Appendix A3:
A Systems View of the Modern Grid

RESISTS ATTACK

Conducted by the National Energy Technology Laboratory
for the U.S. Department of Energy
Office of Electricity Delivery and Energy Reliability
January 2007

Office of Electricity
Delivery and Energy
Reliability

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The systems view of the modern grid features seven principal characteristics. (See Figure 1.) The ability to resist attack is one of those characteristics and the subject of this paper.

Figure 1: The Modern Grid Systems View provides an "ecosystem" perspective that considers all aspects and all stakeholders.

The energy industry's assets and systems were not designed to handle extensive, well-organized acts of terrorism aimed at key elements.

The U.S. energy system is a huge network of electric generating facilities and transmission lines, natural gas pipelines, oil refineries and pipelines, and coal mines. Occasionally, these systems have been tested by large-scale natural disasters such as hurricanes and earthquakes. Generally, industries have restored energy relatively quickly. Sabotage of individual components has caused some problems, but the impacts have been managed. We've been lucky.

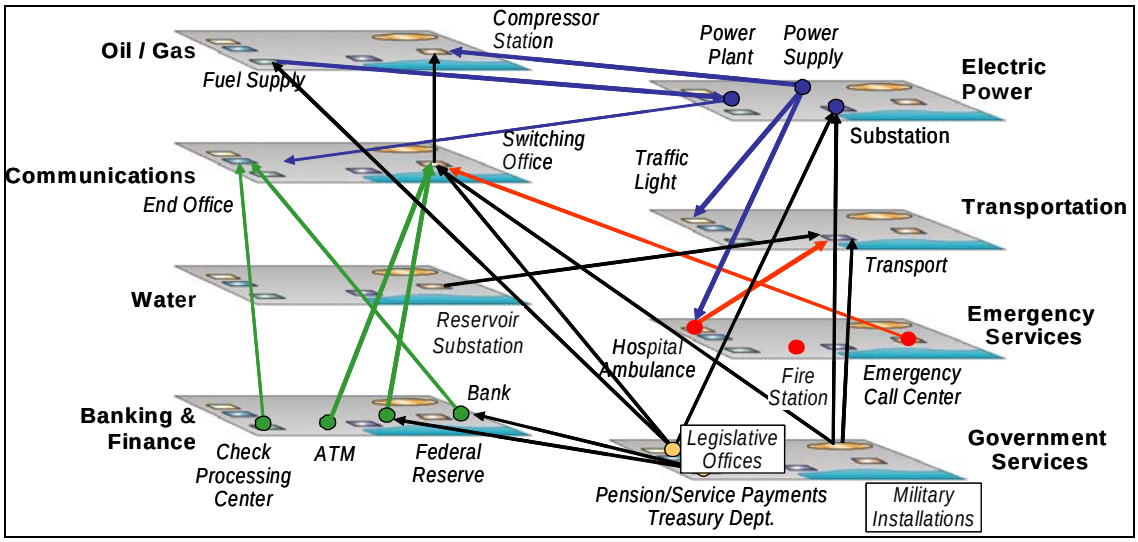


Figure 2: Interdependence of Energy and Other Sectors: Losing power in even one region damages the whole economy. Image courtesy of Science Applications International Corporation (SAIC).

The dependency of other key elements of the economy on the electrical power part of the energy system (see Figure 2) is apparent when millisecond outages disrupt sensitive digital processes, and outages extending days or weeks can deprive a community or region of running water. Telecommunications, financial, and health sectors try to ensure uninterrupted power by installing generators, batteries, or redundant systems. Even these, however, can be limited in their effectiveness. Generators, for example, are limited by the availability of fuel.

With the introduction of digital technology throughout our society, the cost of outages (e.g., from equipment failure or weather-related incidents) has significantly increased – from $30 billion in 1995 to $119 billion in 2001 (National Research Council, 2002)

It is critical for the modern grid to address security from the outset, making security a requirement for all the elements of the grid and ensuring an integrated and balanced approach across the system.

Threats to the infrastructure are usually broken into two categories: physical (explosives, projectiles) attacks and cyber (computer launched) attacks. Whatever the specific nature of the threat, the designers of the modern grid should plan for a dedicated, well-planned, and simultaneous attack against several parts of the system.

