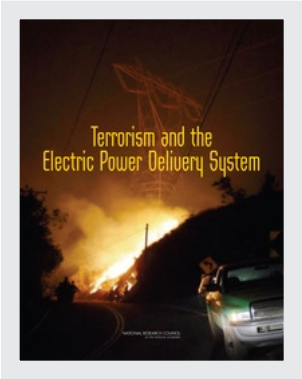


Terrorism and the Electric Power Delivery System

DETAILS

146 pages | 8 1/2 x 11 | PAPERBACK
ISBN 978-0-309-11404-2 | DOI 10.17226/12050

AUTHORS

Committee on Enhancing the Robustness and Resilience of Future Electrical Transmission and Distribution in the United States to Terrorist Attack; Board on Energy and Environmental Systems; Division on Engineering and Physical Sciences; National Research C

Terrorism and the Electric Power Delivery System

Committee on Enhancing the Robustness and Resilience of Future Electrical Transmission and Distribution in the United States to Terrorist Attack

Board on Energy and Environmental Systems

Division on Engineering and Physical Sciences

NATIONAL RESEARCH COUNCIL
OF THE NATIONAL ACADEMIES

THE NATIONAL ACADEMIES PRESS
Washington, D.C.
www.nap.edu

THE NATIONAL ACADEMIES PRESS • 500 Fifth Street, NW • Washington, DC 20001

NOTICE: The project that is the subject of this report was approved by the Governing Board of the National Research Council, whose members are drawn from the councils of the National Academy of Sciences, the National Academy of Engineering, and the Institute of Medicine. The members of the committee responsible for the report were chosen for their special competences and with regard for appropriate balance.

This study was supported by Contract HSHQPA-05-C-00016 between the National Academy of Sciences and the U.S. Department of Homeland Security. Any opinions, findings, conclusions, or recommendations expressed in this publication are those of the author(s) and do not necessarily reflect the views of the organizations or agencies that provided support for the project.

International Standard Book Number 13: 978-0-309-11404-2
International Standard Book Number 10: 0-309-11404-7

Available in limited supply from Board on Energy and Environmental Systems, National Research Council, 500 Fifth Street, NW, Keck W934, Washington, DC 20011, 202/334-3344.

Additional copies available for sale from the National Academies Press, 500 Fifth Street, NW, Keck 360, Washington, DC 20011, 800/624-6242 or 202/334-3313, Internet, http://www.nap.edu.

Printed in the United States of America

THE NATIONAL ACADEMIES

Advisers to the Nation on Science, Engineering, and Medicine

The **National Academy of Sciences** is a private, nonprofit, self-perpetuating society of distinguished scholars engaged in scientific and engineering research, dedicated to the furtherance of science and technology and to their use for the general welfare. Upon the authority of the charter granted to it by the Congress in 1863, the Academy has a mandate that requires it to advise the federal government on scientific and technical matters. Dr. Ralph J. Cicerone is president of the National Academy of Sciences.

The **National Academy of Engineering** was established in 1964, under the charter of the National Academy of Sciences, as a parallel organization of outstanding engineers. It is autonomous in its administration and in the selection of its members, sharing with the National Academy of Sciences the responsibility for advising the federal government. The National Academy of Engineering also sponsors engineering programs aimed at meeting national needs, encourages education and research, and recognizes the superior achievements of engineers. Dr. Charles M. Vest is president of the National Academy of Engineering.

The **Institute of Medicine** was established in 1970 by the National Academy of Sciences to secure the services of eminent members of appropriate professions in the examination of policy matters pertaining to the health of the public. The Institute acts under the responsibility given to the National Academy of Sciences by its congressional charter to be an adviser to the federal government and, upon its own initiative, to identify issues of medical care, research, and education. Dr. Harvey V. Fineberg is president of the Institute of Medicine.

The **National Research Council** was organized by the National Academy of Sciences in 1916 to associate the broad community of science and technology with the Academy's purposes of furthering knowledge and advising the federal government. Functioning in accordance with general policies determined by the Academy, the Council has become the principal operating agency of both the National Academy of Sciences and the National Academy of Engineering in providing services to the government, the public, and the scientific and engineering communities. The Council is administered jointly by both Academies and the Institute of Medicine. Dr. Ralph J. Cicerone and Dr. Charles M. Vest are chair and vice chair, respectively, of the National Research Council.

www.national-academies.org

COMMITTEE ON ENHANCING THE ROBUSTNESS AND RESILIENCE OF FUTURE ELECTRICAL TRANSMISSION AND DISTRIBUTION IN THE UNITED STATES TO TERRORIST ATTACK

M. GRANGER MORGAN, NAS,[1] Carnegie Mellon University, *Chair*
MASSOUD AMIN, University of Minnesota
EDWARD V. BADOLATO,[2] Integrated Infrastructure Analytics Inc.
WILLIAM O. BALL, Southern Company Services
ANJAN BOSE, NAE,[3] Washington State University
CLARK W. GELLINGS, Electric Power Research Institute
MICHEHL R. GENT, North American Electric Reliability Corporation (retired)
DIANE MUNNS, Edison Electric Institute
SHARON L. NELSON, State of Washington Attorney General's Office (retired)
DAVID K. OWENS, Edison Electric Institute
LOUIS L. RANA, Consolidated Edison Company of New York
B. DON RUSSELL JR., NAE,Texas A&M University
RICHARD E. SCHULER, Cornell University
PHILIP R. SHARP, Resources for the Future
CARSON W. TAYLOR, NAE, Bonneville Power Administration (retired)
SUSAN F. TIERNEY, Analysis Group
VIJAY VITTAL, NAE, Arizona State University
PAUL C. WHITSTOCK, Marsh USA Inc.

Project Staff

Board on Energy and Environmental Systems

ALAN CRANE, Study Director
DUNCAN BROWN, Senior Program Officer (part time)
HARRISON T. PANNELLA, Senior Program Officer (until July 2007)
JAMES J. ZUCCHETTO, Director, BEES

National Academy of Engineering Program Office

PENELOPE GIBBS, Senior Program Associate

[1]NAS, National Academy of Sciences.

[2]The committee notes with regret Edward Badolato's death in November 2008. It greatly appreciates his contributions to this report.

[3]NAE, National Academy of Engineering

BOARD ON ENERGY AND ENVIRONMENTAL SYSTEMS

Staff

NOTE: Board and staff membership as of the date of initial approval of this report in 2007.

Foreword

The electric power transmission and distribution system (the grid) is a critical and extraordinarily complex part of the nation's infrastructure. The National Academy of Engineering called the grid the world's largest integrated machine and a central part of the greatest engineering achievement of the 20th century—electrification of modern society. Reliable electricity service is essential to health, welfare, national security, communication, and commerce. Because of its scale, geographic reach, and complexity, however, the grid also poses many security challenges in maintaining reliable operation. Furthermore, more than 90 percent of the U.S. power grid is privately owned and regulated by the states, making it challenging for the federal government to address potential vulnerabilities to its operation, and perhaps especially its vulnerability to terrorist attack.

This report, prepared by a committee of dedicated experts assembled by the National Research Council (NRC), addresses those vulnerabilities and how they can be reduced. The committee began work in the fall of 2004 and completed it in the fall of 2007 with the intention of releasing the report by the end of that year. As required under the contract, the report was submitted to the sponsor, the Science and Technology Directorate of the Department of Homeland Security (DHS), for security classification review.

In August 2008, following protracted discussions regarding the information that would be suitable for public dissemination, DHS concluded that the report would be classified in its entirety under the original classification authority vested in the DHS undersecretary for science and technology. Because the committee believed that the report as submitted contained no restricted information, the NRC requested the formal classification guidance constituting the basis for the classification decision. That guidance was not provided, and so in August 2010, the NRC submitted a formal request for an updated security classification review. Finally, in August 2012, the current full report was approved for public release, reversing the original classification decision, except that several pages of information deemed classified are available to readers who have the necessary security clearance.

We regret the long delay in approving this report for public release. We understand the need to safeguard security information that may need to remain classified. But openness is also required to accelerate the progress with current technology and implementation of research and development of new technology to better protect the nation from terrorism and other threats.

Even though the committee's work was completed in 2007, the report's key findings remain highly relevant. We believe that we have a responsibility to make this report available to the public. Major cascading blackouts in the U.S. Southwest in 2011, and in India in 2012, underscore the need for the measures discussed in this report. The nation's power grid is in urgent need of expansion and upgrading. Incorporating the technologies discussed in the report can greatly reduce the grid's vulnerability to cascading failures, whether initi-

initiated by terrorists, nature, or malfunctions. In fact the report already has helped DHS focus on research aimed at developing a recovery transformer that could be deployed rapidly if many large power transformers were destroyed. Electric utilities and other private sector entities, state and local governments, and others involved with electric power are also likely to find the information in this report very useful. Concurrent with the report's release to the public, a workshop is being planned to address changes that have occurred since the report's completion in 2007. It is of vital interest to us all to ensure that the risk of a widespread, long-term blackout is minimized. We hope that the effort reflected in this report will contribute to achieving that goal.

Ralph J. Cicerone
President, National Academy of Sciences
Chair, National Research Council

Charles M. Vest
President, National Academy of Engineering
Vice-Chair, National Research Council

Preface

The electric power transmission and distribution systems are the wires and associated equipment that carry power from central generators to end users. Such systems provide almost all of the electricity that is essential for the operation of the economy and for human well-being. They also are difficult to protect and have been attacked by terrorists elsewhere in the world. Therefore, it is important to think about what can be done to make them less vulnerable to attack, how power can be rapidly restored if an attack occurs, and how important services can be sustained while the power is out. This report explores all of these issues, describes the current situation, and makes recommendations for improvements.

This report was requested by the U.S. Department of Homeland Security as part of its efforts to protect the nation's critical infrastructure. The National Research Council (NRC) established the Committee on Enhancing the Robustness and Resilience of Future Electrical Transmission and Distribution in the United States to Terrorist Attack to conduct the study. The committee's statement of task is given in Appendix A. Committee members were selected from academia, industry, state government agencies, and other organizations. They brought considerable expertise on electric power networks, their operation and regulation, security, and other issues. Biographical sketches of the committee members are presented in Appendix B.

The committee met six times in 2005 and 2006 to gather information from public sources (listed in Appendix C) and to discuss the key issues. It also held several conference calls.

Throughout the study the committee worked carefully to balance the need to explore issues with sufficient depth to ensure that key decision makers and other readers can understand the problem well enough to take informed action, while at the same time not laying out a "cookbook" that tells terrorists how to plan an attack that would do maximum damage. Thus, for example, the committee has been intentionally vague about some specific vulnerabilities or some modes of attack.

Chapter 1 frames the problem. It briefly describes the transmission and distribution systems; notes the differences between common disruptions and intentional attacks on the system; asks who might want to attack the system; and explores what the impact of such attacks might be.

Chapter 2 analyzes the structure and operation of the transmission and distribution system affecting the vulnerabilities that it faces. In the three chapters that follow the committee discusses the vulnerabilities of the system in terms of physical attack (Chapter 3); cyber security for guarding against/thwarting attacks on communications, sensors, and controls (Chapter 4); and the people who run, or have access to, the system (Chapter 5).

Chapter 6 focuses on how the system can be protected and how it can be modified to minimize the damage if it is attacked.

Once portions of the transmission and distribution system have been disrupted, restoring service becomes important. Chapter 7 discusses how this is currently done, how restoration

after a terrorist attack might be different, and what preparations need to be taken to deal with such events.

Because the nation's electric power transmission and distribution systems cannot be made completely impervious to harm from natural or terrorist causes, Chapter 8 explores a different part of the problem—how to ensure that critical services can be maintained if and when the power system is disrupted, especially for a lengthy period.

New technology can do much to reduce the vulnerability of the nation's electric power system to the risks posed by accidental and natural disruption and terrorist attack and reduce the costs of countering those risks. Chapter 9 explores research needs for reducing vulnerability and puts those in the context of overall electric power system R&D needs.

Chapters 2 through 5, which lay out the problems, end with a set of conclusions but no recommendations. Chapters 6 through 9 consider possible solutions to these problems. They end with both findings and recommendations. Chapter 10 draws these recommendations together and highlights those that the committee views as most important.

I greatly appreciate the efforts made by the many highly qualified experts on the committee. The committee operated under the auspices of the NRC Board on Energy and Environmental Systems and is grateful for the able assistance of James Zucchetto, Alan Crane, Panola Golson, and Duncan Brown of the NRC staff, and of Penelope Gibbs of the NAE Program Office staff.

M. Granger Morgan, *Chair*
Committee on Enhancing the Robustness and Resilience
of Future Electrical Transmission and Distribution
in the United States to Terrorist Attack

Acknowledgments

The Committee on Enhancing the Robustness and Resilience of Electrical Transmission and Distribution in the United States to Terrorist Attacks is grateful to the many individuals who contributed their time and effort to this National Research Council (NRC) study. The presentations at committee meetings provided valuable information and insight on electricity technologies and system operations. The committee thanks the following individuals who provided briefings:

Edward V. Badolato, Integrated Infrastructure Analytics Inc.,
William Ball, Southern Company Services,
Tom Bowe, PJM Interconnection,
John Caskey, National Electrical Manufacturers Association,
Christopher L. DeMarco, University of Wisconsin-Madison,
James Fama, Edison Electric Institute,
Joseph Fiorito, Caterpillar Inc.,
Clark Gellings, Electric Power Research Institute,
Michehl R. Gent, North American Electric Reliability Council,
David Hall, Tennessee Valley Authority,
David Hawkins, California ISO,
Bruce A. Hedman, Energy and Environmental Analysis Inc.,
David Meyer, U.S. Department of Energy,
Scott Mix, KEMA Inc.,
Dave Nevius, North American Electric Reliability Council,
David K. Owens, Edison Electric Institute,
William Parks, U.S. Department of Energy,
Lou Rana, Consolidated Edison Company of New York,
William Rees Jr., U.S. Department of Homeland Security,
Julio Rodriguez, Idaho National Laboratory,
Robert Schainker, Electric Power Research Institute,
Gene Tsudik, University of California, Irvine, and
Joseph Weiss, KEMA Inc. (via telephone).

This report has been reviewed in draft form by individuals chosen for their diverse perspectives and technical expertise, in accordance with procedures approved by the NRC's Report Review Committee. The purpose of the independent review is to provide candid and critical comments that will assist the institution in making its published report as sound as possible and to ensure that the report meets institutional standards for objectivity, evidence, and responsiveness to the study charge. The review comments and draft manuscript remain

confidential to protect the integrity of the deliberative process. We wish to thank the following individuals for their review of this report:

Daniel Bienstock, Columbia University,
Earl Boebert, Sandia National Laboratories (retired),
Tom Bowe, PJM Interconnection,
Doug Chapin (NAE), MPR Associates,
Thomas Garrity, Siemens Power Transmission & Distribution,
Michael Greenberg, Rutgers University,
Thomas Overbye, University of Illinois at Urbana-Champaign,
Larry Papay (NAE), Science Applications International Corporation (retired),
Walter Robb (NAE), Vantage Management,
Hal Scherer (NAE), Commonwealth Electric Company (retired),
Rick Sergel, North American Electric Reliability Corporation, and
Irvin (Jack) White, New York State Energy Research and Development Authority (retired).

Although the reviewers listed above have provided many constructive comments and suggestions, they were not asked to endorse the conclusions or recommendations, nor did they see the final draft of the report before its release. The review of this report was overseen by Chris Whipple, Review Monitor, and Naraim G. Hingorani, Review Coordinator. Appointed by the National Research Council, they were responsible for making certain that an independent examination of this report was carried out in accordance with institutional procedures and that all review comments were carefully considered. Responsibility for the final content of this report rests entirely with the authoring committee and the institution.

