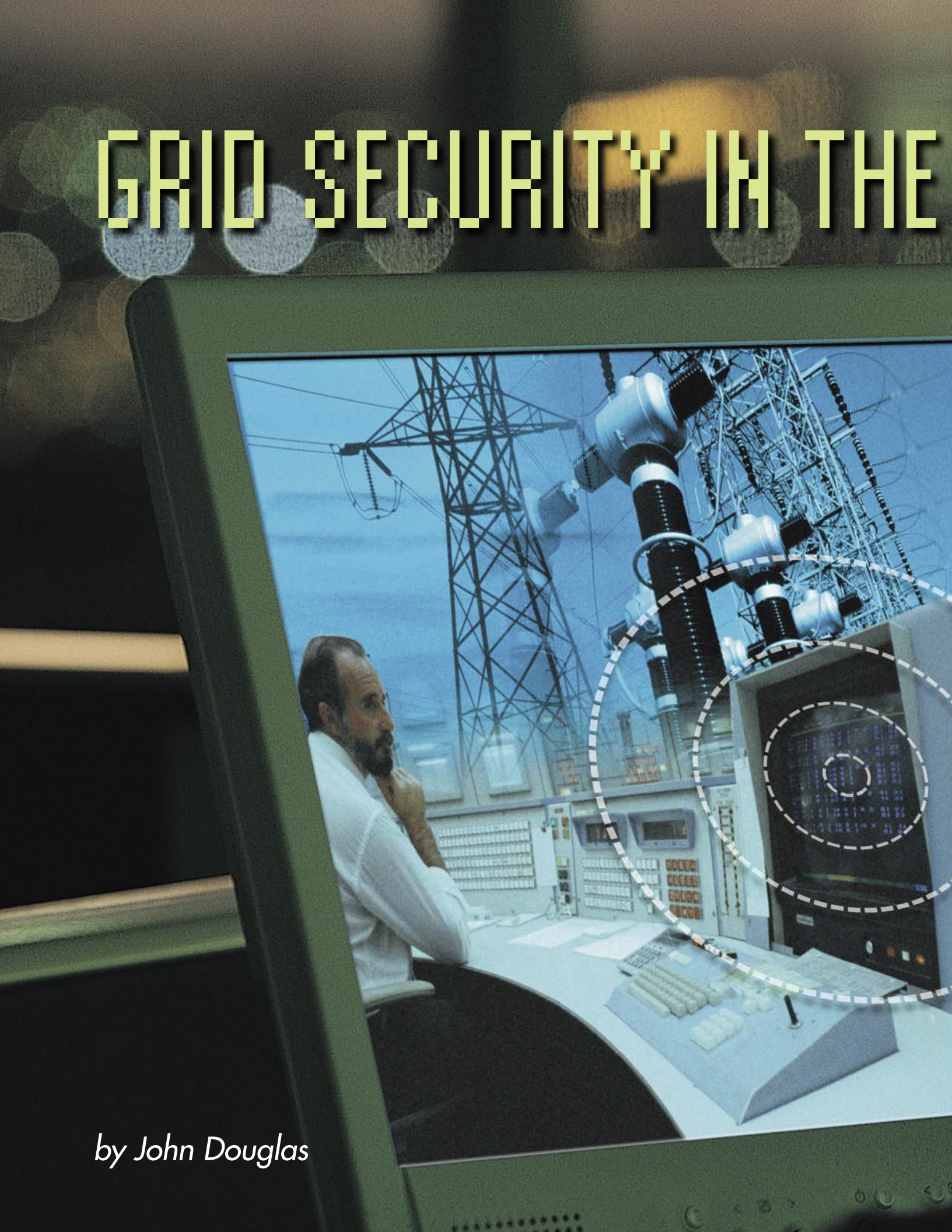