The threat of both physical and cyber attack is growing and a widespread attack against the infrastructure cannot be ruled out. There is evidence that Al Qaeda has been tracking debates in the United States related to the cyber vulnerability of control systems in the energy infrastructure (Hamre, 2003).

- **Cyber attacks** — Computer security incidents are increasing at an alarming rate. According to the Government Accountability Office, in 2002, 70 percent of energy and power companies experienced some kind of severe cyber attack to their computing or energy management systems. (See Figure 3.)

- **Physical attacks** — Physical attacks against key elements of the grid, or physical attacks combined with cyber attacks, cannot be discounted. From a terrorist viewpoint, damage from a physical attack may be more predictable than a cyber attack, and therefore promise more certainty in causing harm.

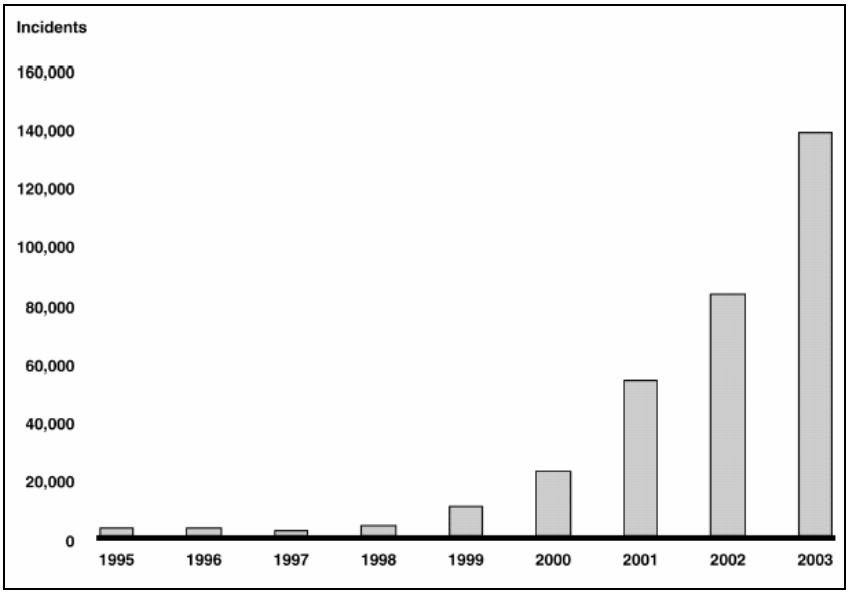


Figure 3: 70% of energy and power companies experienced some kind of severe cyber attack to either their IT or SCADA/EMS network. (GAO analysis based on Carnegie Mellon University's CERT Coordination Center data).

Whether it is going to be a physical or cyber attack, the modern grid must resist two different attack strategies:

1. *Attacks on the* power *system*, in which the infrastructure itself is the primary target.
2. *Attacks through the power system*, in which attackers take advantage of power system networks to affect other infrastructure systems, such as telecommunications, financial, or government.

A study that surveyed over 170 security professionals and other executives concluded that, across industries, respondents believe that a large-scale cyber attack in the United States will be launched against their industry in the near future. (U.S. General Accounting Office, 2004)

An emphasis on security throughout the development and implementation phases of the modern grid is critical. Such an emphasis would:

- Ensure lowest cost for system elements by addressing security concerns during the initial design and throughout the lifecycle.
- Demonstrate benefits of security enhancements to grid efficiency and vice-versa.
- Increase public and business confidence in the modern grid's resilience.

This paper covers four important topics:

1. The current and future states of grid security.
2. The requirements that, if met, would assure a disciplined systems approach and an industry/government partnership.
3. The benefits that accrue to developing a modern grid that resists attack.
4. Recommendations for moving forward.

Although it can be read on its own, this paper supports and supplements “A Systems View of the Modern Grid,” an overview prepared by the Modern Grid Initiative (MGI) team.

CURRENT AND FUTURE STATES

Before we discuss how the modern grid might be developed to resist attack, we need to understand its current vulnerability and how to reduce that vulnerability in the future. This section explores the current state and the desired future state of grid security.

CURRENT STATE

The complexity of the current electrical power system and the reliance on critical nodes to operate without interruption create the potential for single-point failures that can result in widespread disruptions.

In today's grid, failure of a critical node may not be detected or corrected in time to avoid a major disruption. The weak link might become apparent on a hot summer day with specific power flow conditions as the potential catalyst for a widespread blackout, similar to one experienced on August 14, 2003.