The individuals listed below responded to the committee's questionnaire on research and development needs for transmission and distribution systems, as discussed in Chapter 9. This exercise was important in helping the committee to prioritize R&D needs for countering terrorism.

Michael F. Ahern, Northeast Utilities,
Kenneth Anderson, Tri-State Generation & Transmission Association Inc.,
Navin B. Bhatt, American Electric Power Service Corp.,
Steve DeCarlo, New York Power Authority,
John L. Del Monaco, Public Service Electric & Gas Co.,
Douglas R. Fitchett, American Electric Power Service Corp.,
Brice Freeman, Electric Power Research Institute,
Paul Hines, Carnegie Mellon University,
Jim Hunter, International Brotherhood of Electrical Workers,
Ed Jakubiak, Detroit Edison Co.,
Gregg Lawry, Alliant Energy Corporation,
Glenn L. McCullough Jr., TVA (retired),
William E. Muston, TXU Power,
James T. Rhodes, Virginia Power (retired),
David E. Schleicher, PPL Electric Utilities Corp.,
David G. Victor, Stanford University, and
Thomas M. Wick, We Energies.

Contents

APPENDIXES

Tables, Figures, and Boxes

TABLES

FIGURES

BOXES

Summary

The electric power delivery system that carries electricity from large central generators to customers could be severely damaged by a small number of well-informed attackers. The system is inherently vulnerable because transmission lines may span hundreds of miles, and many key facilities are unguarded. This vulnerability is exacerbated by the fact that the power grid, most of which was originally designed to meet the needs of individual vertically integrated utilities, is now being used to move power between regions to support the needs of new competitive markets for power generation. Primarily because of ambiguities introduced as a result of recent restructuring of the industry and cost pressures from consumers and regulators, investment to strengthen and upgrade the grid has lagged, with the result that many parts of the bulk high-voltage system are heavily stressed.

A terrorist attack on the power system would lack the dramatic impact of the attacks in New York, Madrid, or London. It would not immediately kill many people or make for spectacular television footage of bloody destruction. But if it were carried out in a carefully planned way, by people who knew what they were doing, it could deny large regions of the country access to bulk system power for weeks or even months. An event of this magnitude and duration could lead to turmoil, widespread public fear, and an image of helplessness that would play directly into the hands of the terrorists. If such large extended outages were to occur during times of extreme weather, *they could also result in hundreds or even thousands of deaths due to heat stress or extended exposure to extreme cold.*

The largest power system disruptions experienced to date in the United States have caused high economic impacts. Considering that a systematically designed and executed terrorist attack could cause disruptions that were even more widespread and of longer duration, it is no stretch of the imagination to think that such attacks could entail costs of hundreds of billions of dollars—that is, perhaps as much as a few percent of the U.S. gross domestic product (GDP), which is currently about $12.5 trillion.

Electric systems are not designed to withstand or quickly recover from damage inflicted simultaneously on multiple components. Such an attack could be carried out by knowledgeable attackers with little risk of detection or interdiction. Further well-planned and coordinated attacks by terrorists could leave the electric power system in a large region of the country at least partially disabled for a very long time. Although there are many examples of terrorist and military attacks on power systems elsewhere in the world, to date international terrorists have shown limited interest in attacking the U.S. power grid. However, that should not be a basis for complacency. Since all parts of the economy, as well as human health and welfare, depend on electricity, the results could be devastating.

This report focuses on measures that could:

1. Make the power delivery system less vulnerable to attacks,
2. Restore power faster after an attack,
3. Make critical services less vulnerable while the delivery of conventional electric power has been disrupted.

THE NATURE OF THE PROBLEM

The U.S. power delivery system is remarkably complex. It is a network of substations, transmission lines, distribution lines, and other components that people can see as they drive around the country; it also includes the less visible devices that sense and report on the state of the system, the automatic and human controls that operate the system, and the intricate web of computers and communication systems that tie everything together. Enormous complexity and diversity also characterize the organizations and human systems that operate and manage the power delivery system. That complexity and diversity have become even greater in recent years as some parts of the system have been restructured while others

have not, and as the role of state and federal regulators and other oversight bodies has shifted.

Today most power is generated by large central generating stations that are located far from the customers they serve. Transformers increase the voltage so that it can be carried efficiently over long distances. Substations then reduce the voltage and carry the power into the distribution network for delivery to customers.[1] Unlike trains or natural gas in pipelines, electric power cannot simply be sent via specific lines wherever dispatchers choose. Current flows through the system according to a set of physical laws. The system must be continually adjusted to keep all parts synchronized and in electrical balance. If corrections are not made immediately when imbalances occur, the result can be oscillations and other disturbances in the system that can result in a cascading failure over a wide area, as happened in the Northeast blackout of 2003.

Recent years have witnessed dramatic organizational changes in the U.S. electric power system. In some states, traditional vertically integrated companies that owned and operated the entire system from the generators to the customers' meters have been restructured in an effort to introduce competition. However, a few states are trying to undo some of the changes, and some states may never restructure. The push by federal regulators to introduce competition in bulk power across the country also has resulted in the transmission network being used in ways for which it was not designed. There have also been shifts in the relative responsibility of state and federal regulators.

Largely as a consequence of the uncertainties introduced by these changes, incentives for investment by private firms have become mixed, with the result that the physical capabilities of much of the transmission network have not kept pace with the increasing burden that is being placed on it. Other trends are more promising. The Energy Policy Act of 2005 includes provisions to strengthen the electric grid, including provisions for the introduction of mandatory reliability standards. Although not aimed specifically at protecting the grid against terrorism, the activities initiated under this statute will—if implemented—lead to a more robust transmission system that will be better able to withstand major disruptions.

Physical Vulnerability

Disruption in the supply of electric power can result from problems in any part of the system. The primary concern of this report is with power delivery. Substations and the large high-voltage transformers they contain are especially vulnerable, as are some transmission lines where the destruction of a small number of towers could bring down many kilometers of line. Terrorist attacks on multiple-line transmission corridors could cause cascading blackouts.

High-voltage transformers are of particular concern because they are vulnerable to attack, both from within and from outside the substation where they are located. These transformers are very large, difficult to move, custom-built, and difficult to replace. Most are no longer made in the United States, and the delivery time for new ones can run to months or years. The industry has made some progress toward building an inventory of spares, but these efforts could be overwhelmed by a large attack. Although easier to move and replace, other large components, such as high-voltage circuit breakers, are also a concern.

These problems are exacerbated by the current state of the transmission grid. It is aging and increasingly stressed, leaving it especially vulnerable to multiple failures following an attack. Many important pieces of equipment are decades old and lack improved technology that could help limit outages.

Cyber Vulnerability

Modern power systems rely heavily on automation, centralized control of equipment, and high-speed communications. The most critical systems are the supervisory control and data acquisition (SCADA) systems that gather real-time measurements from substations and send out control signals to equipment, such as circuit breakers. The many other control systems, such as substation automation or protection systems, can each only control local equipment. Other online computer systems, such as energy management systems (which analyze the reliability of the system against contingencies) or market systems (which manage the buying and selling of electricity), have only an indirect impact on the grid. But all such systems are potentially vulnerable to cyber attacks, whether through Internet connections or by direct penetration at remote sites. Any telecommunication link that is even partially outside the control of the system operators is a potentially insecure pathway into operations and a threat to the grid.

If they could gain access, hackers could manipulate SCADA systems to disrupt the flow of electricity, transmit erroneous signals to operators, block the flow of vital information, or disable protective systems. Cyber attacks are unlikely to cause extended outages, but if well coordinated they could magnify the damage of a physical attack. For example, a cascading outage would be aggravated if operators did not get the information to learn that it had started, or if protective devices were disabled.

Personnel Vulnerability

Workforce issues are critically important to maintaining a reliable supply of electricity, particularly in the event of a terrorist attack. Utility employees and contractors interact with the electric power system as managers, operators, line-crews,

[1] A few transmission lines operate with direct current (DC), which requires conversion from alternating current (AC) at one substation and then back again at the receiving substation. DC also is used to interconnect the four major regions in the United States and Canada because its use avoids the necessity of keeping their AC systems synchronized.

suppliers of materials and services, and users, among other roles. Although workers and managers in this industry have an outstanding record of reliable performance, even a few pernicious people in the wrong place are a potential source of vulnerability should they choose to disrupt the system.

A second issue is that, to a greater extent than in most other industries, the electricity workforce is aging, and many skilled workers and expert engineers will soon retire. As the current workforce retires, utilities may have increasing difficulty hiring sufficient qualified replacements to keep the system operating effectively and reliably and to undertake all the upgrades that are needed, let alone cope with damage from terrorist attacks. This issue requires sustained and high-level attention by both the industry and federal agencies.

REDUCING RISKS

Reduce Vulnerability

The extent of the damage from an attack can be limited by a variety of means, including improving the robustness of the system to withstand normal failures; adding physical and cyber protections to key parts of the system; and designing it to degrade gracefully after catastrophic damage, leaving as many areas as possible still with power. Research and development can make particularly important contributions in these areas. Table S.1 lists examples of changes that could be made starting now and others that could become options in the long term. Many of the changes discussed in this report

TABLE S.1 Examples of Options for Minimizing Vulnerability

	Selected Options Currently Available	Selected Options That R&D Could Make Available
Physical vulnerability	Hardening of key substations and control centers Increased physical surveillance Addition of transmission towers that can prevent domino-like collapse For additional examples, see Chapter 3	Improved intrusion sensors Development of strategies to provide greater system capacity Greater use of distributed generation and micro-grids For additional examples, see Chapter 9
Cyber vulnerability	Elimination of all non-essential pathways to external systems Use of high-quality cyber security on all links For additional examples, see Chapter 4	Improved cyber security for sensors, communication, and control systems Systems to monitor for, and help avoid, operator error For additional examples, see Chapter 9
Personnel vulnerability	Improved employee and contractor screening Improved training for attack response Improved planning and coordination with government (especially law enforcement) For additional examples, see Chapter 5	Improved training simulators Expansion of support for educational programs in power engineering that have atrophied in large part because of very limited research investment For additional examples, see Chapter 9
Increased system robustness and graceful degradation	A change in institutional arrangements and incentives to ensure adequate modernization of the transmission system Greater use of high-voltage power electronic technology Greater use of DC interconnects Expanded and more selective demand-side management and distribution automation For additional examples, see Chapter 6	Lower-cost undergrounding Improved probabilistic vulnerability assessment Improved sensors, communication, real-time analysis, and system visualization Improved automatic control Improved capability for islanding and self-healing Improved energy storage For additional examples, see Chapter 9
Accelerated restoration	Expanded planning for very large outages Designation of some utility employees as first responders. For additional examples, see Chapter 7	Development and stockpiling of restoration transformers and other key equipment of long leadtime Improved assessment and planning tools For additional examples, see Chapter 9
Maintenance of critical services while grid power is disrupted	Use of robust systems such as light-emitting diode (LED) traffic lights with trickle charge batteries Co-location of generation with critical loads such as pumps for water supply Comprehensive contingency planning Avoidance of cross-dependencies (e.g., backup power for cell phone sites; gas rather than electric pumps on gas pipelines) For additional examples, see Chapter 8	Massively distributed architectures Improved energy storage For additional examples, see Chapters 8 and 9

could convert an attack that today could cause a blackout over a wide region of the country into one that would do less damage to the electric system and leave the system in a better position to accommodate the damage that does occur. Cascading failures could be limited, and many areas within a blacked-out region could maintain power because they could isolate themselves from the failing grid and maintain a balance of generation and demand within their borders.

Physical protection of critical facilities includes hardened enclosures for key transformers, improved electronic surveillance, and system tools that can identify physical and control system problems and potential incidents. Such measures may deter as well as blunt an attack.

Cyber security is best when interconnections with the outside world are eliminated. When interconnections are unavoidable, best practices for security must apply. Wireless communications within substations is a particular concern.

The risk of insider-assisted attacks can be reduced by strengthening background checks for new and existing employees and contractors. If subversive or disaffected workers can be identified, attackers will lose a major potential advantage. Training operators and other workers to recognize and react to attacks or other major disruptions will be helpful in limiting the extent of outages and further damage during a cascading failure. System simulators are likely to be very useful in this endeavor. In the long term, supporting engineering and other technical education will help to maintain the availability of the necessary skills in the workforce.

Even if terrorist attacks were not a concern, the transmission system should be modernized and upgraded to handle the increasing flow of power. A robust, modern system could ride out disturbances that would cause major problems to today's stressed system. The new operating standards being prepared by the electric industry and its reliability organizations under the Energy Policy Act of 2005 (EPAct) will help, but EPAct doesn't directly grant authority to order upgrades in the physical system. Industry, the Federal Energy Regulatory Commission (FERC), the Department of Energy (DOE), and state public utility commissions are aware of such needs, but building new transmission lines and other delivery enhancements is expensive and difficult. Upgrading sensors and controls can allow more power to flow on existing lines, which will help under some conditions. The terrorist threat suggests that additional upgrades may be important to reduce major outages. Current standards are met if no significant outage occurs following the failure of one major line or certain related double outages. Damage by terrorists could greatly exceed this level. A higher standard would be to maintain reliability when two major related failures occur, known as an $N - 2$ event, which, in most cases, would entail additional costs. Improving the information flow to operators and the tools they can use to analyze and react to disturbances also would help prevent outages from cascading.

In the longer term, changes to the configuration of the power system could have dramatic impacts on its vulnerability. Among these, increasing generation within or close to major load centers, expanded use of distributed resources (co-generation, micro-grids) with associated automatic control, and the successful development and deployment of storage technology would help limit cascading failures and leave islands of power within a blacked-out region.

Expedite Restoration

After an attack, an electric utility's main focus will be on restoring power to its customers. Many of the steps to be taken would be similar to those taken in response to a major natural disaster, such as a hurricane: that is, identify the damage, clean it up, repair equipment, and restore power. However, there are also important differences. Unlike hurricanes, terrorists may strike with no warning and selectively destroy the most important facilities, such as major substations. Some of the lost equipment may take months or even years to replace. Unless prior arrangements have been worked out, law enforcement officers might exclude utility workers from the crime scene while they investigate, delaying assessment of the damage and restoration activities. In addition, utility workers might be subjected to unexpected risks, such as chemical contamination.

Although detailed restoration plans cannot be formulated until specific damage is identified and the extent of an outage determined, advance planning can greatly speed the process of recovery. This is a well-established tenet in the industry. Utilities and transmission operating entities can—and do—make contingency plans. In preparing for a possible terrorist attack, they should set up an incident command system, establish good communications with government agencies, and reach agreements as to responsibilities and authority over various aspects of the restoration. Further work to address any specific issues that might arise in a terrorist incident is critical. Designating utility workers as first responders would improve their access to damaged substations and other facilities to assess the damage. Drills should be conducted for plausible scenarios of destruction to ensure that plans are adequate.

Key equipment, especially *large power transformers*, can be backed up with spares. The Edison Electric Institute (EEI) is developing the Spare Transformer Equipment Program (STEP), which will make spare transformers available in case of emergency. These transformers are very expensive, and not many spares are available. Transformers are also very large, heavy, and difficult to move. A major attack could quickly exhaust the inventory, and the world has limited manufacturing capacity. A promising solution is to develop, manufacture, and stockpile a family of universal recovery transformers that would be smaller and easier to move. These would be less efficient than those normally operated and so would only be for temporary use, but they could drastically reduce the delay before the electric system is back in full operation. Emergency backup policies also should be imple-

mented for other key equipment such as large bushings and circuit breakers, which could take many weeks to replace.