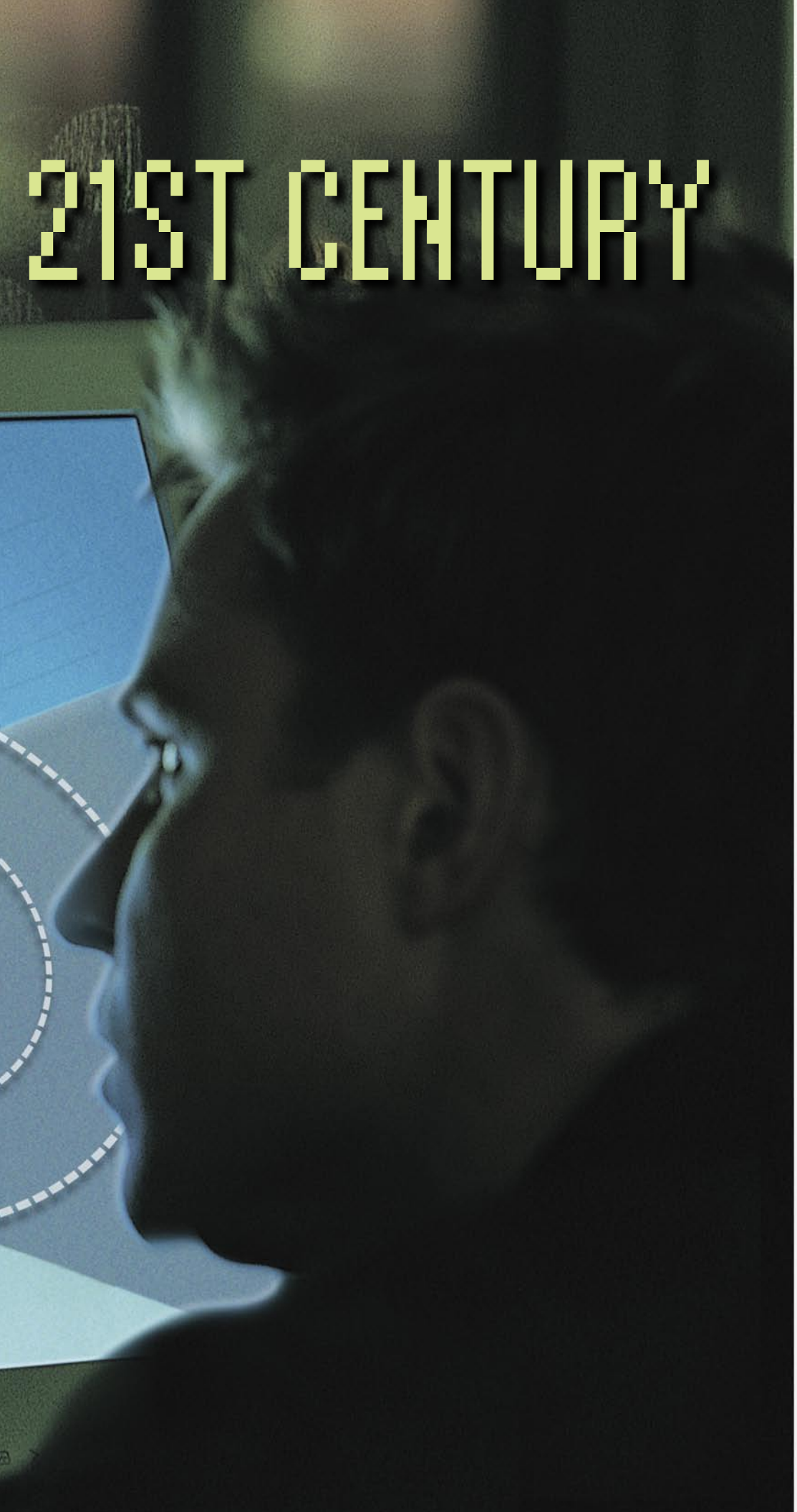
GRID SECURITY IN THE



