are multiple potential ways for a cyber attacker to gain access to energy management and control systems through the corporate network. Each operator’s systems are different and the level of security varies significantly between energy firms. Often, security tools, such as firewalls or authentication systems, are in place to protect IT systems (not operational control systems), but are misconfigured leaving security holes. Some examples of these vulnerabilities include: links between historical and modeling databases and control systems; allowing web browsing from control systems; vulnerable corporate workstations have direct access to control systems; allowing control systems administrators to check their e-mail from their workstations, etc.
able to gain unauthorized access to an energy firm’s corporate network, he is usually able to take control of or manipulate the control systems.

**Control System Procedures**

Cyber security procedures do not exist from factory check-out to field implementation of control systems. Existing IT security procedures do not address control systems’ unique characteristics and prescribe actions that could inhibit control system security and/or performance. Therefore, it is necessary to have security procedures for IT and control systems (and environments where these may overlap).

**Communication Failures**

A gulf exists between an energy company’s corporate IT security staff and control system engineers and operators. This introduces vulnerabilities. Both groups know too little about each other’s systems, configurations, tasks and needs, as well as the connections between management and control systems and corporate networks. Compartmentalized security responsibilities in this area leave systems unprotected. As demonstrated by recent security assessments, lack of communication within the operational organizations can also leave control systems at risk.

The following specific cyber vulnerabilities also affect electric energy management and control systems:

- Substations and power plants are particularly vulnerable to cyber attacks because automated monitoring and control devices in power plants and transmission and distribution substations are poorly protected. Remote access to these systems (dial-in modems, pcAnywhere\textsuperscript{TM}, ftp and Internet) is often allowed by the power plant or substation staff. RTUs and IEDs at substations serve as automated, remotely programmable, breakers, switches, relays, and transformer tap changers. Vulnerabilities could result in switches or relays being changed, denial of service to these devices or even physical damage to hardware. Unauthorized access to power plant control systems could result in changes to valves, motors, or pumps, potentially causing physical damage to the plant or regulatory compliance issues.

- Poor authentication and access control measures for remote access to management and control systems is a further problem, especially as maintenance of EMS and control systems is increasingly outsourced. Some systems use default vendor passwords (sometimes burned into the firmware) or have no additional safety measures in place. Passwords are generally a problem. Too often, weak passwords or a single password for various control system are used.\textsuperscript{7} In addition, control system passwords are sometimes stored with little or no protection on the corporate network.

- Host machines in the control center that control SCADA systems (or DCSs in power plants) - using Xwindows software or ActiveX controls for display, for instance – are vulnerable to cyber attacks. Windows-based X servers are usually

\textsuperscript{7} It should be noted that the use of strong passwords may be impractical to implement in some operational environments, such as at substations or power plants, because transient conditions requiring immediate operator response could be impaired.
open by default, potentially giving an attacker the same level of control as an operator sitting at the console.

- Direct dial-in connections are often allowed to RTUs and control, monitoring and diagnostic devices for employees and vendors. This circumvents existing security measures. These connections are used for troubleshooting, performing system administration functions and operating some EMS and control system applications. They provide a further avenue of attack for electronic intruders.

- Built-in system safeguards could be manipulated on energy management and control systems. For instance, circuit breakers on the power distribution grid are electronically controlled and could be manipulated to shut off circuits when there is no danger, or security settings could be revised to higher tolerance levels resulting in damage to equipment. This could make recovery after an attack more difficult and time consuming.

- Communications systems used by energy providers to send control signals are also vulnerable to attack. Severing the lines could disrupt signals on designated wired lines. Other wireline and wireless signals could be jammed or manipulated through cyber attacks. Most communication systems do not utilize point-to-point encryption, potentially allowing for spoofed control signals, as well as denial of service attacks against substations or other targets. Such attacks alone would not normally endanger the reliability of the power supply, but could be problematic in combination with other attacks on power management and control systems.

- Control system communication protocols are insecure. Newer protocols, such as DNP3 and ICCP, are not difficult to understand. Protocol analyzers are commonly available, and could be used by unauthorized individuals to change control settings or initiate control actions. Consequently, ‘security through obscurity’ is not a viable security option in this context.