Utility restoration workers need adequate food, water, fuel for vehicles, and other essentials that may not otherwise be available during an extended outage. Communication networks also may degrade or fail in an extended outage, and it is essential that utilities have backup systems available that can be operated without grid power.

In addition, utilities and transmission operators should ensure that sufficient generating plants have black-start capability. This is provided by units that can be started with no offsite power available, a likely situation in a widespread blackout.

Reduce Vulnerability of Critical Services in the Event of Outages

Society is becoming ever more dependent on electric power. While system owners and operators should do all that they reasonably can to ensure that their systems are able to withstand anticipated assaults from natural and human sources, there are practical limits to how much these highly distributed systems can be hardened. Even without the threat of terrorism, there is a risk of occasional power outages, some of which will have large spatial scale and may last for many hours or even days. Terrorism increases the probable extent and duration of such outages and could cause them to occur at particularly inconvenient or damaging moments.

Since the complete elimination of all possible modes of failure is simply not feasible, an important design objective (in addition to resilience and the ability to rapidly restore the system after a problem occurs) should be the ability to sustain critical social services while an outage persists. Thus, in addition to strengthening the grid, society should also focus on identifying critical services and developing strategies to keep them operating in the event of power outages—be they accidental or the result of terrorist attack.

Strategies for managing an extended outage will require detailed planning and preparation to ensure that critical facilities can continue to operate, either from the remaining grid or from emergency power systems. Metropolitan areas with high demand and high reliance on transmission to deliver power from distant generating stations should be of particular concern in this regard. Critical facilities (such as hospitals) often have emergency backup power generation capability, but some of these are only intended to operate for several days. An extended outage could easily exhaust the supply of fuel. Many critical service providers have no emergency power at all.

Although it is not reasonable to expect federal support for all local and regional planning efforts, the Department of Homeland Security (DHS) and/or the DOE should each initiate and fund several model demonstration assessments at the level of cities, counties, and states. These assessments should systematically examine a region's vulnerability to extended power outages and develop cost-effective strategies that can be adopted to reduce or, over time, eliminate such vulnerabilities. Building on the results of these model assessments, DHS should develop, test, and disseminate guidelines and tools to assist other cities, counties, states, and regions to conduct their own assessments and develop plans to reduce their vulnerabilities to extended power outages. To facilitate these activities, public policy and legal barriers to communication and collaborative planning will need to be addressed.

At a national level, DHS should perform, or assist other federal agencies to perform, additional systematic assessment of the vulnerability of national infrastructure, such as telecommunications and air traffic control, in the face of extended and widespread loss of electric power, and then develop and implement strategies to reduce or eliminate vulnerabilities. Part of this work should include an assessment of the available surge capacity for large mobile generation sources. Such an assessment should include an examination of the feasibility of utilizing alternative sources of temporary power generation to meet emergency generation requirements (as identified by state, territorial, and local governments, the private sector, and nongovernmental organizations) in the event of a large-scale power outage of long duration.

Government entities need to provide incentives (e.g., grants, fee-based awards, taxes, regulation) to support incremental costs associated with public and private sector risk prevention and mitigation efforts to reduce the societal impact of an extended grid outage. Such incentives could include incremental funding for those aspects of systems that provide a public good but no private benefit and the development and implementation of building codes or ordinances that require alternative or backup sources of electric power for key facilities.

THE IMPORTANCE OF INVESTMENT IN RESEARCH

There are many technologies and strategies that could be employed to make the power system more robust in the face of terrorist attack, make service restoration more timely after an attack, and continue the provision of critical services while the power is out. The best way to make needed changes affordable, and to develop new, even more effective and affordable approaches, is through research. Chapter 9 of this report discusses the current state of research for electric power, along with a set of recommendations for addressing research needs and developing related strategies.

The research that is needed to address the problems of terrorism is, for the most part, the same as the research that would address the broad problems faced by the transmission and distribution grid. The recovery transformer noted above is one of the few exceptions of terror-specific technologies that should be pursued. For example, the advanced computational system under development to improve control of flows on the grid also would be very useful in minimizing a cas-

cading failure after a terrorist attack. The committee reached this conclusion in part from an informal questionnaire the committee developed and distributed to leading technical experts in the field. This questionnaire identified a variety of potential short- and long-term R&D needs for transmission and distribution. Respondents were asked to prioritize needs first for the industry as a whole and then strictly in terms of reducing vulnerability to terrorism. With a few exceptions, the research needs in the two cases were identical.

The committee is very concerned that the level of actual investment in power system research is currently *much* smaller than it should be as measured according to a variety of societal metrics. However, agreeing on institutional arrangements that can significantly increase the levels of nongovernmental research investment in this field has been a persistent problem. Chapter 9 discusses one possible strategy, but the committee was unable to reach a unanimous view on how best to resolve this problem.

WHAT SHOULD THE DEPARTMENT OF HOMELAND SECURITY DO?

The level of protection for and resiliency of the electric power grid against terrorist attacks needs to increase. However, the level of security that is economically rational for most infrastructure operators will be less than the level that is optimal from the perspective of the collective national interest. Therefore, the DHS should develop a coherent plan to address the incremental cost of upgrading and protecting critical infrastructure to that higher level.

In the specific context of electric power delivery, the Department of Homeland Security should:

- **Recommendation 1** Take the lead and work with the DOE and with relevant private parties to develop and stockpile a family of easily transported high-voltage recovery transformers and other key equipment. Although the expected benefits to the nation of such a program are difficult to quantify, they would certainly be many times its cost if the transformers are needed (see Chapters 3, 6, and 9).
- **Recommendation 2** Work to promote the adoption of many other technologies and organizational changes, identified in this report, that could reduce the vulnerability of the power delivery system and facilitate its more rapid restoration should an attack occur (see Chapters 6 and 7).
- **Recommendation 3** Work with the power industry to better clarify the role of power system operators after terrorist events through the development of memoranda of understanding and planned and rehearsed response programs that include designating appropriate power-system personnel as first responders (see Chapters 7 and 8).
- **Recommendation 4** Offer assistance to the Federal Energy Regulatory Commission, to state public service commissions, and to other public and private parties in finding ways to ensure that utilities and transmission operators have appropriate incentives to accelerate the process of upgrading power delivery and eliminating its most obvious vulnerabilities (see Chapter 6).
- **Recommendation 5** Work with the Department of Energy and the Office of Management and Budget to substantially increase the level of federal basic technology research investment in power delivery. The committee notes that (1) much of what is needed has the nature of a "public good" that the private sector will not develop on its own; (2) current levels of research investment are woefully inadequate; and (3) most of the system's vulnerabilities to terrorism are integrally linked to other more general problems and vulnerabilities of the system and cannot be resolved in isolation (see Chapter 9).
- **Recommendation 6** Take the lead in initiating planning at the state and local level to reduce the vulnerability of critical services in the event of disruption of conventional power supplies, and offer pilot and incremental funding to implement these activities where appropriate (see Chapter 8).
- **Recommendation 7** Develop a national inventory of portable generation equipment that can be used to power critical loads during an extended outage. Explore public and private strategies for building and maintaining an adequate inventory of such equipment (see Chapter 8).

1

The Electric Transmission and Distribution System as a Terrorist Target

Terrorists could destroy key elements of the electricity generation and delivery system, causing blackouts that are unprecedented in this country in duration and extent. The U.S. economy depends on a reliable supply of electricity, and widespread disruptions of long duration could cause enormous economic damage and suffering. Under some circumstances (e.g. a heat wave) such blackouts could also lead to significant loss of life. On the other hand, attacks on the U.S. power system would not immediately kill large numbers of people or cause massive destruction of familiar structures or facilities, and therefore probably would not be as dramatic as the September 11, 2001, attacks.

There is considerable debate over just how serious a threat terrorists pose to U.S. infrastructure such as the electric transmission and distribution system (NRC, 2002; Meade and Molander, 2006; Mueller, 2006). Electricity is ubiquitous, reliable, and taken for granted . . . until the lights go out. Occasional large accidental outages caused by "cascading failures" in the high voltage transmission system (such as the Northeast blackout of August 2003) have briefly raised public concern about potential vulnerabilities, but to date such concerns have rapidly disappeared once power is restored. Power outages caused by damage to the distribution system, the lower voltage lines that carry power to customers, are far more common. Recent examples include the destruction after hurricanes in Florida and the Gulf Coast, as well as the July 2006 outage in New York City's borough of Queens.

While the inconvenience and cost of these accidental disruptions of the nation's transmission and distribution system have been large, they pale in comparison with the impacts that might result from a large, well planned, terrorist attack. Even if the probability of such an intentional attack were assessed to be quite low, the consequences are large enough that the nation needs to protect this essential service.

This chapter briefly reviews the electric power system and its vulnerabilities, identifies the types and motivations of potential attackers, explores the potential costs associated with the loss of power, and reviews a few of the actions that have been taken to date to reduce vulnerability.

THE ELECTRIC POWER SYSTEM AND ITS VULNERABILITY

Today in the United States, and in most of the rest of the industrialized world, power flows from large generating plants to customers through a complex, dynamic system whose structure is the result of gradual evolution over more than a century. Early power systems had small generating stations close to local distribution systems that fed power to streetlights and homes at relatively low voltage. As systems became larger and power had to be carried over longer distances, power lines were operated at ever higher voltage in order to minimize losses. Efficient high-voltage transmission lines also made it possible to locate ever larger generators in remote areas rather than close to towns and cities. By the middle of the 20th century, system operators began to connect individual high-voltage systems together so that power could be moved from region to region, both to promote economic efficiency and to increase reliability by making it possible to move power into regions suffering from temporary shortages.

Once electric power has been generated, the voltage is stepped up[1] and power moves over long distances through the high-voltage transmission system, a complex network of lines, most of which are carried aboveground on tall towers. At key points throughout this system are substations that contain transformers to increase and decrease the voltage, switching gear that connects the system in desired configura-

[1]The voltage of AC power can be easily increased or decreased using transformers. High voltage is used to move power long distances in order to minimize losses that result from the current heating the line. The power carried by a line is the product of the current and the voltage. However, for a given line, losses from heating go up as the square of the current. In moving a given amount of power, using a higher voltage reduces the current, and thus reduces the loss due to heating.

tions, and circuit breakers that open and close connections while also acting as giant fuses to protect expensive equipment from damage, as well as a variety of other devices. Most substations sit out in the open protected only by a simple chain-link fence. All but a few high voltage lines are also in the open. Thus, both substations and the lines that connect them are vulnerable to damage from storms and to terrorist attack.

When power reaches an area where it will be used, the voltage is reduced and power is distributed to customers over lower-voltage distribution lines. Unlike the transmission system, which is a large interconnected network, many distribution systems branch out radially to deliver power to customers, although some older, dense urban areas, such as New York City, use network configurations for distribution. All the elements of the transmission system, and increasingly those of the distribution system, are monitored and controlled by information and communication systems.

Although problems in any part of the system can disrupt the supply of electric power, this report focuses on the transmission and distribution (T&D) system, substations, and other associated parts, discussing generation only as it relates to issues involving transmission and distribution. Details on how the T&D system is controlled, operated, managed, and regulated are given in Chapter 2.

Non-malicious Threats to the Electricity Delivery System

By its very nature, the T&D system is not perfectly reliable. Even without terrorist activity, the power sometimes goes out, usually for just a few seconds, minutes, or hours, but sometimes for a few days. On very rare occasions, and in limited locations, outages may stretch on for weeks. As the duration and geographic extent of an outage increase, people become seriously inconvenienced, and economic and other costs rise, but people generally do not experience "terror."

Keeping power flowing to customers is a continuous process of control, recovery, and repair. Most outages are local, brief in duration, and caused by problems at the level of the distribution system—such as lightning strikes, wind storms and tree falls, short circuits caused by wild animals such as squirrels, vehicles that crash into power poles, and similar events. Line crews can usually fix these outages in a matter of hours. Distribution systems that incorporate automation can often isolate a problem and restore service for many affected customers in a matter of seconds or minutes.

Outages caused by disruptions in the high-voltage transmission system are less common. When they do occur, because of faulty equipment, weather, or for other reasons, many such outages are never noticed by customers, because automatic controls and system operators can limit their impact and maintain the supply of power to the distribution system. But, of course, the transmission system does occasionally experience problems that result in loss of service to customers. Weather events, such as hurricanes and ice storms, earthquakes, and similar natural events, can bring down many transmission lines, and, less frequently, can damage transformers, circuit breakers, and other equipment such as the terminal facilities for direct-current (DC) lines. Inadequate attention to maintenance can also contribute to blackouts—as in the recent case of an improperly sized circuit breaker in London, or several instances of arcing to vegetation that have resulted from inadequate tree trimming in the United States.

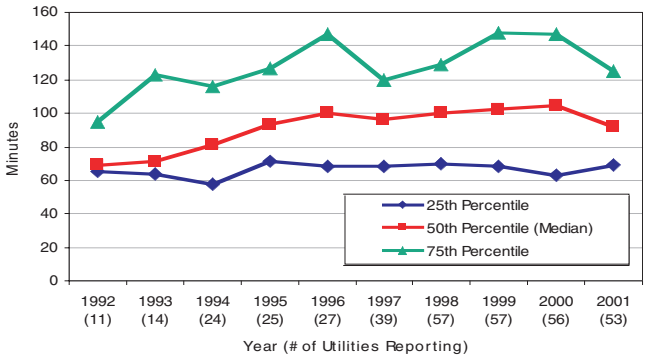


FIGURE 1.1a System Average Interruption Duration Index (SAIDI) indicators for U.S. utilities for the period 1992 to 2001 (excluding major events). SOURCE: EPRI (2003).

As explained in greater detail in Chapter 2, the transmission system is much more stressed, and thus more vulnerable, than it was a few decades ago, principally as a result of two factors: (1) years of underinvestment in system upgrades stemming from ambiguities and altered incentives that resulted from electric power restructuring and associated changes in the regulatory environment and (2) demands on the system to move power between sellers and buyers in new competitive power markets in greater volume and in ways in which the system was not designed to operate.[2]

Figures 1.1a and 1.1b show the trend in two common measures of power supply disruption in the United States over the decade from 1992 to 2001—the System Average Interruption Duration Index (SAIDI), which indicates the average time that customers are without power during the period analyzed (Figure 1.1a), and the System Average Interruption Frequency Index (SAIFI), which indicates the average number of interruptions per customer served per year (Figure 1.1b). Both reflect principally the effects of distribution system disturbances and exclude outages caused by major events. Figures 1.2a and 1.2b show SAIDI and SAIFI measures of reliability internationally. Reliability in the United States appears to be poorer, on average, than that experienced by customers for electric power in some other

[2]Much of the transmission system was originally designed to serve the needs of vertically integrated regulated utilities. Following deregulation of the power industry and the introduction of competition among generators, the transmission system is now being expected to move power in ways that have resulted in patterns of power flow that did not exist previously under regulation.