by John Douglas



The Story in Brief

The rise of terrorism in the modern world necessitates a closer look at the vulnerability of the power grid to physical and cyber assaults. A new, industrywide initiative focuses on protecting electric power systems from hackers and worse.

Because electricity drives virtually all of the nation's critical infrastructures—from telecommunications to waterworks—the electric power system presents an inviting target for international terrorists. A coordinated attack on major power plants or substations could trigger a cascading blackout with major social and economic impacts. Depending on the extent and success of such an attack, daily life and business could be disrupted for several days across a wide area of the country, and a complete return to normalcy could take months to years.

Especially worrisome in a time of increasing industry dependence on the Internet is the fact that a devastating attack need not be directly physical: The perpetrators could remain anonymous and remote, achieving their goals by disrupting a utility's computer network or power system controls. A successful cyber attack, for example, could potentially allow a terrorist to destroy equipment by sending false control signals or by disabling electricity grid protective relays. Every day, a typical large electric utility must fight off hundreds or even thousands of cyber intrusions that appear to originate with hackers trying to disrupt normal business, obtain sensitive data, or exert control over parts of the grid.

Most utilities, of course, have already enhanced their efforts to protect both physical facilities and computer networks. The fact that virtually all of the illegal entry attempts so far have failed indicates the effectiveness of these security measures. "Utilities throughout North America have made significant strides to implement cyber and physical security," says Luther Tai, senior vice president, central services, Consolidated Edison Co. "While these have greatly reduced the vulnerabilities, there is more that can be done through the research and development work that is now under way at EPRI."

Part of the problem is that, with electric power networks so tightly interconnected, a significant security breach anywhere on the system can have an effect on the system as a whole. Since there are many different types of utilities in the United States, each at a different level of cyber preparedness, there is a compelling incentive to improve the coordination of security precautions taken by all utilities.

Utility decision makers face a number of challenges in this area. The broad scope of the security issue has led to development of multiple and sometimes overlapping requirements from various government agencies. At the same time, utility efforts to increase security are often constrained by limited access to useful information produced by these agencies and others, either because of the highly classified nature of the data or because the data are distributed across multiple locations. As a result, utility executives have often been forced to make security-related decisions on the basis of sparse, uncertain, or anecdotal information. A further challenge for electric utilities involves internal communications—how to effectively communicate security weaknesses identified by utility operations, planning, and engineering personnel to higher-level management.

Since 2001, a number of individual utilities have pioneered important cyber security efforts, each producing valuable results. However, a lack of effective technology transfer and broad industry support has limited the effectiveness of these results for the industry as a whole. Because security is only as strong as the "weakest link" in the chain of interconnected information and communication systems that utilities use, increased industry support, participation, and successful implementation of new security tools are crucial for effective industrywide cyber security.

In order to help provide the needed coordination and establish a unified response to cyber threats, EPRI and other leading industry organizations have formed the PowerSec Initiative. In addition, important new results are emerging from EPRI's own long-standing R&D work on electricity infrastructure security as a whole.

Early Efforts to Enhance Security

EPRI was leading an industrywide effort to reinforce U.S. power infrastructure security well before September 11, 2001. But as with most of the nation's protection and emergency response programs, the terrorist attacks sparked a fundamental rethinking, expansion, and refocusing of utility security efforts. While earlier concerns largly centered on the effects of natural disasters, system control anomalies, and small-scale vandalism, the twenty-first-century equation clearly must include protection against calculated assaults designed to disrupt American life and commerce on a large scale. EPRI's Infrastructure Security Initiative (ISI) was launched in response to these challenges and was designed to develop both prevention countermeasures and enhanced recovery capabilities.

As part of the work to provide utilities with immediately useful countermeasures, ISI is documenting lessons learned from actual terrorist attacks and other catastrophic events at utilities around the world for use by ISI participants. One of the highlights of this effort came in 2004 with the receipt of a draft report from Israel Electric Corporation on best practices they have developed to defend their grid against terrorist attacks. The countermeasures project is also providing utilities with information on new ways to protect their physical facilities, including a covert detection system that uses a magnetic field to identify potential intruders by size, speed, and electrical conductivity. Another system uses artificial intelligence technology to automatically analyze the streaming video from cameras in remote locations to detect, for example, whether an intruder has dropped a suspicious object.