The grid is aging, based largely on technology developed in the 1950s or earlier. This aging infrastructure is stressed by lack of adequate investment to meet the growing demand for electric power.

From 1988 to 1998, U.S. total electricity demand rose by nearly 30 percent but its transmission network's capacity grew by only 15 percent. From 1999 to 2009, analysts expect demand to grow by 20 percent, while planned transmission systems grow by only 3.5 percent (Amin 2003, 19–25).

Ironically, recent advances in technology and changes in the electricity sector, such as deregulation and dependence on 20th century technologies, may be adding to the security problem. Examples include:

- Increased reliance on unprotected telecommunications networks and on associated SCADA systems.
- The growth of independent power producers without the budget to address security.
- Outsourcing of maintenance and security by larger companies.

In general, deregulation has increased the number and types of industry players and interfaces, adding complexity and thereby increasing the potential for security gaps. (Committee on Science and Technology for Countering Terrorism, National Research Council, 178-179, 2002)

Attacks on the grid could be aided by today's easy accessibility to open sources of information. In the electric power industry, industry publications, maps and material are all available on the internet. These are sufficient to allow someone to identify the most heavily loaded transmission lines and the most critical substations in the power grid.

Hackers could gain access to "open" electric power control systems, crack passwords, and lower protective relay settings, causing circuit breakers to "trip" at normal current flow. They could raise, at the same time, the settings on neighboring circuit breakers so that diverted power would damage the infrastructure protected by those breakers (GAO 2004, 14–16).

Threats to the security of the grid's cyber backbone are increasing. Application of existing security technologies, such as encryption and the widespread use of routine security procedures could help somewhat. However, too many control devices in use on today's grid do not have the bandwidth and processing power to use even the current state of the art in cyber protection.

FUTURE STATE

The modern grid will address critical security issues from the outset, making security a requirement for all the elements of the grid and adopting a systems view that enables an integrated and balanced approach.

Planning for manmade threats will consider not only single, but also multiple points of failure. Parts of the system will need more risk reduction than others. With a systems view, security decisions will be based on prioritized options to reduce risk. Federal, state, and local officials will work with individual utilities to address acceptable risk, possibly with support from DOE and homeland security officials.

Federal, state and local policies and regulations will be developed that allow utilities and others in the electricity industry to recoup reasonable costs for security upgrades that are part of the overall system design.

Security will benefit from key modern grid technologies that include:

- Integrated Communications for real-time information & control.
- Sensing & Measurement.
- Advanced Components & Distributed Energy Resources (DER).
- Advanced Control Methods.
- Improved Interfaces & Decision Support.

Table 1 notes some of the security solutions offered by these technologies.

Modern Grid Key Technologies	Security Solutions
Integrated Communications for real-time information & control	■ Use communication for prediction and decision support. ■ Wide-area secure communications instead of internet monitoring. ■ Monitor and respond to threat conditions instantaneously.
Sensing & Measurement	■ Remote monitoring that detects problems anywhere in the grid. ■ Events detected in time to respond.
Advanced Components & DER	■ Tolerant and resilient devices. ■ Fewer critical points of failure. ■ Distributed, autonomous resources.
Advanced Control Methods	■ Islanding to isolate vulnerable areas of the grid. ■ Automated network "agents" for dynamic reconfiguring. ■ Self-healing with preventive or corrective actions in real-time.
Improved Interfaces & Decision Support	■ Operator training for response to attacks. ■ System recommendations for best response. ■ Simplification of operator interaction with the system.

Table 1: The key technologies of the modern grid contribute to solutions that resist attack.

A modern, more resilient grid will leverage technologies for rapid, wide-area communication of the status of grid components. New control technologies will quicken response to events and easily integrate DER.

Enterprises will focus people and processes on implementing and maintaining security. People with experience assessing risk and designing security in complex systems will help develop and operate the modern grid. Process improvements can provide a substantial benefit at low cost. Additionally, processes for resolution of inter-company and inter-regional issues will be put in place.

In the modern grid, implementing cost-effective options to enhance security will also have positive impacts on reliability and resilience. For example, the data required for computer simulations that provide operators with information to predict disruptions could also be used to identify and mitigate attacks against the grid.

Government and industry will jointly conduct exercises that will improve the security aspects of the modern grid, as well as its design and operation. Metrics will be used to gauge success and guide iterative improvements.