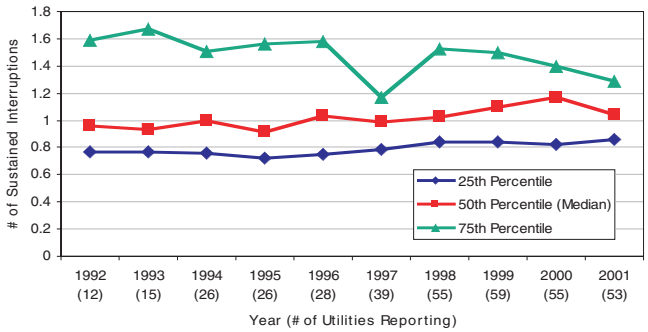


FIGURE 1.1b System Average Interruption Frequency Index (SAIFI) indicators for U.S. utilities for the period 1992 to 2001 (excluding major events). SOURCE: EPRI (2003).

developed countries, although much of this difference is due to major differences in population density and power system configurations.

As indicated in Figure 1.3, large outages in the United States between 1984 and 2000 were more frequent than might have been anticipated on the basis of a simple exponential distribution. Although in recent years in the United States there has been no significant change in the frequency of outages (Figure 1.4), there has been a very significant increase in the frequency of transmission loading relief events (Figure 1.5).[3]

Most problems occurring in the transmission of electric power can easily be corrected by automatic controls and actions taken by system operators. However, occasionally these actions are not sufficient to keep power flowing. Problems or failures originating in one part of the system may give rise to problems (such as overloads) in other parts of the system, which in turn cause additional problems that may ultimately result in a cascading power failure. The fact that the power system uses alternating current (AC) means that the system's behavior is sometimes further complicated by oscillatory or other complex dynamic behavior, as illustrated in Figure 1.6. Although they are rare, such events sometimes cause a loss of power to many customers (Table 1.1 and Figure 1.3).

Potential Attacks on the Electric Power System

Because electricity is so essential to modern industrialized societies, the power system has frequently been identified as a potential terrorist target. For example, more than 15 years ago, in a report titled Physical Vulnerability of the Electric System to Natural Disasters and Sabotage (OTA, 1990. p. 14), the Office of Technology Assessment concluded:

> Some terrorist groups hostile to the United States clearly have the capability of causing massive damage—the loss of so many generating or transmission facilities that major metropolitan areas or even multi-state regions suffer severe, long-term, power shortages. The absence of such attacks has as much to do with how terrorists view their opportunities as with their ability. U.S. electric power systems are only one target out of many ways of striking at America, and not necessarily the most attractive.

More recently, the National Research Council report Making the Nation Safer (NRC, 2002. p. 178) noted that:

> [a]nalysis of possible targets, weapons, and delivery systems and of direct and indirect consequences reveals several very dangerous scenarios. The scenarios of greatest concern involve the electrical system. When service is lost, there are immediate consequences to every person, home, and business. An extended outage of electricity would have profound consequences.

The same report emphasized (p. 180):

> [t]he impact of a prolonged interruption in the electric power supply to any region of the country would be much larger than the economic loss to the energy sector alone. . . . The nation's electric power systems must clearly be made more resilient to terrorist attack.

Potential attackers, as shown in Figure 1.7, include the following.

Terrorists

Most problematic are terrorist groups with significant technical capabilities and resources who want to kill large numbers of people or cause widespread societal or economic damage. Although not very likely, as noted above, such terrorists might view the power system as a primary target. As discussed later in this chapter, a sophisticated attack could cause a lengthy blackout over an extensive region. An attack during a period of extreme weather, such as a heat wave, might lead to the deaths of many people, albeit in a far less spectacular way than in a large explosion or a chemical or biological attack. However, the drawn-out agony produced by such an attack would clearly create great public anxiety and outrage, especially if government and private responses were seen as inadequate, and perhaps, too, if the first attack were followed by other similar attacks. Public confidence could also be eroded, and anger heightened, if terrorists were able to hold the grid hostage by mounting limited demonstration attacks with promises of worse to come if demands were not met.

Although international terrorist groups such as al-Qaeda have been more interested in killing people that in causing economic damage, different groups with different motivations could emerge. An attack that brought a power system

[3]A transmission loading relief event occurs when congestion on the transmission system prevents the transmission of electricity for which a transaction has been contracted.

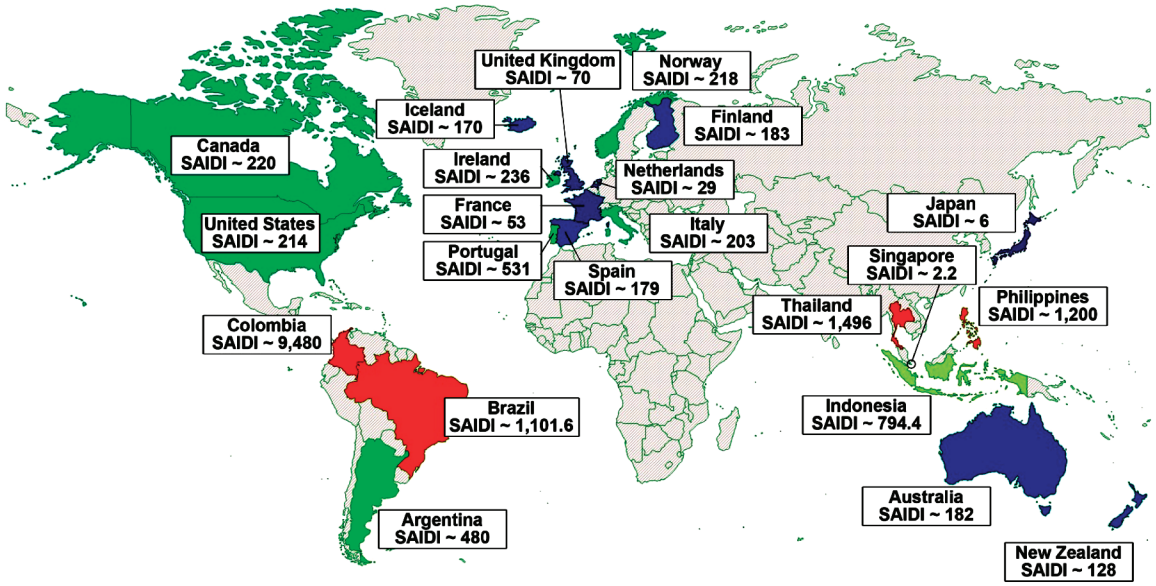


FIGURE 1.2a System Average Interruption Duration Index (SAIDI) indicators internationally for the period 1992 to 2001 (excluding only interruptions caused by major storms and hurricanes). SOURCE: EPRI (2003).

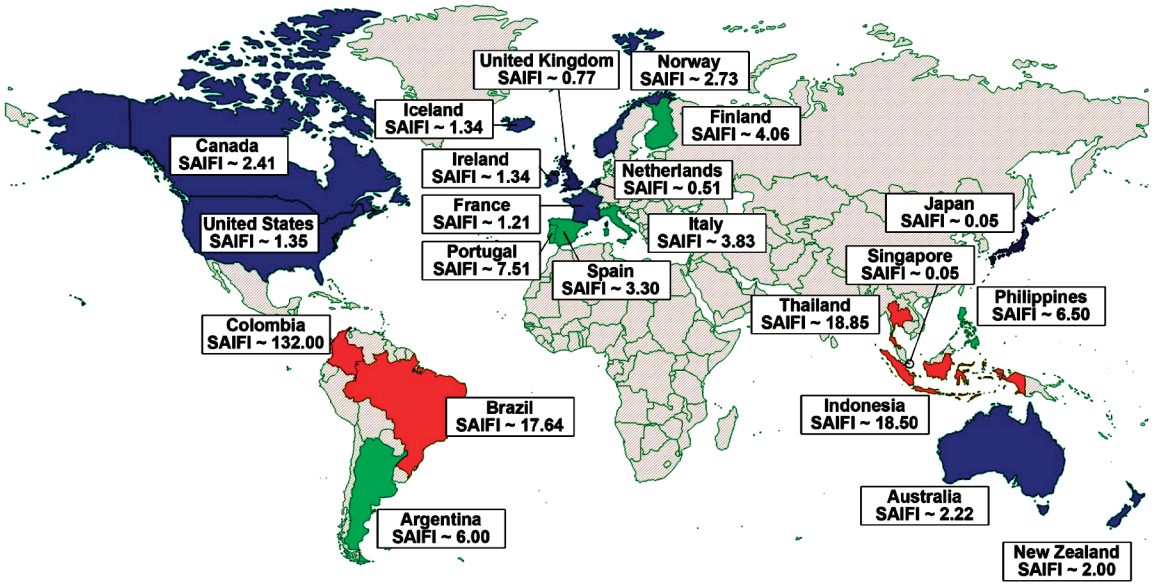


FIGURE 1.2b System Average Interruption Frequency Index (SAIFI) indicators internationally for the period 1992 to 2001 (excluding only interruptions caused by major storms and hurricanes). SOURCE: EPRI (2003).

down for an extended period could cause enormous economic damage, as discussed below.

Terrorists could, under some circumstances, view the transmission and distribution system as an important secondary target.

Terrorist attacks probably would involve physical destruction of key system facilities. However, a combined cyber attack and physical attack could be especially serious, particularly if mounted by someone with detailed knowledge of the electric power system, its physical characteristics, and its vulnerabilities.

Hackers and Other Nonterrorist Individuals and Groups

Terrorist attacks are the main focus of this report, but other types of attackers are also relevant. Not only are lower-level

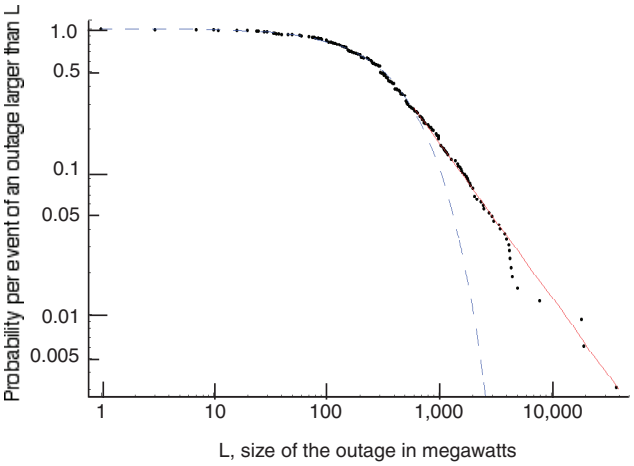


FIGURE 1.3 Relative frequency of electrical outages in the United States between 1984 and 2000. Of the 533 transmission or generation events shown, 324 involved a power loss of >1 MW (average of once every 19 days), and 46 involved a power loss of >1,000 MW (average of 3 per year). Dots indicate actual outage events. The dashed line is an exponential (Weibull) distribution fit to the failures below 800 MW loss. The solid line is a power law fit to the NERC data over 500 MW loss. SOURCE: Data compiled by NERC DAWG, plotted by Jay Apt, Carnegie Mellon University, 2006.

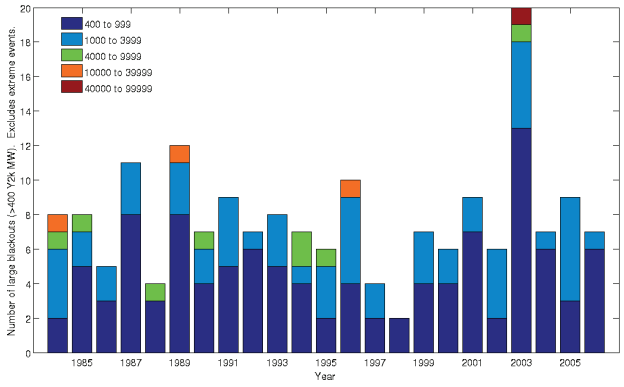


FIGURE 1.4 Frequency of electrical outages in the United States over time. Note that while there is significant year-to-year variability, there is no long-term trend. SOURCE: Data compiled by NERC DAWG, plotted by Paul Hines, Carnegie Mellon University, 2006.

attacks more likely, but many of the steps that should be taken to strengthen the system against terrorists will help against these attacks also. This section briefly describes the types of attacks that may be encountered.

Individuals or small low-tech groups with limited resources who want to kill people or cause widespread societal damage could pose a serious threat, but the amount of harm that one or a few such people could do to the electric system is probably limited. Individuals or groups that want to harm the power system but not kill a lot of people or cause widespread societal damage or harm might include

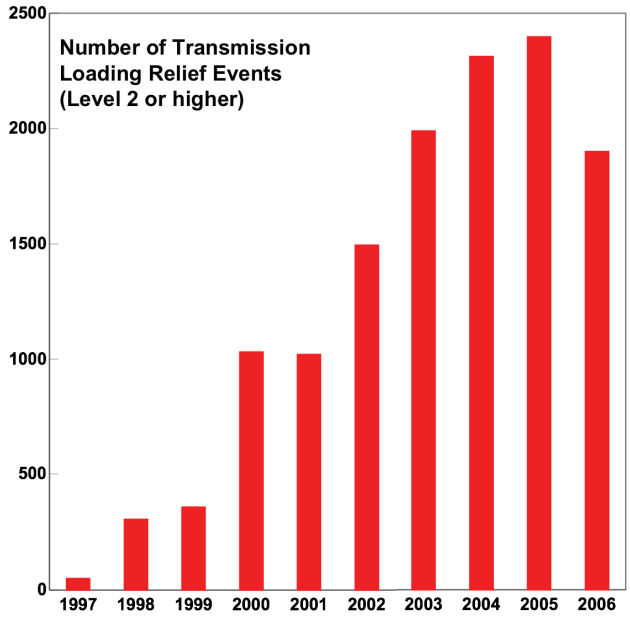


FIGURE 1.5 Annual number of transmission loading relief events since 1997. The substantial increase indicates that over the past decade the level of stress on the system has grown considerably. SOURCE: NERC data plotted by Jay Apt, Carnegie Mellon University, 2006.

people angry at the power company, bored hunters taking pot shots at insulator strings, or individuals who view the power company as an important symbol of something they oppose. For example, the Earth Liberation Front has reportedly been involved in a plot to bring down high-voltage power lines.[4] Any such attack could be serious, especially if undertaken by a current or former employee with detailed insider knowledge. Between 1984 and 2000, approximately 3 percent of major disturbances in the United States were attributed to sabotage.[5] The authors of *Making the Nation Safer* note that sabotage of individual components has "posed a nuisance, but the impacts have generally been manageable" (NRC, 2002, p. 177). Pernicious hackers are people whose primary motivation is not to kill people or cause specific damage, but rather to test limits and perhaps gain recognition within a subculture by demonstrating technical prowess by disrupting the operation of an important and highly visible societal system. Their motivation would be similar to that of computer hackers who release computer viruses and worms, or disrupt corporate and government computer sites. It is likely that such attacks would come from lone individuals or small groups.

Finally, harmful activity could be motivated by commercial benefit. A power company seeking a competitive

[4]See "11 Indicted in Eco-terror Arsons," available at http://abcnews.go.com/US/Terrorism/story?id=1526225.

[5]Based on NERC Disturbance Analysis Working Group (DAWG) data available at http://www.nerc.com/~dawg/.