Among potential infrastructure targets attractive to terrorists, high-voltage transformers represent a critical vulnerability. These transformers cost several million dollars each and usually take one to two years to procure, build, and install. In

response to this threat, ISI came up with the concept and developed preliminary designs for a new type of transformer that can be easily stored, transported, and installed for emergency use. An important milestone in development of this so-called recovery transformer was achieved in 2004 with completion of preliminary designs for two units, rated at 500 kV and 345 kV. Both can be transported by truck, rail, or military cargo plane, and once all parts are available on site, they can be installed in about 48 hours.

The design studies for the recovery transformers indicate that they will be about 30% lighter and smaller than conventional units, have an efficiency of 99%, and have an expected life of about 35 years. EPRI is currently working with the Department of Homeland Security (DHS) seeking sponsorship for the production of prototypes for these transformers. EPRI would provide funding through ISI for the factory testing efforts to ensure that electric utility short-circuit criteria and other critical performance requirements are met.

In addition, ISI is in the process of developing emergency recovery plans for substations that have been knocked out by a terrorist attack or other devastating event. These plans identify methods that utilities can use to assess which equipment is still salvageable, to identify the need and availability of spare parts, and to attempt to "harden" key sites against possible attack.

Emergency communications technologies are also being evaluated by ISI in order to recommend the best alternatives for use in case of emergency. The aim is to provide utilities with secure ways of communicating with each other and with emergency services after a successful, multi-regional terrorist attack. This work is being coordinated with related projects being carried out by government agencies and in other countries. In particular, the use of satellite phones—which support both voice and data communication—is being explored.

Dealing With Cyber Vulnerability

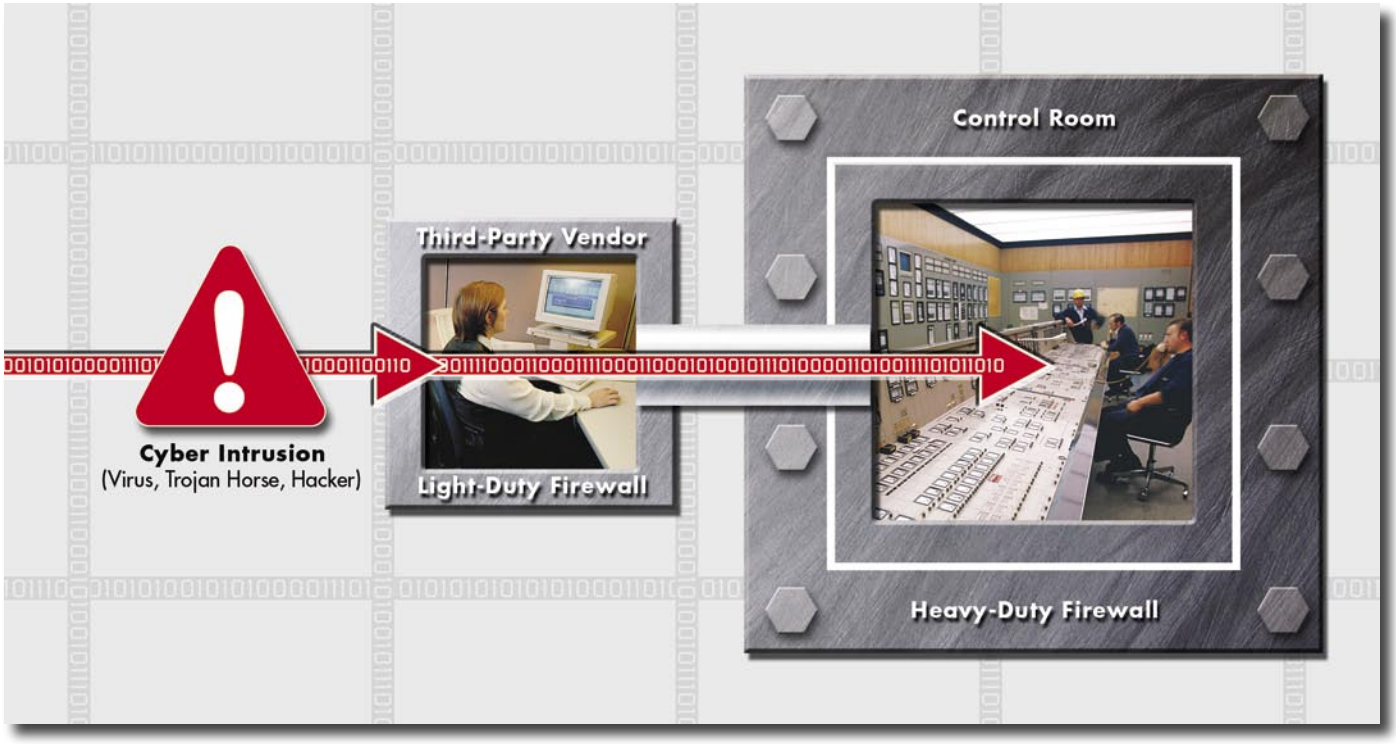
In this age of ubiquitous digitization, physical attacks are far from the only concern. The known successes of cyber attacks on a surprising variety of industries offer chilling testimony to the need for countermeasures against computer-based intrusions.