Penetration tests and vulnerability assessments of control systems and related information systems have repeatedly shown that energy management and control systems are vulnerable to online attacks – unauthorized intrusions, misinformation and denial of service attacks. In fact, these security assessments have been successful in compromising control systems most of the time, according to the security firms that conduct these tests. Similar penetration tests and security audits by the Department of Energy (DOE) also found SCADA and DCS systems vulnerable. Most of the time, penetration tests and vulnerability assessments were able to exploit flaws – both in the management and control systems themselves, or in corporate networks that link to these systems – that security personnel and operators had no idea existed, or believed were sufficiently protected. Moreover, a lack of real-time monitoring of management and control systems results in intrusions or attacks being detected after the fact, preventing active defensive measures.

There are only a handful of major vendors that produce SCADA, DCS and PLC systems. The same technologies (hardware and software) and associated training are used around the world, including in countries hostile to the United States or where terrorists or

---

8 ‘Hackers Target Energy Industry’, Charles Piller, Los Angeles Times, July 8, 2002
terrorist sympathizers reside. Furthermore, considerable information on operating and programming these devices is freely accessible on the Internet. Therefore, specialized knowledge of these systems – and the vulnerabilities they contain - is widely dispersed and available.

It should be noted that storms, accident and errors currently cause most power outages.\(^9\) While the electric energy sector remains vulnerable to such occurrences, it also has ample experience in recovering from such events. In addition, storms, accidents or errors are unlikely to lead to more than local or regional disruptions. However, these events cause stress on the system and could be used as a cover to launch attacks that utility repair crews would be unprepared for and hard pressed to handle.

**Threats**

Terrorists and hostile nation-states pose a realistic threat to the electric energy sector. In 1997 the President's National Security Telecommunications Advisory Committee’s Information Assurance Task Force determined that “Physical destruction is still the greatest threat facing the electric power infrastructure.”\(^10\) This probably still holds true as it is in accordance with known terrorist tactics, and high-yield targets in the sector lend themselves to physical assault. These physical threats could take any number of forms, which have been dealt with elsewhere\(^11\) and exceed the scope of this investigation.

That said, cyber threats are mounting – especially if viewed in the context of compound attacks combining physical and cyber strikes. Cyber attacks now pose a serious threat to energy management and control systems. Hacking and cyber attack techniques are constantly evolving and growing in sophistication. Many attack tools have become automated and some of these tools have been demonstrated to impact control systems. In addition, a sharp rise in the number of cyber vulnerabilities has been documented in the past two or three years that could facilitate indirect attacks against control systems via related information networks.

Specific hacking and intrusion data from the electric energy sector – both concerning control systems and business systems - is hard to come by due to power companies’ understandable reluctance to share such potentially damaging information.\(^12\) Further,

\(^9\) According to NERC, 28 of 58 system disturbances reported to NERC and the DOE in 2000 were related to bad weather, twelve were linked to “personnel related actions”, and ten were caused by equipment failure. ‘2000 System Disturbances – Review of Selected Electric System Disturbances in North America’, North American Electric Reliability Council, September 2001, P. 5


\(^12\) The much-publicized hack in May 2001 against California Independent System Operator (Cal-ISO) has been mentioned as a cyber attack against the U.S. infrastructure. While worrying, the attack affected a ‘test network’, not the power grid or the power distribution network. See ‘California Power Grid Hack Overshadows Threat to U.S.’, Robyn Weisman, NewsFactor, June 13, 2001. The following research paper gives examples of mainly unintentional cyber impacts in the pulp and paper industry: ‘Protect That
when events with cyber implications have occurred, the government has been slow to release findings to the private sector.\textsuperscript{13} However, recent reports highlight that attacks against the electric power sector’s business systems are on the rise.\textsuperscript{14}

Cyber threats could come from the following groups:

**Hostile nation-states**
Upward of 20 countries are believed to be actively developing cyberwarfare capabilities.\textsuperscript{15} This number will likely grow in an age of asymmetric conflicts. These states have the resources, capabilities, and knowledge of management and control systems necessary to pose the most serious threat to the electric energy sector.

**Cyberterrorists**
There has been no known/publicized example of cyberterrorism to date, according to strict definitions of that term. However, terrorist groups are undoubtedly developing IT skills, which have so far been put to use to communicate securely, recruit new members, gather information on potential targets (including electric power assets and energy management and control systems), and spread propaganda. According to the Washington Post, government officials assume that terrorist groups are developing cyber attack capabilities,\textsuperscript{16} perhaps aided by nation-states that share their beliefs and goals. These capabilities could be used in cyber attacks against the power grid.