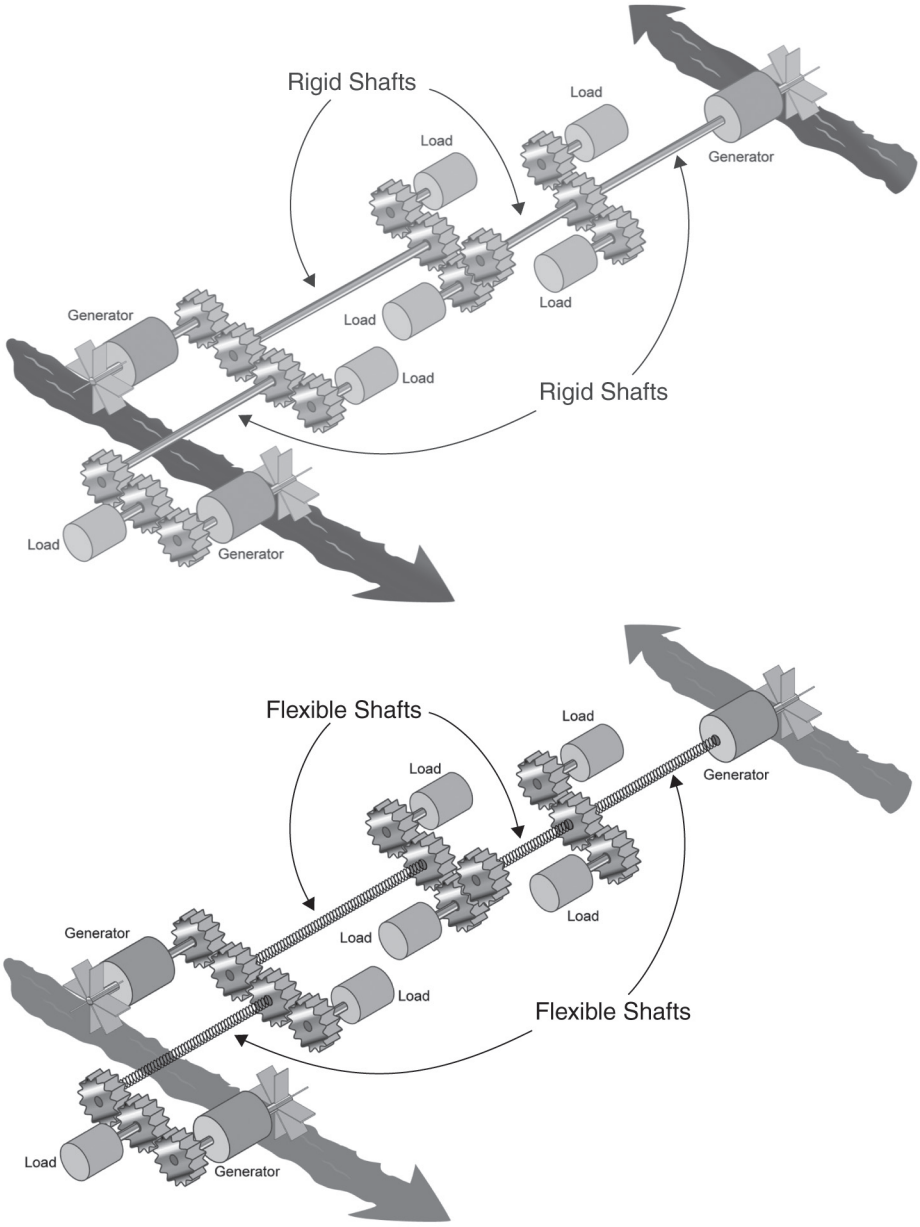


FIGURE 1.6 Illustrative analogy of electric transmission and distribution. Unlike a set of rigid drive shafts (above) that move power from generators to loads, AC power transmission and distribution systems are more accurately thought of in terms of a series of coil springs of varying stiffness through which power is transmitted by twisting (below). Since these links are not rigid, under some circumstances they can exhibit complex oscillatory behavior, or even become so tangled that they can no longer transmit power.

advantage might sabotage its competitor's equipment, and in the process compromise the integrity of the system. Until the pernicious actions of Enron traders were revealed, few would have given such a possibility a second thought. With tighter oversight and greater awareness within the industry, plus FERC's increased emphasis on market monitoring, such activity is probably unlikely, but the potential for it should not be ignored. The possibilities include, for example, (1) generators in one independent system operator (ISO) capturing transfer rights on tie-lines between control areas in order to increase congestion at those facilities and thereby maintain local market power, or (2) large buyers creating transient disturbances on the system in an effort to reduce the number of other buyers, thereby lowering system load and price. A simplified model illustrates how two or more small, physically separated generators acting together might have their supply frequencies altered and produce resonant phenomena that might cause protective devices on other large competi-

TABLE 1.1 Some Worldwide Examples of Cascading Power Failures with Potential or Actual Widespread Impact

Date	Location	Notable Consequences
November 9, 1965	Northeastern United States (10 states), Ontario	Power to 30 million customers (20,000 MW) interrupted (USFPC, 1965)
June 5, 1967	Middle Atlantic Region	4 million people affected
May 1977	Miami, Florida	Power to 1 million customers over 15,000 square miles interrupted
July 13, 1977	New York City	Power to 9 million customers (6,000 MW) interrupted for as long as 24 hours; widespread looting, chaos; police made about 3,000 arrests (DOE/FERC, 1978)
December 1978	France	Power in part of France interrupted due to voltage collapse
January 1981	Idaho, Utah, and Wyoming	Power to 1 million customers interrupted for 7 hours
March 1982	Oregon	Power to more than 900,000 customers interrupted for 1.5 hours
1987	Tokyo	Power to 2.8 million customers interrupted
1989	Quebec	Power to 9 million customers interrupted; geomagnetically induced currents from solar storm
1990	Egypt	Power for entire country affected by sandstorms
December 1994	Western United States	Power to 2 million customers interrupted from Arizona to Washington state
1996	Malaysia	Power to 20 million customers interrupted
1996	Philippines	Half of country affected by power plant outages
July 2, 1996	Western United States	Power to 2 million customers (11,850 MW) interrupted in 14 states for approximately 6 hours (WSCC, 1996)
July 3, 1996	Western United States	Recurrence of July 2 disturbance; operators interrupted power supply to most of Boise, Idaho, vastly reducing the extent of the event (WSCC, 1996)
August 1996	Indonesia	Power to 100 million customers interrupted
August 10, 1996	Western United States	Power to 7.5 million customers (28,000 MW) interrupted; economic damage estimated at $1 billion to $3 billion (WSCC, 1996)
1998	North central United States/ central Canada	Power to 152,000 customers interrupted by lightning
January 1998	Québec, Northeastern United States	Power to 2.3 million customers interrupted due to ice storms
February 1998	Auckland, New Zealand	Power cables failed, central business district was without power for about 5 weeks, affecting as many as 60,000 of the 74,000 people who worked there
June 25, 1998	Midwestern United States, central Canada	Power to 152,000 customers (950 MW) interrupted
November 1988 to June 2003	Western India	29 large cascading failures over 15 years—1.9 per year; power to millions of customers interrupted in most cases (Roy and Pentayya, 2004)
1998 to 2001	Western and midwestern United States	Rotating blackouts in several markets because of summer prices
December 1998	San Francisco	Power to 0.5 million affected
1999	Brazil	24.5 GW of load lost short-circuit 440 KV Busbar
1999	Denmark	Power to 100,000 customers interrupted by a hurricane
1999	France	Power to 3.6 million customers interrupted by storms
1999	Taiwan	Entire country affected by transmission tower collapse due to earthquake
July 1999	New York City	Power to 300,000 customers interrupted for 19 hours
2000	Portugal	Power to 5 million customers interrupted by failure of protection system
2001	Nigeria	Power to 20 million to 50 million customers affected
2002	Argentina	Power to 2 million customers interrupted by damaged cables
2002	Colombia	One-third of country affected by rebel attacks

continued

TABLE 1.1 Continuedt

Date	Location	Notable Consequences
2002	Philippines	Half of country affected by power plant outages
2003	Algeria	Entire country affected by power plant breakdown
2003	Denmark	Power to 5 million customers interrupted by a transmission line fault
2003	Georgia, Eastern Europe	Entire country affected by transmission tower collapse
2003	North Carolina, Virginia	Power to 2,200,200 customers interrupted by Hurricane Isabel
August 14, 2003	Midwestern and northeastern United States, southeastern Canada	Power to 50 million customers interrupted; estimated social costs from $4 billion to $10 billion; massive traffic jams in New York City (U.S.-Canada, 2004)
August 30, 2003	London	Power to 410,000 customers interrupted by incorrect relay operation
September 18, 2003	Tidewater region, United States	Power to 4 million customers interrupted
September 23, 2003	Denmark and Sweden	Power to 4 million customers interrupted
August 24, 1992	Florida	Power to 1 million customers interrupted
September 27, 2003	Italy	Power to 57 million customers interrupted; at least 5 people died; 30,000 passengers stranded in trains for hours (BBC, 2003; CNN, 2003)
2004	Florida, Alabama	Power to 5 million customers interrupted by Hurricanes Charley, Frances, Ivan, and Jeanne over a 6-week period
2004	Kyushu, Japan	Power to 1 million customers interrupted by typhoon
July 12, 2004	Southern Greece	Voltage instability as a result of high power transfers into Greece; operator-initiated load shedding unable to prevent voltage collapse; blackout a cause of additional concern due to proximity to 2004 Olympic games
2005	Alabama, Florida, Louisiana, and Mississippi	Power to 2.2 million customers interrupted by Hurricane Katrina
2005	Moscow	Power to 1.5 million to 2 million customers interrupted by explosion and fire at substation
May 24, 2005	Moscow	Power to 4 million customers (2,500 MW) interrupted
September 12, 2005	Los Angeles	Large portion of city lost power because error in substation tripped several circuit breakers

tive generators to trip off the system, or perhaps even cause physical damage. With the instrumentation now deployed on power systems, it could be very difficult to detect and identify the initiator of these events. In the now unlikely event that they were to occur, competitively induced congestion, dynamic instabilities, or equipment disruptions could disrupt the system and perhaps also render it more vulnerable to compounding terrorist assault (DeMarco, 1998).

Precedents for Attacks on Power Systems

Although to date attacks on the U.S. power transmission and distribution system have been limited to small-scale vandalism by a few individuals or small groups with limited technical sophistication, elsewhere in the world the electric power system in general, and particularly the transmission and distribution system, have been a focus of considerable terrorist activity.

In a few cases, such as in Baghdad, successful attacks have been mounted against generation plants. More often, as in Colombia, efforts to attack generation have been prevented by the high levels of security that can be provided for such large concentrated targets. As a consequence, most of the attacks that have occurred have been against transmission and distribution systems. These systems make more attractive targets because they are physically widely dispersed and hence very vulnerable. Often facilities are located in remote places, making them difficult if not impossible to defend against explosions or bullets or other projectiles fired from a distance.

While there is a growing internationalization of some terrorist activity, most attacks in the past have been mounted by indigenous groups bent on damaging or destabilizing established ruling power structures. For example, in the past the Irish Republican Army mounted bomb attacks on power substations in the United Kingdom. More recently

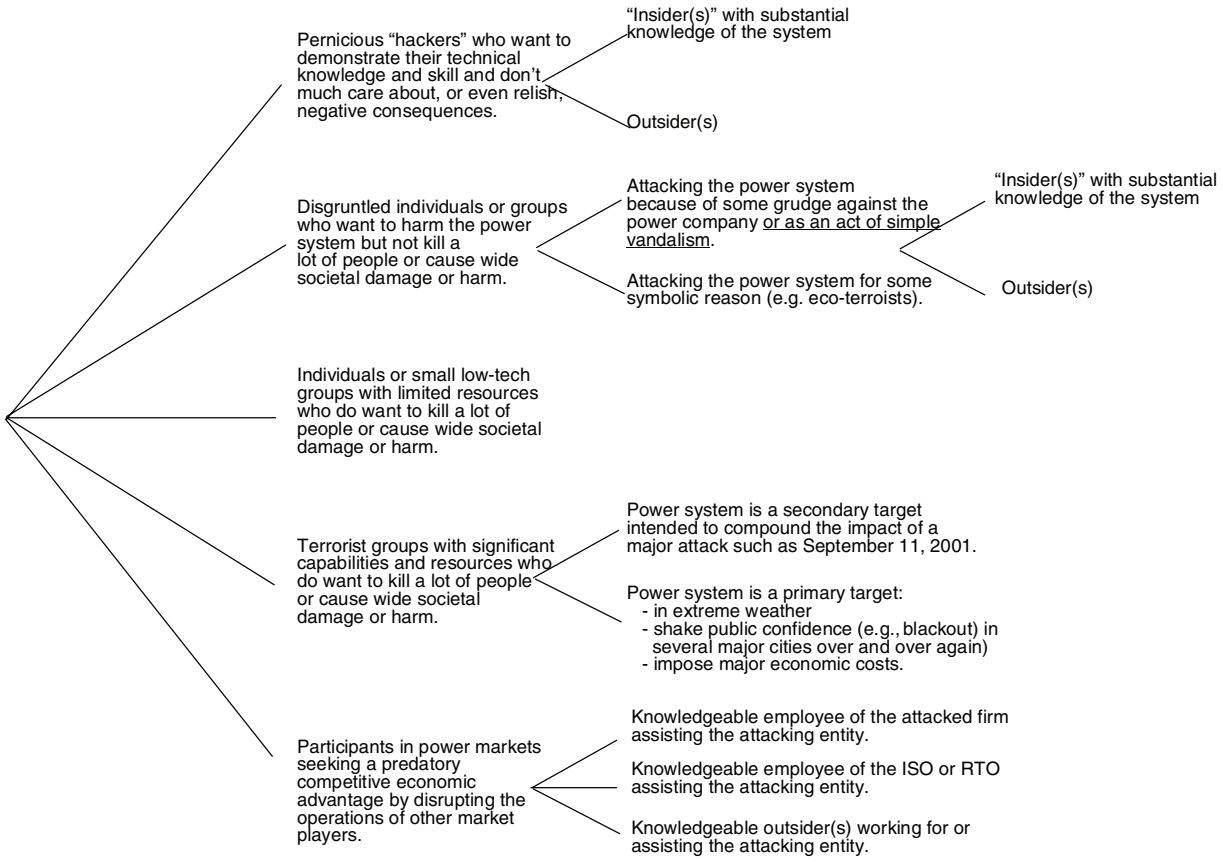


FIGURE 1.7 Simple classification of potential power system attackers.

in Columbia, FARC (Fuerzas Armadas Revolucionarias de Colombia) has mounted hundreds of attacks on a monthly basis against transmission and distribution systems with the objective of diminishing the power and standing of the central government authority and strengthening FARC's hand in any possible future political settlement. Twenty years previously, Sendero Luminoso mounted similar attacks in Peru. With the capture and imprisonment of almost all of the senior leadership of that organization, such attacks have now largely ceased.

There have been frequent attacks on transmission and distribution facilities in Iraq by insurgent groups intent on contributing to general social disruption, embarrassing central authorities, and preventing the normalization of daily life.

Many such attacks have occurred across Asia. For example, terrorist groups in Thailand have recently increased the size and numbers of their attacks against electric power facilities as part of a broader campaign to bring down the central government in Bangkok. Many parts of Africa have also witnessed such attacks.

Although in the United States attacking the power system may not be as attractive to serious terrorist groups as bombings, or radiological, chemical, or biological attacks, there are enough examples of attacks elsewhere around the world, and enough plausible circumstance under which an attack might occur in the United States, to warrant serious attention and careful planning and preparedness.

The Department of Homeland Security (DHS) has developed a range of worst-case terrorist attack scenarios for use in gaming, in consequence assessment and management, and in supporting the development of detailed plans and response strategies (Lipton, 2005). Most of these scenarios deal with weapons of mass destruction which would not be particularly appropriate for attacks on the power systems, and in particular on the transmission and distribution system.

Nevertheless, the power industry itself has conducted scenario-based tabletop exercises to examine possible attack scenarios and their consequences. These have included a variety of exercises involving attacks against the transmission and distribution system. Individual power companies, as well as reliability organizations and trade and research organizations, have also conducted detailed power system attack simulation studies and threat assessments in order to identify vulnerable assets and to develop protective actions as well as response and recovery strategies.