While physical assaults—be they facility break-ins, weapon attacks, or bomb explosions—are certainly frightening possibilities, cyber attacks have the potential to be every bit as destructive and carry the insidious added threats of stealth and long-distance control. "If a cyber terrorist is able to get through a company's firewall and other protection systems, it doesn't matter if he's on the other side of the world," points out technical executive Robert Schainker, who manages EPRI's security work. "If he's linked in through the Internet—which is available virtually everywhere—and he penetrates the protections to your operational systems he may as well be sitting in your control room."

Indeed, the incredible power and flexibility of the Internet has made cyberspace part of the global battlefield, and several nations have incorporated explicit plans for attacking information systems into their military preparations. Russia, for example, has documented successes in cyber attacks against key Chechen web sites. India and Pakistan have pursued competing preparations for electronic warfare. China has formulated an official cyber warfare doctrine, and North Korea has experimented with offensive cyber technologies. Terrorist organizations in the Middle East have shown increasing sophistication in the use of information technologies and have made no secret of their intent to attack critical American infrastructures.

The U.S. government has long been concerned over the wide-ranging effects that computer-based attacks could have on the nation's key infrastructures. After the Morris computer worm brought 10% of the country's Internet systems to a standstill in 1988, the Defense Advanced

Modern-day security threats can be both physical and cyber-based. An intruder could destroy a substation transformer with a bomb or by setting a fire, but a computer hacker could accomplish the same end by sending the transformer overload signals, causing it to rapidly overheat and explode.



While utilities go to great lengths to protect their critical facilities from cyber intrusion, their connections with third-party vendors can be an unrecognized weak spot. Hackers stopped by strong firewall systems protecting the control room, for example, may be able to make it in through weaker, standard security measures protecting vendors that provide procurement or billing services. Once in the "back door," the intruder may be able to move to a utility's grid operation and control systems.

Research Projects Agency (DARPA) set up the Computer Emergency Response Team (CERT) Coordination Center at Carnegie Mellon University to monitor cyber threats and respond to serious security incidents. According to CERT, keeping ahead of the trouble is no easy task: "Along with the rapid increase in the size of the Internet and its use for critical functions, there have been progressive changes in intruder techniques, increased amounts of damage, increased difficulty in detecting an attack, and increased difficulty in catching the attackers."

Earlier this year, DHS set up the Process Control Systems Forum (PCSF) to focus specifically on threats to the computerized automated control systems that underlie operation of most of the country's critical infrastructures, including the electric power grid. The PCSF will leverage security knowledge currently dispersed among different infrastructures and stimulate cross-functional discussions between those responsible for information technology and operations. EPRI is coordinating with the PCSF to ensure that the utility industry's security concerns and solutions are shared on a confidential basis.

Technologically, utility industry restructuring has created several unforeseen effects that increase this vulnerability. Power companies are now much more interconnected than previously, which not only provides more points of entry for an attacker but also means that potential damage may be more widespread. Open (as opposed to proprietary) operating systems and communications protocols were successfully designed to improve ease of use, but they may have made the task of an intruder easier as well. And remote access systems, such as those used to monitor field data and revise set points for relays, may have opened new portals for intrusion.