**Hackers**
Hackers come in many shades. The large majority of teenage hackers, or script kiddies, are not a threat to the electric energy sector because their skills and specialized knowledge are insufficient to cause significant damage. A small group of technically cognizant hackers with detailed knowledge of energy systems and networks, and experience in network penetrations and unauthorized intrusions, pose a real threat to energy systems. Such an elite hacker in the paid service of a terrorist group or hostile nation-state could cause disruptions to management and control systems. A small number of hacktivists from environmental groups or with an anti-capitalist agenda may also have the motivation and skills to disrupt power operations.

\textsuperscript{13} The Bellingham, WA, oil pipeline rupture is a good example of this. The National Transportation Safety Board took two years to release its findings that showed that development work on the SCADA system that was being used to operate the pipeline contributed to the disaster. See ‘Pipeline Rupture and Subsequent Fire in Belligham, Washington, June 10, 1999’, NTSB Number PAR-02/02 NTIS Number PB2002-916502.

\textsuperscript{14} A recent Internet threat assessment report by Riptech found that the number of ‘severe’ and ‘highly aggressive’ cyber attacks against power and energy companies’ business systems (not operational systems) is higher than attacks against other sectors, and has risen significantly in 2002. ‘Riptech Internet Security Threat Report – Attack Trends for Q1 and Q2 2002’, Riptech Inc., July 2002. It should be noted that, since most power plants and substations have no firewalls or intrusion detection capabilities, it is impossible to know whether control systems are being attacked.


\textsuperscript{16} ‘Cyber Attacks by Al Qaeda Feared’, Barton Gellman, Washington Post, June 27, 2002
Insiders
Disgruntled or ex-employees with technical knowledge of control systems could also jeopardize the smooth functioning of energy systems.\(^{17}\) However, as the same EMS and SCADA technologies are used worldwide, ‘insider’ knowledge of management and control systems is widely dispersed and available.

Potential Consequences

Vulnerabilities and threats clearly exist. The real difficulty is understanding what consequences could ensue from an attack against control systems in the electric energy sector. No definitive answer is possible at present. Accidents or errors have shown that causing small local or regional outages or disruptions is relatively easy.\(^{18}\) Cyber attackers could achieve similar results by taking out one or several RTUs, attacking SCADA systems in substations or other locations, or attacking individual power plant DCSs. This would not be too hard to do, but would probably have little impact on the power grid as a whole. Further, unless the attack caused physical damage to hardware (which is possible), recovery could be achieved rapidly, assuming that the attack or intrusion was detected. Since most power plants and substations have no firewalls or intrusion detection systems (at the control system level), a cyber intruder could manipulate control systems or procedures precluding early recovery. A Trojan horse or other malware could also be installed to complicate recovery efforts.

There is the potential for regional power outages, and these have happened in the past.\(^{19}\) In 1997 a majority of utilities questioned by the NSTAC’s Information Assurance Task Force admitted “that an electronic attack capable of causing regional or widespread disruption lasting in excess of 24 hours is technically feasible.”\(^{20}\) Since then, both the vulnerability of control systems and the online threats against them have risen. There are a number of ways that multiple power plants or substations could be simultaneously attacked using cyber means that could lead to significant regional impacts. Additionally,

\(^{17}\) In April 2000, an Australian man hacked into the Maroochy Shire, Queensland, computerized waste management system and caused millions of liters of raw sewage to spill into local parks and rivers. The man had insider knowledge of the system. See ‘Hacker jailed for revenge sewage attacks’, Tony Smith, The Register, October 31, 2001.

\(^{18}\) On May 14, 1996, an improper setting on a high-voltage circuit breaker at a single substation resulted in an 8-hour blackout affecting 290,000 customers through southern Delaware and across the eastern shores of Maryland and Virginia. This relatively minor outage is estimated to have cost local businesses as much as $30.8 million. ‘Electric Power Information Assurance Risk Assessment’, Op. Cit.,

\(^{19}\) The largest instance of a sustained regional power outage occurred on November 9, 1965 and knocked out power in eight U.S. states and Canada for up to 13 hours. However, smaller regional power outages have affected hundreds of thousands of people on various occasions since 1996. For examples of recent power outages and their effects see ‘Report of the U.S. Department of Energy’s Power Outage Study Team – Findings and Recommendations to Enhance Reliability from the Summer of 1999’, March 2000. A report by the President’s Commission on Critical Infrastructure Protection found that Western power outages in August 1996 cost consumers several billion dollars, clearly showing that economic costs of infrastructure attacks should also be taken into consideration. ‘Economic Impacts of Infrastructure Failures’, Report to the President’s Commission on Critical Infrastructure Protection, 1997

targeting the cyber vulnerabilities of a single key SCADA or DCS supplier could cause nationwide problems. It is hard to gauge the risk of outages that would affect the national grid, although regional events could lead to cascading national impacts. National-level impacts would probably require significant planning and reconnaissance activities and a large-scale coordinated attack. However, too little information is currently available to accurately assess the potential impact of cyber attacks on the national grid.