IMPACTS OF WIDESPREAD, LONG-LASTING BLACKOUTS

Electricity is essential to the U.S. economy and to this country's way of life. Annual sales in 2006 were $326 billion, approximately the same size as telecommunications (DOE/EIA, 2007). Moreover, the value of electricity is far greater than the price that consumers pay multiplied by the amount they consume. Economists refer to this extra value as "consumer surplus."

Estimating the economic cost of large-scale or long-duration blackouts is difficult. The Wall Street Journal reported that the economic costs of the massive blackout that struck the Midwest, the Northeast, and parts of Canada in August 2003 could have been as high as $4 billion to $6 billion (Hilsenrath, 2003). North American Reliability Council data indicate that the amount of power not delivered during that blackout was approximately 920,000 megawatt-hours (MWh). Together, these two numbers suggest that the economic cost of the 2003 blackout came to approximately $5 per forgone kilowatt-hour,[6] a figure that is roughly 50 times greater than the average retail cost of a kilowatt-hour in the United States. However, many of the affected industries appear to have made up for much of the lost output once power was restored. In a disruption of longer duration and greater geographic extent, a post-blackout rebound could be much more modest.

Lecomte et al. (1998) estimated that the 1998 ice storm that disrupted power to 1,673,000 customers, of whom 1,393,000 were in Quebec, resulted in economic losses of $1.6 billion in Canada and $1 billion in repair costs to the Hydro-Quebec and Ontario Hydro systems. A significant fraction of the 28 deaths in Canada and 17 deaths in the United States also resulted from the lack of power.

Large-scale disruption caused by damage to the high-voltage transmission system garners wide attention, but widespread damage in the distribution system, such as that caused by recent Florida and Gulf Coast hurricanes, can be more expensive. Schuler (2005) notes that Florida Power and Light incurred repair costs of $890 million from damage done by hurricanes in August and September of 2004, largely to distribution systems, and estimates that "the societal costs were probably even greater than those incurred in the 2003 Northeast blackout."

Loss of power can have profound impacts on other critical infrastructures, as illustrated in an analysis by Chang et al. (2005) of a January 20, 1993, windstorm in the Pacific Northwest with documented impacts on emergency services, transportation, health care, building support, the food supply, and government. Losses included 2.5 million customer-hours of power outages disruptions for up to 3.5 days in some areas.

In the past, the pumping stations on natural gas pipelines were powered by the gas they were transporting. However, as gas prices have risen, often more rapidly than the price of electricity (half of which is generated from coal), many gas pipelines have begun to convert their compressor stations from gas to electricity—thus creating a coupled vulnerability between what were once two independent energy supply systems. Similar coupling vulnerabilities can occur with oil delivery systems, communication systems, railways, and other critical infrastructure.

Power disruptions also put people out of work. For example, Statistics Canada reported that "an estimated 2.4 million workers in Ontario and Gatineau, Quebec, lost 26.4 million hours of work time in the second half of August because of the [2003] Ontario-U.S. power outage and subsequent conservation period."[7]

Several models have been used to estimate the economic impacts of hypothetical local and regional blackouts. Greenberg et al. (2007) used a regional econometric model to examine the economic impacts of a variety of outage scenarios involving blackouts of one New Jersey utility (Public Service Electric and Gas, PSE&G, which serves about half the state) and estimated statewide impacts. The most severe scenario studied involved the loss of 95 percent of power during the first day with 10 percent of power not restored until the end of the second month. Assuming the attack occurred in the summer of 2005, the worst case resulted in a loss of 3.4 percent of the gross state product during that year ($389 billion year in 2000 dollars) followed by a positive rebound of 2 percent the following year. Since the simulated event is assumed to be localized, one of the more interesting issues explored is the extent to which businesses would choose to move to other regions thought to be less at risk of future attack.

Despite the difficulty of producing precise numbers, it is clear that blackouts of large scale or long duration can easily result in economic costs of many billions of dollars. Other infrastructure and services are also lost or are seriously degraded, further disrupting the lives of people who find themselves in dangerous situations, without work, and without conventional services such as operating bank machines and gas stations.

A systematically designed and executed terrorist attack could cause disruptions considerably more widespread and of much longer duration than the largest power system disruptions experienced to date. Since those disruptions have entailed economic impacts approaching 10 billion dollars, it appears possible that terrorist attacks could lead to costs of hundreds of billions of dollars—that is, perhaps as much as a few percent of the U.S. gross domestic product, which is currently about $12.5 trillion. If large, extended outages were to occur during times of extreme weather, they could also result in hundreds or even thousands of deaths due to heat stress or extended exposure to extreme cold.

[6]OTA (1990) estimated in 1990 that disruptions of similar duration would impose costs of $1 to $5 per kilowatt-hour.

[7]As cited at http://www.ontariotenants.ca/electricity/articles/2003/cp-03j31.phtml.

Even without intentional attacks, power systems are always undergoing damage and recovery. While system owners and operators should do all that they reasonably can to ensure that their systems are able to withstand anticipated assaults from natural and human sources, there are practical limits to how much such systems can be "hardened" because of its highly distributed nature. The complete elimination of all possible modes of failure is simply not a feasible objective. Thus, even in the absence of threats from terrorists, an important design objective should be resilience, i.e., the ability to rapidly restore the power system after a problem occurs and the ability to sustain critical social services while the problem persists.

ACTIONS TAKEN SO FAR TO REDUCE VULNERABILITY

The need to reduce the vulnerability of the U.S. electric power system is well recognized in the government and industry. Although related action has been somewhat slow and limited, many improvements made behind the scenes are rarely reported in detail to the media. Reducing the vulnerability of electric power systems is becoming a top priority of utility management. In addition, the Energy Policy Act of 2005 (EPAct) includes provisions to strengthen the system and make temporary improvements permanent. Under authorization provided by EPAct, the North American Electric Reliability Council (NERC) is now moving to improve U.S. electric power system performance through the creation of the national Electric Reliability Organization (ERO), which has the authority to develop mandatory reliability standards. EPAct also provides incentives for both expanding the transmission system and removing barriers to siting transmission lines, and it addresses the problem of relieving areas of critical congestion on the transmission system. Improving the resilience of the transmission system to relatively routine failures will also reduce vulnerability to deliberately caused failures.

Actions by the Utility Industry

Actions by the utility industry to deal with terrorism focus on prevention, detection, and restoration. Prevention measures that the industry has implemented include:

- Self-determination of the proper alert level for physical and cybersecurity in conjunction with the advice of the DHS,
- Security improvements such as physical barriers and an increased security workforce for protecting physical facilities, and
- More stringent security requirements for facility entry.

In the area of detection, several activities are ongoing, such as:

- Training system operators to consider sabotage and terrorism as a possible explanation for disturbances,
- Implementing a real-time data collection process for reporting indicators of potential physical and cyber-events to DHS (such as the presence of strange vehicles and aircraft near critical facilities),
- Holding conferences sponsored by industry and government, conducting dialogs, holding scheduled conference calls, and exchanging security-related alerts, brochures, and newsletters.

Restoration activities include:

- Preparing contingency plans for restoring service,
- Stocking equipment needed for service restoration,
- Cataloging and agreeing to share spare transformers following an attack.

Actions by Government

The most relevant provision of EPAct is establishment of the Electric Reliability Organization to develop and enforce reliability standards for the bulk transmission system. Before it was designated as the ERO in July 2006, NERC could only recommend upgrades as needed to maintain reliability. Now, those standards will be mandatory, but they must also be approved by FERC. NERC will base its standards in part on existing data and experience with past operating incidents. According to Section 236 of the ERO certification order:

> NERC states that the purpose of a Reliability Standard, or its reliability objective, should derive from one or more of the following eight general objectives: (1) the Bulk-Power System should be planned and operated to perform reliably under normal and abnormal conditions; (2) the frequency and voltage of the Bulk-Power System should be controlled within defined limits by balancing real and reactive power supply and demand; (3) information necessary for the planning and operation of the Bulk-Power System should be made available to those who need it; (4) emergency operations plans should be developed and implemented; (5) facilities for communication, monitoring, and control should be provided, used and maintained; (6) personnel must be trained, qualified and must have the authority to implement actions; (7) the reliability of the Bulk-Power System should be monitored on a wide-area basis; and (8) the Bulk-Power System must be protected from malicious physical or cyber attacks. (FERC, 2006)

Only the last general objective directly addresses the potential for terrorist attacks. Basing NERC standards on past experience will make it difficult to ensure that they protect against effects of terrorism, as there are no data on the

nature or results of terrorist attacks on electric power systems in this country. Furthermore, NERC's intention to consider costs as well as benefits may work against protection against extreme but unlikely risks that cannot be quantified, including terrorist attacks. Overall, however, establishment of an ERO with real authority is a significant step forward. In addition, EPAct includes measures that should encourage the construction of new transmission lines and the development of new technologies to improve the efficiency and reliability of the power grid, steps that should also provide increased resistance to terrorist attacks. DOE's report *On the Road to Energy Security* describes how it is carrying out its responsibilities under EPAct (DOE, 2006).

DHS's *National Infrastructure Protection Plan* (NIPP) provides an overall approach to protecting critical infrastructure, including electric power systems (DHS, 2006a). DHS's analysis of terrorist capabilities and motivations suggests that infrastructure could be a prime target, especially as protection is enhanced at other targets. The plan calls for (1) strong public-private partnerships to foster relationships and facilitate coordination within and across critical infrastructure and key resource sectors; (2) robust multidirectional information sharing that will enhance the ability to assess risks, make prudent security investments, and take protective action; and (3) a risk management framework establishing processes for combining consequence, vulnerability, and threat information to produce a comprehensive, systematic, and rational assessment of national or sector risk. Not addressed in the NIPP, however, is the issue of how private entities can be expected to assume the large costs required to make the system more robust against low-probability events.

DHS's revised *National Response Plan*, a broad, comprehensive plan for preparing for a wide range of emergencies, also addresses critical infrastructure, including electric power systems (DHS, 2006b).

CONCLUSIONS

- By their very nature, electric power transmission and distribution systems are not perfectly reliable. Keeping power flowing to customers is a continuous process of control, recovery, and repair. Most outages involve only the distribution system. However, occasionally storms, accidents, or other events cause disruption of the high-voltage transmission system. Power systems are designed and operated to cope with such disturbances and to restore service as rapidly as possible.
- Well-planned attacks on the power system, undertaken by informed terrorists, could result in power outages with extents and durations that are much larger than those produced by all but the largest natural events. Damage to critical, difficult-to-replace system components could be extensive, making restoration of power slow and extremely difficult.
- Although major terrorist organizations have not attacked the U.S. power delivery system, such terrorist attacks have occurred elsewhere in the world. Simply turning off the power typically does not terrorize people. However, the United States should not ignore the possibility of an attack that turns off the power before staging a large conventional terrorist event, thus amplifying the latter's consequences. Nor should the possibility of a series of attacks designed to do major damage to the economy and to the public's sense of security and well-being be ignored.
- Economic costs from a carefully designed terrorist attack on the U.S. power delivery system could be as high as *hundreds of billions of dollars* (i.e., perhaps as much as a few percent of U.S. gross domestic product).
- Both industry and government have begun to address the risks of terrorism to the power delivery system, but there is much more that can and should be done.

REFERENCES

BBC. 2003. "Italy Launches Blackout Inquiry." BBC news online. September 30, 2003. Available at http://news.bbc.co.uk/2/hi/europe/3150788.stm. Accessed August 2007.

Chang, S.E., T.L. McDaniels, and D. Reed. 2005. "Mitigation of Extreme Event Risks: Electric Power Outage and Infrastructure Failure Interactions." Pp. 70–90 in *The Economic Impacts of Terrorist Attacks*, H.W. Richardson, P. Gordon, and J.E. Morre II, eds. Northampton, Mass.: Edward Elgar Publishing.

CNN. 2003. "Italy Recovering from Big Blackout." CNN. Sept. 28, 2003. Available at http://www.cnn.com/2003/WORLD/europe/09/28/italy.blackout/index.html. Accessed August 2007.

DeMarco, C.L. 1998. "Design of Predatory Generation Control in Electric Power Systems." Pp. 32–38 in *Thirty-First Annual Hawaii International Conference on System Sciences*, Vol. 3. New York: IEEE.

DHS (Department of Homeland Security). 2006a. National Infrastructure Protection Plan. Available at http://www.dhs.gov/dhspublic/interapp/editorial/editorial_0827.xml. Accessed September 2006.

DHS. 2006b. *National Response Plan*. Available at http://www.dhs.gov/xprepresp/committees/editorial_0566.shtm. Accessed October 2006.

DOE (U.S. Department of Energy). 2006. *On the Road to Energy Security: Implementing a Comprehensive Energy Strategy: A Status Report*. Available at http://www.energy.gov/media/FINAL_8-14_DOE_booklet_copy_sep.pdf. Accessed September 2006.

DOE/EIA (Energy Information Administration). 2007. *Revenue from Retail Sales of Electricity to Ultimate Customers by Sector, by Provider*. Available at http://www.eia.doe.gov/cneaf/electricity/epa/epat7p3.html. Accessed October 2007.

DOE/FERC (Federal Energy Regulatory Commission). 1978. *The Con Edison Power Failure of July 13 and 14, 1977*. Washington, D.C.: U.S. Government Printing Office.

EPRI (Electric Power Research Institute). 2003. *Distribution Reliability Indices Tracking Within the United States*. Report No. 1008459. Palo Alto, Calif.: EPRI.

FERC. 2006. Order Certifying North American Electric Reliability Corporation as the Electric Reliability Organization and Ordering Compliance Filing. Available at ftp://www.nerc.com/pub/sys/all_updl/docs/ferc/20060720_ERO_certification.pdf. Accessed September 2006.

Greenberg, M., N. Mantell, M. Lahr, N. Felder, and R. Zimmerman. 2007. "Short and Intermediate Economic Impacts of a Terrorist Initiated Loss of Electric Power: Case Study of New Jersey." *Energy Policy* 35(1): 722–733.

Hilsenrath, J. 2003. "The 2003 Blackout: Economy Won't Likely Be Derailed—Cost Could Hit $6 Billion as Major Sectors Are Hurt; a Few Reaped Benefits." *Wall Street Journal*, August 18.

Lecomte, E.L., with A.W. Pang and J.W. Russell. 1998. Ice Storm '98, ICLR Research Paper Series No. 1. Institute for Catastrophic Loss Reduction, Toronto, Canada. Available at www.iclr.org/pdf/icestorm98_english.pdf. Accessed August 2007.

Lipton, E. 2005. "U.S. Report Lists Possibilities for Terrorist Attacks and Likely Toll." *New York Times*, March 16.

Meade, C., and R.C. Molander. 2006. "*Considering the Effects of a Catastrophic Terrorist Attack*." RAND Technical Report. Available at www.rand.org/pubs/technical_reports/TR391/. Accessed August 2007.

Mueller, J. 2006. "Is There Still a Terrorist Threat?" *Foreign Affairs* 85(5): 2–8.

NRC (National Research Council). 2002. *Making the Nation Safer: The Role of Science and Technology in Countering Terrorism*. Washington, D.C.: The National Academies Press.

OTA (Office of Technology Assessment). 1990. *Physical Vulnerability of Electric System to Natural Disasters and Sabotage*. OTA-E-453. Washington, D.C.: U.S. Government Printing Office.