Changing business practices may also inadvertently open new opportunities for cyber intrusion. For example, an increasing number of businesses—including utility companies—are turning to third-party vendors to provide day-to-day administrative or service functions such as payroll, accounting, and maintenance. As a result, a power plant's operating control system may have direct communication links to a vendor-managed purchase/selling function, such as procurement or billing. But the vendor's computer system may not be as strongly protected from the outside world as the utility's heavily firewalled control room, providing an easier point of entry for hackers or computer viruses. After gaining access to the utility through this "back door," the intruder may be able to move to more critical areas of the plant, unbeknownst to the utility company.

These and other emerging concerns prompted EPRI to add computer-based

threats to its portfolio of security R&D. EPRI's focus on cyber security had its beginnings in the development of the first utility open-systems architecture—the Utility Communications Architecture (UCA), used to share data between various computer systems in a company—and was strengthened after the highly successful program to prepare utility computer systems and equipment for the Y2K transition. Growing concern over the possibility of computer-based security breaches led to development of EPRI's Energy Information Security (EIS) program in 2003. EIS was designed to provide tools that individual utilities could use to enhance their own security programs, including cyber security awareness training, information sharing, approaches to assessing control system vulnerability, and risk management protocols.

The EIS program has already produced valuable results. When vulnerabilities were discovered in standard communications protocols, such as those specified in UCA, EIS researchers developed enhancements designed to increase security. Early exploratory work has also been conducted on fast encryption and instruction detection technologies to protect data and control systems. Publication of the *Security Vulnerability Self-Assessment Guideline for the Electric Utility Industry* (1001639) enabled companies to conduct their own risk analyses, while the *Guidelines for Detecting and Mitigating Cyber Attacks on Electric Power Companies* (1008396) provided basic procedures for enhancing network security.

PowerSec: A Coordinated Approach

Much progress has been made through EPRI's ISI and EIS programs. But considering the complexity of the nation's power infrastructure, the ever-increasing capabilities of cyber attackers, and the diverse nature of current security efforts, a more comprehensive, highly coordinated effort is clearly required. In response—and in cooperation with several industry organizations and the EPRI Board of Directors—EPRI drafted a proposal for an industrywide program, identified ongoing security work at various industry and government organizations, and obtained feedback from more than 60 utilities, representing all segments of the electric power industry. As a result, an alliance has been formed to create the PowerSec Initiative, which initially will bring together EPRI staff, a variety of industry organizations, and several industry experts to address the cyber threat issue.

By examining threats, vulnerabilities, and potential consequences, the PowerSec Initiative will evaluate the industry's current cyber attack readiness, identify gaps in this readiness, and specify existing best practices for filling these gaps. In some cases, even current best practices will not be sufficient to handle emerging attack techniques; the initiative will therefore also identify vulnerabilities that require new solutions and specify what R&D work is needed to develop and test these solutions.

One important goal of PowerSec is to consolidate and leverage ongoing and completed cyber security work from utilities, government, regulatory agencies, and others. Appropriate information on best practices will be disseminated to the industry using methods consistent with the safeguard of confidential or classified information. In addition to integrating and sharing disparate information, the initiative will serve as a model of how the utility industry, regulators, and government can work together to solve complex security problems.

"EPRI has long been a leader in building security awareness in the electric power industry," says Tom Kropp, EPRI project manager for electric power critical infrastructure protection. "Now the information and products we have developed over the years can help form the foundation of a coordinated, industrywide effort."

Early Goals

The PowerSec Initiative will focus first on electric utility supervisory control and data acquisition (SCADA) systems and energy management systems (EMS), both of which have been identified by experts as critical systems to secure. Identifying and filling existing security gaps in communication and control systems will make it more difficult for potential intruders to gain access and cause damage. Improvements in these systems will also tend to increase overall levels of power system reliability, providing a more secure business environment for wholesale power markets and enabling utilities to offer better service to their customers.