Protective Measures

Protecting electric energy infrastructures has become a high-priority national issue. Although “Industry-wide or market-driven standards are almost always reactive,”21 there is a real opportunity to implement effective security procedures and measures in the electric power sector before a large-scale attack occurs. Officials from the Federal Energy Regulatory Commission (FERC) are holding talks with energy operators and other experts to develop mandatory security standards for any organization that participates in the electric energy marketplace. The FERC standards, which are expected to take force on January 1, 2004, prescribe minimum security measures for physical and cyber security of “the operational infrastructure of monitoring, dispatch and market software and systems.”22 The FERC standards and vulnerability assessment and security guidelines developed by the DOE’s Office of Energy Assurance have helped shape the following recommendations.23 However, they have been supplemented by additional recommendations and revised to reflect the specific requirements of control system security.

Before security measures can be implemented, energy companies must first assess their vulnerability, develop a security strategy and establish security policies. A crucial step in this process is to conduct security audits and vulnerability assessments of electric power grid systems. This includes management and control systems AND an energy firm’s business systems, as well as the linkages between them. These tests should be repeated periodically to ensure that new technologies or practices have not created additional vulnerabilities, or that employees are implementing security policies. At the national level, the Office of Energy Assurance, in cooperation with other official bodies, is conducting a vulnerability assessment to understand vulnerabilities and threats affecting the power grid as a whole.

It is also important to keep up-to-date with the latest vulnerabilities and threats. IT vulnerability and threat information is currently shared through the energy-ISAC

22 ‘Security Standards for Electric Market Participants – Draft Version’, FERC, July 24, 2002 and ‘Cyber Security Standards for Electric Wholesale Market Operations Participants – Appendix G - Final CIPAG comments of Security Sections of FERC SMD NOPR’, November 7, 2002. While the cyber security standards are scheduled to take effect on January 1, 2004, complete compliance is not expected until January 1, 2005 for budgetary reasons. It should also be noted that all references to power plant and substation control systems were removed from the latest NERC CIPAG recommendations.
Control system cyber vulnerabilities and intrusions have not been formally captured or shared. It would be beneficial to create a center for collecting information on control system cyber security vulnerabilities and events across all industries that would be an information resource for all applicable ISACs.

Once an understanding of vulnerabilities and threats has been attained, energy firms should create a secure network architecture. This should go hand-in-hand with developing, implementing and enforcing sensible security policies, and providing management and control system operators and all users of potentially vulnerable systems with training and awareness programs. Education programs should make business units aware of how their decisions may introduce vulnerabilities into management and control system. For instance, linking the control center to the corporate network to obtain timely system data could inadvertently open control systems to online attacks. IT security personnel and control system operators should also be brought together to allow them to understand each other’s needs and problems. This would enhance an understanding of interconnections between the two areas, as well as interconnections and interdependencies within the control systems.

Background checks should be conducted for all employees and contractors with access to energy management and control systems and other critical assets. This should apply to new hires and existing employees. Background checks should be repeated at intervals, depending on the level of access the employee has.

To secure energy management and control systems, the following key recommendations should be considered:

- Establish a security perimeter that includes all remote access points and defend the critical physical and cyber assets within this perimeter. This should include protection for all entry and exit points for personnel, supplies or communications, and stipulate requirements for access controls.
- Minimize and secure remote connections to control networks – only absolutely necessary remote connections to management and control systems and networks should be allowed for monitoring and control functions, as well as maintenance. All other remote links should be disabled. The remote connections that are required to maintain the smooth operation of the system should be secured using encrypted communication links and strong authentication measures.
- Minimize and secure links between corporate networks and control systems – too many connections currently exist between corporate networks and management and control systems. These links are often poorly understood, ignored or not

---

24 It should be noted that the British Columbia Institute of Technology’s (BCIT) Internet Engineering Lab (IEL) has established an Industrial Security Incident Database to track incidents of a cyber security nature that directly affect industrial control systems and processes. This includes events such as accidental impacts, external hacks, DoS attacks, etc. Data is collected by both research into publicly known incidents and private reporting. The database currently contains approximately 40 incidents, and access to the information can be obtained by contributing an incident or paying a subscription fee.