Rose, A., and S-Y Liao. 2005. "Modeling Regional Economic Resilience to Disasters: A Computable General Equilibrium Analysis of Water Service Disruptions." *Journal of Regional Science* 45(1): 75–112.

Rose, A., S-Y Liao, and G. Oladosu. 2005. "Regional Economic Impacts of Terrorist Attacks on the Electric Power System of Los Angeles: A Computable General Disequilibrium Analysis." Paper presented at the Second Annual Symposium of the DHS Center for Risk and Economic Analysis of Terrorism Events, University of Southern California, Los Angeles, Calif., August 20.

Roy, A., and P. Pentayya. 2004. "Experience of Blackouts and Restoration Practices in the Western Region of India." Slides presented at the IEEE Power Engineering Society General Meeting, Denver, Colo., July.

Schuler, R.E. 2005. "Float Together/Sink Together? The Effect of Connectivity on Power Systems." Pp. 91–118 in *The Economic Impacts of Terrorist Attacks*, H.W. Richardson, P. Gordon, and J.E. Morre II, eds. Northampton, Mass.: Edward Elgar Publishing.

U.S.-Canada (U.S.-Canada Power System Outage Task Force). 2004. *Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations*. Available at http://www2.nrcan.gc.ca/es/erb/erb/english/View.asp?x=690&oid=1221. Accessed August 2007.

USFPC (U.S. Federal Power Commission). 1965. *Northeast Power Failure: November 9 and 10, 1965*. Washington, D.C.: U.S. Government Printing Office.

WSCC (Western Systems Coordination Council) Operations Committee. 1996. *Western Systems Coordinating Council Disturbance Report*. Butte, Mont.: WSCC.

2

The Electric Power System Today

The electric power delivery system in North America encompasses a wide diversity of institutions, technologies, organizational structures, economic mechanisms, and regulatory oversight. Some parts of the system are provided by federal, state, or municipal governments; others are customer-owned cooperatives. Much of the power supply is from privately owned, regulated utilities. Functionally, many of those traditional utilities were vertically integrated, i.e., providing generation, transmission, and end-use sales to customers over their own distribution system—although some federal agencies, like the Tennessee Valley Authority and the Bonneville Power Administration, provide only generation and transmission services, and many rural cooperatives provide only distribution and transmission services. In areas with deregulated, market-based supplies, different entities may furnish each of the three services through marketing agents who negotiate between generators and customers for their energy purchases, and in other jurisdictions, the generators are separated from combined transmission and distribution utilities. Regulatory oversight responsibility also varies by utility and location and is divided between federal and state agencies, with franchises for placing lines along public roads being granted by local municipalities.

Many generators are now independent producers without normal rate-of-return regulation, but they are still subject to federal antitrust laws and, in many instances, the market-monitoring oversight of the Federal Energy Regulatory Commission (FERC) and the independent system operator/regional transmission operator (ISO/RTO) that coordinates their wholesale market. These ISO/RTOs, many of which have been authorized by FERC, conduct the wholesale markets and clear transactions (that in some instances are also subject to Federal Commodities Exchange Commission oversight). They also have responsibility for operating the bulk power system reliably, dispatching power that results in flows over transmission lines that are owned by other public or private regulated entities. Six ISO/RTOs in North America are subject to FERC oversight of their wholesale markets, and 8 of 10 come under FERC's reliability oversight, with the remaining 2 being subject to Canadian regulation.

Technological differences are also widespread. Different voltages are used by different companies for their distribution and transmission systems. Also, two conceptually different physical configurations are used among utilities for their three-phase electrical systems governing how faults are grounded, the number of wires strung on poles, and therefore their relaying, control, and maintenance procedures. These different voltage standards and electrical configurations among suppliers require different equipment, which has implications for manufacturing costs and the size of inventories for spare components that are usually available. Furthermore, many systems use a radial spatial configuration of lines, whereas others, primarily in densely populated urban areas, have a network configuration with parallel interconnected paths. Each of these different system designs implies different operating and emergency response procedures.

Early electricity supply systems in the late 19th century were private, unregulated entities that competed for customers at their borders. The rapid technological advances in generation (economies of scale) and in transmission (higher voltages) quickly led to the aggregation of small companies into larger entities that had effective monopoly power over wide regions. Economic regulation or (in places) government acquisition of assets and public provision of services were natural responses.

In most of the country, adjacent suppliers interconnected their facilities with neighboring supplier facilities to provide redundancy of supply at lower cost, and to engage in occasional transfers of power if one utility had spare generating plants that had lower costs than its neighbor. Many of these exchanges were bilateral arrangements, but in some instances multilateral arrangements were formalized into power pools (e.g., the New England Power Pool). In all instances cohesive electrical zones were identified where the lines of responsibility for reliability were clearly established. In most urban centers, electric utilities were investor-owned,

for-profit corporations that were given legal rights to be the exclusive provider of electricity in a specified geographic area. In exchange for these franchise rights, the utility typically agreed to (1) pay franchise taxes based on assets in place within the area and (2) serve all customers reliably at a reasonable cost. In most jurisdictions these franchises are exclusive, thereby granting a monopoly status to the supplier, but in some states it is possible to grant multiple franchises to serve the same location.

After World War II, the process of interconnection and integration continued—leading to extensive integrated systems and large regional interconnections between electrical zones. The combination of economies of scale in generation, achieved by building larger units that were frequently grouped in larger power stations, with scale economies in transmission, gained through the use of higher transmission voltages, that facilitated this integration and allowed the delivery of large amounts of power over great distances at low cost. These cost reductions spurred demand and provided a ready market for the increased supply capacity, thus setting the stage for the next wave of cost-reducing innovation. Thus it frequently proved economical to locate large generating plants close to fuel sources, rather than transport fuel to generators located near customers. This trend was facilitated also by the lower land costs and easier approvals to locate power plants in rural areas. But it was the large interconnected systems that made possible these economies of scale in providing both energy and reliability. Thus, over time very large power markets and huge interconnected regions have developed in the United States and elsewhere in North America.

THE POWER DELIVERY SYSTEM

Overview Description

The power delivery system includes four components: (1) the grid, or high-voltage transmission system that connects the bulk power generation system with the distribution systems; (2) the distribution system, which delivers power to consumers (or electrical "loads"); (3) the operations system, which handles interconnections; and (4) the customers or consumers. (Some large industrial consumers are connected directly to the grid.) In North America, the system contains more than 200,000 miles of lines operating above 230 kV serving over 120 million customers and nearly 300 million people.

Electricity is generated at 13 to 25 kV from a variety of energy sources. Most U.S. electricity is generated from coal, nuclear energy, natural gas, and hydro power; but recently wind generation has been growing rapidly.

Alternating current (AC) circuits predominate in the U.S. power delivery system. AC circuits allow the use of transformers to step up voltage to a higher level for economical transmission with small losses and to step the voltage down for distribution to consumers. U.S. transmission voltages are typically 115, 230, 345, or 500 kV. Voltages of 765 kV and higher are considered extra-high voltage (EHV). In most regions of the United States, 230-500 kV systems are the backbone of the U.S. electricity grid, although in some areas, lines with voltages up to 765 kV are employed.

Prior to the 1960s, the loosely connected, cohesive electrical zones offered modest reliability at a reasonable cost to the nation's consumers. But following a massive blackout in the Northeast in 1965, an increasing concern evolved among policy makers and industry executives alike about the power system's reliability. In response, the electric utility industry voluntarily formed regional reliability organizations to coordinate activities related to the transmission system's performance, most notably the North American Electric Reliability Council (NERC). Reliability is now administered by over 100 control area operators in North America and coordinated by regional reliability organizations (RROs) as members of NERC, which has established operating and planning standards based on seven concepts:

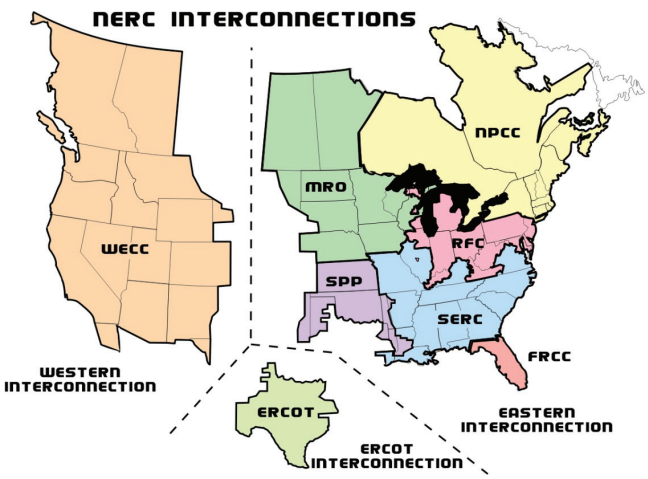
- Keep generation and demand in balance continuously.
- Balance reactive power supply (necessary to maintain system voltage) and demand.
- Monitor flows over grid circuits.
- Maintain system stability.
- Operate the system so it is able to sustain stability even if one component fails.
- Plan, design, and maintain the system to operate reliably.
- Prepare for emergencies.

Controlling the dynamic behavior of interconnected electricity systems presents a great engineering and operational challenge. Demand for electricity is constantly changing as millions of consumers turn on and off appliances and industrial equipment. The generation and demand for electricity must be balanced over large regions to ensure that voltage and frequency are maintained within narrow limits (usually 59.98 to 60.02 Hz). If not enough generation is available, the frequency will decrease to a value less than 60 Hz; when there is too much generation, the frequency will increase to above 60 Hz. If voltage or frequency strays too far from its prescribed level, the resulting stresses can damage power systems and users' equipment, and may cause larger system outages.

A variety of techniques and processes are used to keep the system safe—such as sensors, circuit breakers, and relays—to ensure that component failures and electrical faults are quickly isolated. If protection systems are poorly designed or do not operate properly, faults or equipment failures can cause outages and may cascade or propagate into blackouts. Once an overloaded circuit or transformer in the system either fails or is intentionally removed from service, the power flows through other available circuits in proportion to

the paths of least resistance. These alternative circuits may in turn become overloaded and either fail or be taken out of service by the protection system. This repeated, possibly uncontrolled, cycle of overload and equipment removal/failure is a dynamic, frequently oscillating phenomenon that can lead to a cascading outage. A local failure can escalate into a cascading failure in a matter of a few minutes, potentially leading to a wide-area blackout.

Operationally, the electric system of the United States and Canada is divided into four sections, known as "interconnections," linked mainly by direct current (DC) transmission, with transmission within each section using largely AC transmission. The DC ties between interconnection areas allow each interconnection to operate assets independently of the other sections. Within each interconnection, electricity is produced the instant it is used and flows over the path of least resistance (using virtually all transmission lines within each interconnection) from generators to loads (i.e., customers). Figure 2.1 shows the four basic North American interconnections with the underlying regional reliability councils responsible for operational coordination in the sub-areas within the interconnections. Generation and loads are constantly being balanced within each interconnection.



NOTE:
ERCOT: Electric Reliability Council of Texas (RRO)
FRCC: Florida Reliability Coordinating Council (RRO)
MRO: Midwest Reliability Organization (RRO)
NERC: North American Electric Reliability Council
NPCC: Northwest Power Coordinating Council (RRO)
RFC: Reliability *First* Corporation
RRO: Regional Reliability Organization (regional member of NERC)
SERC: Southeastern Electric Reliability Council (RRO)
SPP: Southwest Power Pool Inc. (RRO)
WECC: Western Electricity Coordinating Council (RRO)

FIGURE 2.1 The NERC regions, along with the interconnection areas. (Note that the Quebec Interconnection within Canada and the Eastern U.S. Interconnection are shown here as the Eastern Interconnection.) SOURCE: NERC Interconnections, available at http://www.nerc.com/regional/NERC_Interconnections_color.jpg, accessed June, 11, 2007.

The advent of competition in the wholesale electricity market in North America has increased the operational complexity of the power delivery system. Power generators in one area are able to sell power in another area so long as adequate transmission interconnections are available. Initiatives by the U.S. Congress and FERC to unleash a competitive wholesale electricity market have led to an enormous increase in the number of power transactions that are carried over the electric power transmission system.

The existing power system, however, was designed to handle the needs of individual integrated utilities, with transfers between utilities mainly to improve the reliability of supply. It was not originally designed for handling common-carriage interconnections, which require different controls and regulation. Merchant generators want to sell their electricity to buyers who are willing to pay the highest price. These generally are in high-priced regions, which may be distant from the generation facility. Control areas for the power system, which previously may have had a few dozen transactions between buyers and sellers before the advent of wholesale markets, now attempt to settle hundreds, if not thousands, of transactions per day. This has led to a system already under stress, even in the absence of any homeland security concerns.

An additional challenge to the power delivery systems is the evolving nature of electricity demand due to digital technology. Billions of microprocessors have been incorporated into industrial sensors, home appliances, and other devices. These digital devices are highly sensitive to even the slightest disruption (an outage of a small fraction of a single cycle can disrupt performance), as well as to variations in power quality due to transients, harmonics, and voltage surges and sags. Today about 10 percent of total electrical demand in the United States feeds or is controlled by microprocessors. By 2020 this level is expected to reach 30 percent or more (EPRI, 2003).

The electric power system was designed to serve analog electric loads—those without microprocessors—and is largely unable to consistently provide the level of digital quality power required by digital manufacturing assembly lines and information systems, and, soon, even our home appliances. Achieving higher power quality places an additional burden on the power system even before homeland security issues are considered.

A more positive aspect regarding the development of power markets and microprocessor technology derives from the advent of publishing widely varying prices when market or associated system capability conditions change. This provides some natural damping in the system as more and more customers are provided with electronic sensors and real-time pricing. This natural modulation of extreme

operating conditions may ease some operating issues as a result of well-designed markets that vary the prices that retail customers pay in real time.

Regional Differences Among Electric Power Systems in the United States

Notwithstanding the many technical similarities, many differences also exist in the electric system within and across sub-regions. The differences stem from numerous factors, including asset ownership, operational control, indigenous natural resources, market development, topography, weather conditions affecting energy production and use, regulatory practices and traditions, business differences (e.g., business configuration), and so forth.

For example, energy use peaks at different times of the day in different regions. Some regions have generation capacity surpluses, whereas others are generation constrained. Some regions have adequate transmission capacity to allow for economic and reliable transfer of energy to other regions; others are transmission constrained, preventing otherwise economic generation to serve customer demand. Because of social and political factors and environmental, health, and public safety concerns (not to mention perceived adverse impacts on property values), some regions have great difficulty adding new transmission capacity on new or even existing rights-of-way; others are able to build new transmission readily.

Likewise, regions with plentiful coal have a history of reliance on coal-fired generation, whereas other regions burn less coal because it must be transported great distances, or because air pollution problems have inhibited significant coal use, or because there is adverse public reaction to the use of coal because of global climate change concerns. In a number of instances, different states have enacted more stringent environmental regulations than has the U.S. government, most notably in the area of carbon emissions, but these regional differences in environmental standards can also lead to greater problems for systems operators in meeting their reliability objectives. Public concerns about conventional energy sources have lead to some states and communities promoting the use of renewable-energy-based resources for generation, like wind and hydropower, but these energy sources are frequently located far from the customers and may not be available when demand for electricity is greatest, so their use imposes even greater complications on system design and operation.

Again, some regions have large, investor-owned utilities, while others have many small publicly owned utilities (known as cooperative utilities and municipal utilities). Some regions have vertically integrated electric utilities that own generation, transmission, and distribution systems, while other regions have ownership patterns that focus on one part of the business or another. Some regions have regional transmission organizations (RTOs) that administer central wholesale markets, whereas others do not.