EPRI and its members have defined a set of general objectives for the PowerSec Initiative, the first of which is to develop an overview of the electric power industry's current cyber security posture. From this, the initiative will provide utilities with a list of vulnerabilities for each major type of SCADA and EMS control system commonly deployed across North America and will tailor this information to reflect the particular combinations of systems in use. A comprehensive, prioritized list of viable cyber threats will also be developed, along with the compendium of best practices with recommendations on how to maximize cyber security using currently available tools and methods. A compendium of current cyber security projects being pursued by both government and private industry will be developed to clarify which areas are being adequately studied and which need more attention.

Together, these results will be used to identify gaps between viable threats and defenses, both current and planned; the analysis will lead to an R&D action plan for developing technologies to eliminate any gaps, identified or perceived.

Clearly the first order of business for PowerSec will be to assess the vulnerability of information and control systems currently used by utilities and system operators. This work will begin with on-site interviews and inspections and will be supplemented by evaluation of past or ongoing security analyses by individual

Artificial intelligence software offers new tools to help identify physical threats. In this airport baggage claim area, a video surveillance camera is able to automatically monitor and analyze the activities of groups and individuals. When the man circled in yellow sits down and then leaves the scene without the small bag he was carrying, the system identifies the unattended object (red box) and alerts security that there is a suspicious situation. (Photos courtesy ActivEye, Inc.)

utilities, EPRI, and government organizations. Researchers will also examine existing information systems directly to determine their cyber vulnerability, and in some cases, conduct "red teaming" (mock intrusion) exercises at selected host utility sites. Particular emphasis will be placed on examining SCADA and EMS systems to help prevent hackers from using them to take over control of critical utility equipment.

Each PowerSec participant will receive a confidential document identifying the strengths and weaknesses of its own SCADA and EMS systems. Because the report will identify the best practices for those particular systems, PowerSec participants will have the advantage of being able to enact available countermeasures immediately to reduce the threat of successful cyber attack.

Information gleaned from the vulnerability assessment process is also intended to complement ongoing security standards development by the North American Electric Reliability Council (NERC) and the Federal Energy Regulatory Commission. The Urgent Action Cyber Security Standard 1200 adopted by NERC in 2003 already specifies actions to be taken to protect utility systems in 16 areas, such as access control, information protection, personnel training, incident response, and recovery planning, among others. This standard, which was originally adopted as a temporary measure, is now being extended and modified for development into a set of permanent security standards: CIP-002 through CIP-009.

PowerSec's assessment phase—expected to take about a year—will provide an objective assessment of the industry's cyber security. If significant security gaps are identified, EPRI staff will work with PowerSec participants to propose solution approaches to be developed and tested in later phases.

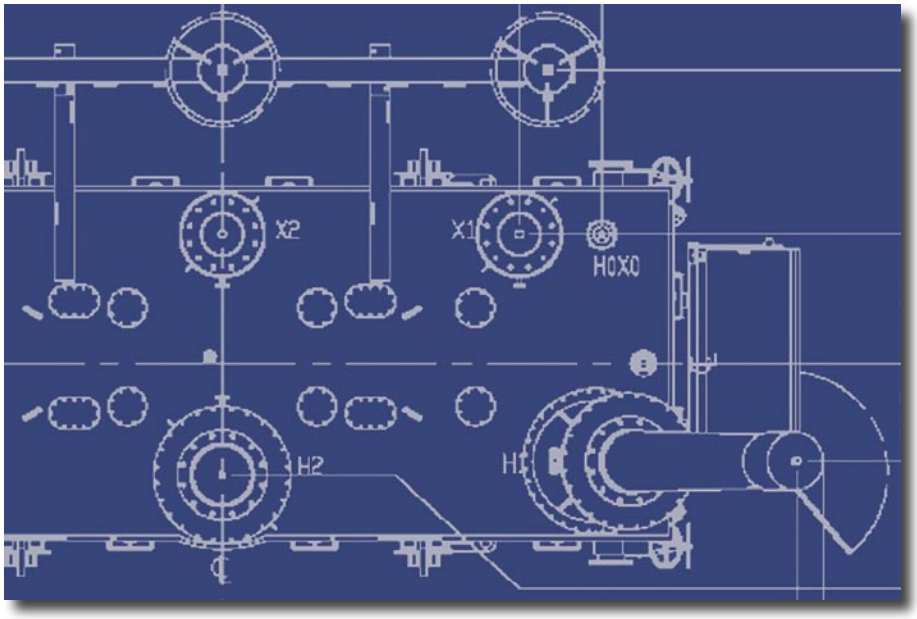
The effectiveness of PowerSec results will be evaluated using independent testbed exercises at the Idaho National Laboratory and Sandia National Laboratory, as