25 The NERC CIPAG Process Controls Self-Directed Working Group is developing security requirements and procedures for control systems, including remote access.
protected. Unnecessary connections should be severed and the rest should be secured using firewalls, intrusion detection systems and other security tools. Having some links between corporate networks and control systems is indispensable for business operations. However, instead of allowing multiple separate links, a single, well-secured link point could be established through which all necessary links could pass. Properly securing corporate IT systems by regularly patching software flaws and utilizing anti-virus tools (among other things) would minimize the risk of indirect attacks against control systems via related information networks.

- Implement strong authentication / access control for control systems and related information systems where possible – authentication / access control for control systems and related information systems is inadequate at present. Strong and reliable measures should be put in place to regulate remote access to control systems, and access to these systems through the corporate network. This could be achieved by using digital signatures, security tokens and/or biometrics technologies for authentication for links via the corporate network, and rigorously managing and controlling access rights. Work is ongoing with the Idaho National Engineering and Environmental Laboratory (INEEL) at the National SCADA Test Bed to develop effective authentication technologies specifically for control systems.

The following specific security measures should also be considered for control systems:

- Develop control system cyber security policies and procedures
- Encrypt communications channels and data where possible using VPNs, SSH, PKI etc.
- Use one-way connections, such as diode firewalls, wherever possible
- Use dial-back modems, callback systems, token-based authentication (e.g. SecurId) or other security measures for remote access to control systems
- Remove or disable unnecessary services, applications and ports. Examples include e-mail services and Internet access from control networks
- Remove or change all default passwords from control system hardware, particularly SNMP community strings

Longer-term, it is necessary to develop tools and technologies to secure control systems, networks and protocols. Work is underway to develop encryption, firewalls, IDS, and other security tools for real-time operating systems for energy management and control systems. These efforts should be expanded and supported where possible. Further, in order to be able to accurately assess the potential impact of cyber events on electric power systems, it is imperative to continue and expand control system testing and other research.

There is also currently a lack of available models for conducting control system cyber security auditing. It may be necessary to develop models that combine traditional IT security audit methodologies with safety vulnerability and risk assessment audit methodologies, such as used in the chemical industry. Finally, it is crucial for energy
operators to develop cyber business continuity plans for critical assets to protect the electric power grid and market from cascading effects.

**Conclusions**

The electric energy infrastructure sector underlies the smooth operation of all other infrastructures. Energy assets are vulnerable to physical or cyber attacks. While physical threats against the sector are stagnating or declining due to enhanced safety measures, cyber threats against energy management and control systems are rising as operators abandon proprietary software and control systems become ever-more connected to corporate networks and the Internet. While energy firms have put in place some security measures in recent years to protect their IT systems, control systems remain vulnerable. Furthermore, the anonymity of the Internet and the ability to launch attacks without requiring physical proximity to the target make cyber attacks too appealing to ignore.

Well-planned and executed small-scale attacks against energy control systems could yield a high success rate, but the impact of such attacks would probably be local or regional. More coordinated, simultaneous cyber attacks against multiple power plants or substations (or attacks targeting vulnerabilities of a single key SCADA or DCS supplier) could lead to larger regional or even national impacts. The possibility of a large-scale assault on the national power grid is hard to assess. It would probably require significant planning and reconnaissance, but too little information is currently available to make an accurate assessment. Protective measures and procedures exist that could reduce the sector’s vulnerabilities, but strong security will require greater awareness of existing vulnerabilities, a better understanding of the situation at the national level, and research and development into security tools specifically for energy management and control systems.
Additional Resources

Reports


Media Articles


‘Hacker jailed for revenge sewage attacks’, Tony Smith, The Register, October 31, 2001 - http://www.theregister.co.uk/content/4/22579.html


‘California hack points to possible IT surveillance threat’, Dan Verton, Computerworld, June 12, 2001 - http://www.computerworld.com/industrytopics/energy/story/0,10801,61313,00.html


‘Can Security Exist With Control Systems?’’, Joe Weiss, Intech, August 2002