REQUIREMENTS

With a broad understanding of the current and future state of the electrical power system, we can now discuss some of the requirements that need to be met to move forward. This section explores system requirements, as well as requirements for policy and regulation, and codes and standards.

SYSTEM REQUIREMENTS

The systems approach to electric power security would identify key vulnerabilities, assess the likelihood of threats and determine consequences of an attack. The designers of the modern grid can draw on extensive experience developed by the Department of Defense in assessing threats and system vulnerabilities.

This approach would apply risk management methods to prioritize the allocation of resources for security, including R&D. Particular goals of security programs would include:

- Identification of critical sites and systems.
- Protection of selected sites using surveillance and barriers against physical attack.
- Protection of systems against cyber attack using information denial (masking).
- Dispersing sites that are high value targets.
- The ability to tolerate a disruption (self-healing characteristics).
- Integration of distributed energy sources and using automated distribution to speed recovery from attack.

Resilience must be built in to each element of the system, and the overall system must be designed to deter, detect, respond and recover from manmade disruptions.

For the modern grid to resist attack, it must reduce:

- The *threat* of attack by concealing, dispersing, eliminating or reducing single-point failures.
- The *vulnerability* of the grid to attack by protecting key assets from physical and cyber attack.
- The *consequences* of a successful attack by focusing resources on recovery.

Therefore, its system requirements must include those that:

- Implement self-healing capabilities.
- Enable “islanding” (the autonomous operation of selected grid elements).

- Provide greater automation, wide area monitoring, and remote control of electric distribution systems.
- Acquire and position spares for key assets.
- Use distributed energy resources.
- Ensure that added equipment and control systems do not create additional opportunities for attack.
- Rapidly respond to impending disruptions with the aid of predictive models and decision support tools.

A systems approach with government and industry teamwork will help the requirements and their costs to be allocated sensibly across the modern grid. Adopting a systems approach encourages balanced investment. Security investments must reinforce the weak links in the grid and avoid the costs of ineffective measures. For example, it does no good for a utility to build fences and hire guards to protect its power plant when an unscreened insider or an outside hacker exploiting unencrypted communications can disable the plant.

POLICY AND REGULATION REQUIREMENTS

Federal, state and local policies and regulations need to be developed to allow utilities and others in the electricity industry to recoup reasonable costs for security upgrades that are part of the overall system design.

For example, federal guidelines and regulations mandating the accommodation of distributed energy resources (DER) would require an investment from industry. The integration of distributed energy would enhance the reliability of the overall system, regardless of which entity owned and operated the DER.

Of course, the federal government could take on the role of funding selected security enhancements or pioneering development of certain advanced technologies that would support security of the modern grid. Nevertheless, the question remains as to what entities make the investment to satisfy requirements such as:

- Integrated DER.
- Real-time communications.
- Secure data transfer over wide areas.
- Integrated, standard fault detection and correction across systems involving multiple utilities.

Metrics to measure the results of security measures must also be used to allocate costs fairly. Utilities faced with investment costs to modernize the grid – even with possible government subsidies – will want a clear understanding of which security upgrades can be passed to the ratepayers. Coming up with the answers will require close coordination between federal and state regulatory authorities, DOE, and possibly homeland security officials.

CODES AND STANDARDS REQUIREMENTS

Grid owners and operators must take a systems view of security, applying industry best practices and standards.

The industry has already begun to establish best practices, primarily through the work of the North American Electric Reliability Council (NERC) Critical Infrastructure Protection Committee (CIPC). These practices are made available through the Information Sharing and Analysis Center for Electricity managed by NERC.

BARRIERS

The physical and cyber security of the electric industry is a growing concern. Evolving national security threats, increasing interoperability in the grid, and expanded use of open systems in the grid's architecture all contribute to serious vulnerabilities.