appropriate. These facilities are capable of testing the new tools on a variety of SCADA and other cyber systems provided by manufacturers. Evaluations will also be conducted at individual utilities. The PowerSec team will use the confidential results of these evaluations, together with feedback from the deployment process, to revise vulnerability assessments and enhance the alert system by adding new attack mitigation actions.

An Eye to the Future

After developing the draft proposal for the PowerSec Initiative, EPRI submitted the plans to member utility executives for comment and suggestions. This feedback provided important insights on how to proceed with PowerSec formation. The comments revealed that utilities believe they have made considerable progress toward protecting their own cyber systems but recognize that key vulnerabilities remain across the industry as a whole. The executives generally believe that cyber attacks are likely, from domestic and/or international terrorists, and that disgruntled past or present employees also represent a potentially dangerous threat. They also say that PowerSec should ultimately address a combination of cyber and physical threats and vulnerabilities, because successful physical attacks may involve very long recovery times. An area of particular concern is how to ensure the availability of spare parts for long-lead-time equipment.

The PowerSec Initiative will help participants come quickly up the learning curve about cyber security risks and vulnerabilities and will give them enhanced capabilities to assess cyber-related threats on their own systems. Access to government and regulatory thinking on security issues could also help participants better prepare for potential changes in cyber regulations that impact utilities. "The biggest issue today is the incomplete and anecdotal aspects of the situational data available," concludes Schainker. "Such uncertainties prevent utilities from positioning themselves effectively for dealing with security issues. A more comprehensive understanding of the situation will allow PowerSec participants to better allocate financial and personnel resources to their security preparedness." Ultimately, it is hoped that PowerSec will help focus future government cyber security regulations, spur the development of innovative mitigation tools and methods, and promote enhanced cyber security preparedness by the industry at large.



Loss of a high-voltage transformer is of particular concern for grid security because replacement units typically take one to two years to procure, build, and install. EPRI's Infrastructure Security Initiative is dealing with this problem by sponsoring designs for a smaller, lighter "recovery transformer" for emergency use that can be easily stored, transported, and installed in days. (Courtesy ABB)

But if continued attacks on the grid are inevitable, as many industry leaders believe, prevention will only be part of the answer to grid security concerns. "We've got a lot of smart people working on this problem, but the field of opportunity for intrusions is very broad," says Wade Malcolm, EPRI's vice president for power delivery. "We have to assume that sooner or later an intruder will succeed in breaching our defenses. This is why a long-term program for increasing overall system resiliency becomes crucial—if a hacker or terrorist does manage to compromise a transformer or power line, the grid must be able to withstand the loss without the danger of wide-area cascading outages." EPRI's IntelliGrid℠ Consortium—another industrywide initiative—is working on adaptive, self-healing technologies that can be built into the nation's electric power delivery system to provide just such resiliency.

"The industry is clearly entering a new phase of security consciousness," concludes Schainker. "Some individual utilities have already done a lot to protect their own cyber and physical systems against terrorist attacks, and now the time has come to expand this work through coordinated, industrywide efforts. If we are successful, the payoff will be large indeed: With PowerSec reducing the probable success of attacks and IntelliGrid features limiting the scope of their effects, tomorrow's power grid will have every potential to meet the challenges of a post-9/11 world."

Background information for this article was provided by Robert Schainker (rschaink@epri.com) and Thomas Kropp (tkropp@epri.com).