Most utilities have taken some action on security, but the question remains: Are we gaining ground or losing ground on security? Although we can't provide a definitive answer, we can pinpoint some of the specific barriers that must be overcome to achieve the Modern Grid vision of a system that resists intentional attack. These barriers include:

- **Incomplete understanding of threats, vulnerabilities and consequences.** Some utilities conduct vulnerability and risk assessments and a fraction of them apply the results to security upgrades. Industry as a whole lacks a standard approach to conducting these assessments, understanding consequences, and valuing security upgrades. Additionally, limited access to government-held threat information makes the case for security investments even more difficult to justify.
- **Perception that security improvements are prohibitively expensive.** When examined independently, the costs and benefits of security investments can seem unjustifiable. Approaching grid modernization from a systems perspective provides the significant leverage that can be used to improve security with related technology advances such as sensors, controls and communications.
- **Increasing use of open systems.** Open communication and operating systems are flexible and improve system performance, but are not as secure as proprietary systems. The increasing use of open systems must be met with industry approved and adopted standards and protocols that consider system security.
- **Increasing number of grid participants.** The growing number of participants in the electric system increases the complexity of physical and cyber security issues. Security measures must be built in to the functions that support DER owners, Independent Power Producers, and consumers active in demand response and automated metering programs.
- **Difficulty in recovering costs.** Utilities must be armed with sufficient knowledge and justification to make the case for security investments. Applying a cost-benefit analysis to the system as a whole will reflect the true value of security and system investments that support it.

BENEFITS

The modern grid will deliver substantial benefits if requirements to increase security are met. In this section, we focus on benefits unique to the characteristic of resisting attack.

Besides improving the modern grid's inherent resilience, there are some unique benefits of the modern grid's characteristic to resist attack. These benefits include:

- Deterring an attack in the first place, because it would have little effect.
- Improving the operational readiness of our defense forces by ensuring security-of-supply for electric power
- Reducing the social and economic impacts of a given disruption, for example:
    - Minimizing the costs of grid repair and costs associated with lost productivity.
    - Minimizing the loss of life associated with a loss of power for extended periods of time.
    - Reducing social disruptions.
    - Reducing the geographic extent of outages.
    - Improving the recovery time from outages.
- "Dual use" of security-related improvements to improve reliability such as:
    - Integration of DER.
    - Use of advanced modeling and simulation tools to prevent "normal" outages.
    - Use of spares to mitigate effects of equipment failure.
    - Application of demand response (DR) to increase system robustness.
    - Greater use of distribution automation.

Benefits attributable to other characteristics such as power quality and DER also satisfy security needs as well. Other papers in the MGI collection address these benefits.

RECOMMENDATIONS

To deploy a modern grid that resists attack, the recommendations of the Modern Grid Initiative rely on the coordinated efforts of planners, designers, developers, government, and industry.

Planners of the modern grid should:

- Leverage methods developed by DOD, DOE, and DHS to increase survivability of systems.
- Create a government-industry team, including state regulators, specifically to address issues of acceptable risk to the public from disruptions and ROI for industries' investments in security.

Designers and developers of the modern grid should:

- Consider security as a system requirement that could affect virtually every element and sub-system of the modern grid.
- Ensure that additional equipment and control systems added to the grid do not increase its likelihood of disruption and do not create additional opportunities for malevolent actions against it.
- Apply the ongoing work by industry, government, and academia on physical and cyber vulnerabilities.

Government and industry should:

- Define causes and consequences of outages — as required by the Department of Homeland Security in its development of the National Infrastructure Protection Plan.
- Share their concerns about the cost and expected benefits of security and ensure that the developers of the modern grid integrate security as an inherent characteristic — not as an optional feature.

Once key elements of the modern grid with security-related aspects are identified, the cost/benefit analysis and the risk analysis can be undertaken to determine the benefit of incorporating security upgrades. Then we will be well on our way to a modern grid that resists attack.

SUMMARY

The threat of both physical and cyber attack is growing and a widespread attack against the infrastructure cannot be ruled out.

The 20th century electrical power system is aging and its 1950s infrastructure was never designed to handle well-organized acts of terrorism.

In the 21st century, it is critical for the modern grid to address security from the outset, making security a requirement for all the elements of the grid and ensuring an integrated and balanced approach across the system.

Whether the threat is physical or cyber, the modern grid must resist attacks that employ two different strategies:

1. *Attacks on the* power *system*, in which the infrastructure itself is the primary target.
2. *Attacks through the power system*, in which attackers exploit power system, networks to affect other economic sectors such as telecommunications, financial, or government.

The complexity of the current electrical power system and the reliance on critical nodes to operate without interruption create the potential for single-point failures that can result in widespread disruptions. To resist organized attacks, the modern grid must consider the risk of multiple points of failure, not just single ones.

The systems approach to grid security would identify key vulnerabilities, assess the likelihood of threats that could exploit those vulnerabilities, and determine the probability and the possible consequences of a successful attack. Technologies and solutions to address security issues will complement communications, computing, decision-making support, self-healing aspects, and equipment improvements being developed for the modern grid.

Implementing cost-effective technologies to enhance the security of the grid will have positive impacts on reliability and resilience. Resilience must be built in to each element of the system. The modern grid (if designed in a way to deter, detect, respond, and recover from manmade disruptions) will also achieve other desired characteristics.

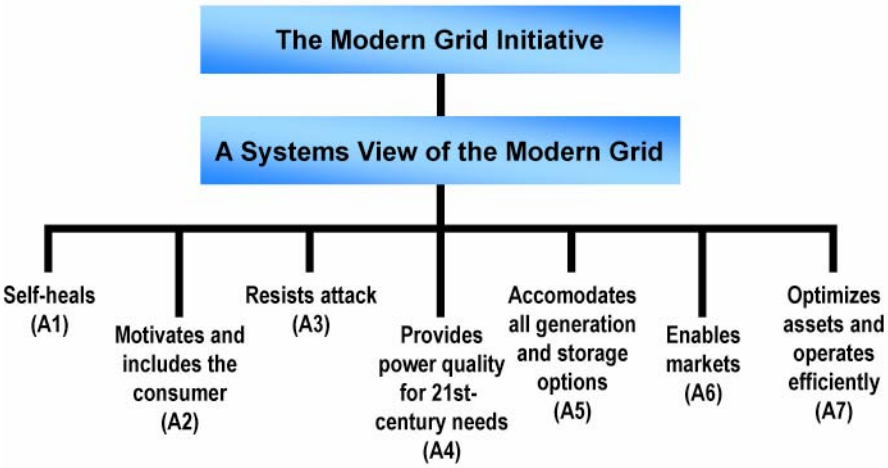
The electrical power industry, partnered with government, must maintain a systems view of security, applying industry best practices and standards. They must establish metrics to measure security effectiveness and allocate costs fairly. Federal, state, and

local policies and regulations need to be developed to allow utilities and others in the electricity industry to recoup reasonable costs for security upgrades that are part of the overall system design.

Addressing the grid as a system will require unparalleled government and industry cooperation. To deploy a modern grid that resists attack, the recommendations of the Modern Grid Initiative rely on the coordinated efforts of developers, government and industry to define and adhere to a total systems approach.

For more information

This document is part of a collection of documents prepared by The Modern Grid Initiative team. For a high-level overview of the modern grid, see "A Systems View of the Modern Grid." For additional background on the motivating factors for the modern grid, see "The Modern Grid Initiative." MGI has also prepared seven papers that support and supplement these overviews by detailing more specifics on each of the principal characteristics of the modern grid. This paper describes the third principal characteristic: "Resists Attack."



Documents are available for free download from the Modern Grid Web site.

The Modern Grid Initiative

Website: www.netl.doe.gov/moderngrid

Email: moderngrid@netl.doe.gov

(304) 599-4273 x101

BIBLIOGRAPHY

1. Amin, M. 2003. North America's electricity infrastructure: Are we ready for more perfect storms? *IEEE Security and Privacy* 1 (September/October): 19–25.
2. Amin, M. 2001. Toward self-healing infrastructure systems. *IEEE Computer Applications in Power, pgs 20-28.*
3. Apt, J. Causes of Major Disturbances. Carnegie Mellon University.
4. Committee on Science and Technology for Countering Terrorism, National Research Council. 2002. *Making the nation safer: The role of science and technology in countering terrorism*. Washington, D.C.: National Academies Press.
5. Hamre, J. 2003. "Cyberwar! Interview with John Hamre." PBS Frontline, February 18.
6. Idaho National Laboratory. Access denied: Defending the network against hackers. Fact sheet.
7. Sandia National Laboratory. Electric power network surety: Critical infrastructure surety. Fact sheet.
8. U.S. General Accounting Office. 2004. Critical infrastructure protection: Challenges and efforts to secure control systems. Report to congressional requestors. GAO-04-354.
9. U.S. Department of Homeland Security. 2004. National Response Plan.
10. Yeager, K. E. and C. W. Gellings. 2004. A bold vision for T&D. Paper presented at the Carnegie Mellon University Conference on Electricity Transmission in Deregulated Markets, Pittsburgh, PA.