Such differences in system configuration, generation and fuel mix, ownership, and so forth create complexities in the operation of the system, even though all parts of the country's electric grid operate according to industry norms and standards.

Operations and Standards

In the United States, a variety of entities exercise some form or other of operational control or coordination over parts of the grid. For example, in most regions, owners of transmission facilities operate them according to standards set by NERC with the input of companies participating in regional reliability councils. In other regions, particularly where market mechanisms determine wholesale power transfers, entities such as ISOs or RTOs carry out some operating functions on behalf of the transmission asset owners and other users of the system.

Real-time monitoring of the transmission system is performed using telemetry along with other data and analytic tools, such as state estimators, to evaluate system conditions on a continuing basis. Conditions monitored include power flows, various physical limits on transmission and other facilities, interchange with adjacent regions, and demand drivers such as weather.

The enforcement of NERC standards is still evolving. Until the passage of the Energy Policy Act of 2005, the electric industry's standards were entirely voluntary.[1] In the absence of federal legislation mandating compliance with NERC rules, programs were developed to encourage compliance with NERC reliability standards. These were "enforced" by peer pressure, regulatory pressures, "enforcement contracts," regional enforcement programs of the reliability councils, and industry norms for best practices, but no penalties were imposed for noncompliance with NERC standards. The Energy Policy Act of 2005 led to these standards becoming mandatory with substantial financial penalties imposed for non-compliance.

Electric Power Industry Institutions and Organizations

The U.S. electric power industry today is composed of a wide variety of players, entities, and institutions, all of which play different roles, and the actions of individual asset owners and operators affect each other. It is a highly regulated industry, and facilities need to operate according to common standards and in coordinated operations. The "system" may behave as one large electrical machine, but its parts are owned and operated by more than 3,000 entities. Table 2.1 highlights the major industry players that own and operate electric power systems. Still, there are numerous

[1]Changes in reliability enforcement as a result of the Energy Policy Act of 2005 are discussed below in this chapter.

TABLE 2.1 Major Industry Players in the U.S. Electric Industry

Asset Owners	Institutional Structures of Asset Owners	Other Asset Operators and Coordinators	Government Entities and Regulatory Authorities	Industry Associations and Institutions
Vertically integrated utilities (owning generation, transmission, and distribution)	Investor-owned electric utilities (IOUs)	North American Electric Reliability Council (NERC)	State regulatory commissions	Electric Power Research Institute (EPRI)
Generation and transmission utilities	Rural electric cooperatives (RECs or Co-ops)	Independent system operators (ISOs)	Power marketing authorities (PMAs)	National Regulatory Research Institute (NRRI)
Transmission utilities or companies	Municipal utilities (MUNIs)	Regional transmission operators (RTOs)	Federal Energy Regulatory Commission (FERC)	Edison Electric Institute (EEI)
Distribution utilities	Federal power agencies	Regional reliability organizations (RROs)	U.S. Department of Energy (DOE)	National Rural Electric Cooperative Association (NRECA)
Generation companies			Energy Information Administration (EIA)	Electric Power Supply Association (EPSA)
Marketing companies			Bonneville Power Administration (BPA)	National Association of Regulatory Utility Commissioners (NARUC)
			Tennessee Valley Authority (TVA)	Association of State Energy Research and Technology Transfer Institutes (ASERTTI)
			Western Area Power Administration (WAPPA)	National Association of State Utility Consumer Advocates (NASUCA)

other stakeholders who actively participate in electric power industry activities.

Regulatory Activities

Due to its technical and economic structure, the U.S. electric power industry is one of the most highly regulated in the nation. While other nations have adopted state-owned or national utilities to provide electric service, the United States early on adopted an approach that included a large number of private firms operating in natural monopoly settings and whose actions (e.g., determining rates, defining terms of electric service) were overseen by public regulatory commissions.

State Regulatory Commissions

Nearly all states have public utility commissions and/or energy offices that govern certain activities of regulated utilities operating pursuant to laws in that state. These commissions govern the rates, terms, and conditions of service of investor-owned utilities in the state and, in a few cases, also regulate the rates of rural electric cooperatives. The scope of regulatory authorities varies by state but often includes approving tariffs, allowed return on investment, and service standards. In many jurisdictions, the most important powers held by state public service commissions are the ability to (1) set consumer prices, (2) impose penalties for noncompliance with rules and regulations, and (3) require prior approval of all financing.

Federal Energy Regulatory Commission

Various activities of entities in the electric power industry are also regulated by FERC, the federal agency authorized to implement, among other things, the Federal Power Act, the Natural Gas Act, parts of the Energy Policy Act, and other federal statutes. FERC regulates the terms and conditions of power delivery and transactions in interstate commerce and, with the enactment of the Energy Policy Act of 2005, is responsible for ensuring enforceable reliability standards for the electric power industry.

In general, users ultimately pay the electric supplier's cost of providing them with service. There is a longstanding tradition of cost-based rates for the parts of the industry not considered competitive, such as transmission and delivery service. In many parts of the country, much generation service is also provided and paid for on the basis of cost, rather than market-based rates.

In the 60 percent of the United States where markets are used to allocate power at the wholesale level, ISO/RTO-type organizations act as regulatory intermediaries under the jurisdiction of FERC and to a lesser extent state regulatory commissions. Their objectives are to administer fair and

efficient markets and maintain bulk power system reliability. For these organizations, reliability concerns take precedence over efficient market operation in periods of insufficient supply and/or system instability.

IMPLICATIONS FOR SYSTEM RELIABILITY OF AN INDUSTRY IN TRANSITION

Structural Changes in the Industry

The electric power industry has undergone considerable changes in the last two decades that have affected how the electricity infrastructure operates. Some of the once vertically integrated electric utilities that supplied generation, transmission, and distribution services have undergone restructuring that separated them into distinct entities with responsibility for only one or a few such services. In 1996, to mandate and facilitate competition at the wholesale level, FERC required transmission-owning utilities to "unbundle" their transmission and power-marketing functions and provide nondiscriminatory, open access to their transmission systems by other utilities and independent power producers. Some utilities pursued unbundling by creating separate divisions within their companies, others spun off certain assets into separate but affiliated companies, and others sold off assets to separate owners (primarily generating facilities). Some states required—or created powerful incentives for—utilities to divest their generation assets as part of a restructuring effort. Others required vertically integrated utilities to divest their transmission assets to independent entities. In addition, power marketers—who often do not own generation, transmission, or distribution facilities—now buy and sell power on wholesale markets and market electricity directly to customers. All of these changes created even greater variations of the operational landscape within the industry.

Competition in the electric power industry has led to significant changes in the operation of the system. More electricity is being shipped longer distances over a transmission system that was initially designed only to provide limited power and reserve sharing among neighboring utilities. However, in some regions of the country, neighboring utilities have long collaborated to operate, and to a lesser extent to plan and design, their combined systems as integrated power pools (e.g., PJM Interconnection in 1926, New York in 1965, and later on, New England). Centralized dispatch of generating capacity to meet demand led these utilities to devise mechanisms to exchange power among themselves in ways that resulted in the smallest production costs (economic dispatch). Electric utilities that were once solely responsible for ensuring that they owned adequate generation to meet the demand of the consumers within their own system now purchase a substantial amount of the power they need from the wholesale market, in some cases relying on independent power producers and other electric suppliers to build and operate plants (NEPDG, 2001).

Over the last 15 years, greater competition has been introduced into the wholesale portion of the electric business by the addition of non-utility power plants. The Energy Policy Act of 1992 made it possible for competitive power producers to be entitled to access and use a utility's transmission system. In some regions, these requirements put new demands on an already stressed power system. In 1996, FERC issued regulatory policies (FERC Orders 888 and 889) that formally required transmission owners to provide open and nondiscriminatory access to the competitive wholesale generation market, and to provide comparable terms and conditions to all market participants, including the generation used to serve a utility's own customers.[2]

FERC policies, in combination with technological and economic changes in the industry, placed extraordinary new demands on transmission systems. Utilities that previously planned and operated their systems for the benefit of their own customers' requirements were now required to take other market interests into account.

In the parts of the country where the traditional vertically integrated industry structure has been retained, there are really two predominant business models for ownership of transmission:

- Ownership separate from the control of transmission (whereby the control functions are handled by a third-party "system operator" and transmission assets are owned by the utility or other entities), which is basically the system that exists in the Northeast, parts of the Midwest, and in California and Texas); and
- Combined ownership of transmission assets and control of the grid (whereby the functions of the transmission service provided are combined in a single, vertically integrated entity—such as principally exists for utilities located in the Southeast).

In the Midwest, the committee believes that the gradual transition from the joint ownership model to the separate ownership and control model will continue.

[2]The long-distance telephone system is sometimes used as an analogy for the electric grid, in that a product can be generated in one place and delivered over a network of wires to the final consumer. From a technical operating point of view, however, an electric power transmission system is very different from the long-distance telephone system because power flows cannot be directed over specific predetermined paths, nor can the loading over any particular path be precisely limited by the system operator. There are limited modulating switches that can be opened or closed like throttles for AC transmission lines, so attempts to wheel power directly from one utility to another may in fact overload the lines of a mutually interconnected neighbor, creating serious operating problems (Linke and Schuler, 1988).

Industry Practice—Normal Planning and Operations

Dealing with Normal Disturbances in System Operations

The reliable operation of the power grid is complex and demanding for two fundamental reasons. First, electricity moves at close to the speed of light (186,000 miles per second, or 297,600 kilometers per second) and is not economically storable in large quantities. Therefore, electricity must be produced the instant it is used. Second, pending the development of affordable control devices, the flow of AC electricity cannot be controlled like a liquid or gas by opening or closing a valve in a pipe, or switched like calls over a long-distance telephone network. Electricity flows freely along all available paths from the generators to the loads in accordance with the laws of physics—dividing among all connected flow paths in the network (U.S.-Canada Power System Outage Task Force, 2004).

A defining feature of the electric power industry is that reliable operations are universally considered to be essential and a central design, operation, and planning challenge. The delicate operational features of the system require that the industry explicitly plan for and operate with the expectation that there will be disturbances that must be addressed to keep the system operating reliably. Planning for and operating around constant variations of conditions in the system is the norm.

NERC's basic reliability standard requires that the bulk power system be operated so that it can survive the single largest contingency—designated *N*–1—such as the failure of a major generating unit or transmission facility. Many utilities actually plan their system to operate somewhere between *N*–1 (at a minimum) and *N*–2 (meaning that the system would continue to operate reliably without two elements).

Causes of Disruptions

There are many reasons why disruptions occur on the electric system. These include human error, natural hazards, design flaws, and deliberate attack on the system. For example, human error can be a factor that contributes to the cause of a blackout. Therefore, electric industry employees must be highly trained to be able to tackle the complex and highly technical nature of power system planning and operations. Natural hazards with the potential to cause extended blackouts include earthquakes, hurricanes, tornados, ice storms, and severe thunderstorms. Such hazards are a major contributor to outages on the system. Various types of design flaws can occur in equipment, plans, procedures, regulations, policy, and response. Where lines are located adjacent to roads, vehicular accidents are a frequent cause of local outages, and stray animal incursions occasionally lead to short circuits in transformers. The industry goes through routine and episodic exercises to improve these systems to address such flaws.

Finally, disturbances can and do occur as a result of direct attack on the system. Insulators on distribution lines are a frequent target for vandals with guns. To date, no long-term blackouts have been caused in the United States by sabotage. However, this observation is less reassuring than it sounds. Electric power system components have been targets of numerous isolated acts of sabotage in this country. Several incidents have resulted in multimillion-dollar repair bills. In several other countries, sabotage has led to extensive blackouts and considerable economic damage in addition to the cost of repair (OTA, 1990).

Norms of Mutual Assistance

The utility industry has a long history of responding to various kinds of emergencies, be they relatively small, such as an outage of a transmission circuit or a generator unit, or more serious, due to tornado damage, hurricanes, or earthquakes. Most utilities have plans in place for restoring service after a total shutdown. These plans involve cooperative agreements and cultural norms in which utility crews from one company assist those in another area that need their assistance. Such cooperation allows much faster restoration of service following extensive damage from hurricanes or other major storms.

Reliability Coordinators

Historically, vertically integrated utilities established "control areas" to operate their individual power systems in a secure and reliable manner and provide for their customers' electricity needs. The traditional control area operator has exclusive operational authority to balance load with generation in its own area, to implement interchange schedules with other control areas, and to ensure transmission reliability (Functional Model Review Task Group, 2003). In sections of the country with integrated power pools, the control area spans several utilities' operating centers, and the pool's system operator maintains control over the facilities of all member companies.

As utilities began to provide transmission service to other competitive entities, the control area also began to perform the function of transmission service provider through tariffs or other arrangements. NERC's operating policies and standards have reflected this traditional electric utility industry structure and ascribed virtually every reliability function to the control area (Functional Model Review Task Group, 2003).

Beginning in the early 1990s with the advent of open transmission access and restructuring of the electric utility industry to facilitate the operation of wholesale power markets, the functions performed by control areas began to change to reflect the newly emerging industry structure. These changes occurred for several reasons. Some utilities separated their transmission from their "merchant

functions" (functional unbundling) and even sold off their generation. Some states and Canadian provinces instituted "customer choice" options for selecting energy providers. The developing power markets often required wide-area transmission reliability assessment and dispatch solutions, which were beyond the capability of many control areas to perform. In fact, even some control areas themselves unbundled some of the functions that they had traditionally performed (Functional Model Review Task Group, 2003). As a result, the then-current NERC Operating Policies, which are centered on control area operations, began to lose their focus and became more difficult to apply and enforce (Functional Model Review Task Group, 2003). Regions where contractually enforced compliance was the norm due to their previously having operated under a collaborative power pool arrangement were exceptions in this regard. In other regions, control-area protocols needed to adjust to the emerging market-driven changes.

The NERC Operating Committee formed the Control Area Criteria Task Force in 1999 to address these coordination problems (Functional Model Review Task Group, 2003). Realizing that there was no longer a "standard" reliability organization, the task force built a "functional model" consisting of the functions that ensure reliability and meet the needs of the marketplace. The functions performed by traditional, vertically integrated control areas; regional transmission organizations; independent system operators; independent transmission companies; and so on were "rolled up," and organizations registered with NERC as one or more of the following:

- Generator owners,
- Generator operators,
- Transmission service providers,
- Transmission owners,
- Transmission operators,
- Distribution providers,
- Load-serving entities,
- Purchasing-selling entities,
- Reliability authorities,
- Planning authorities,
- Balancing authorities,
- Interchange authorities,
- Transmission planners,
- Resource planners,
- Standards developers, and/or
- Compliance monitors.

This approach enabled NERC to rewrite its reliability standards in terms of the entities that perform the reliability functions (Functional Model Review Task Group, 2003).

Reliability coordinators must have the authority, plans, and agreements in place to be able to immediately direct (and count on the compliance of) reliability entities within their reliability coordinator areas to re-dispatch generation, reconfigure transmission, or reduce load to mitigate critical conditions in order to return the system to a reliable state. A reliability coordinator may delegate tasks to others, but it retains its responsibilities for complying with NERC and regional standards. Standards of conduct are necessary to ensure that the reliability coordinator does not act in a manner that favors one market participant over another.

NERC has a Reliability Coordinator Working Group (RCWG) that provides a forum for coordinating system-operating procedures in all four interconnections. This involves the following:

- Coordinating implementation of reliability standards to ensure consistency across the interconnections;
- Assessing fuel supply adequacy;
- Reviewing operating experiences from the previous peak demand season and planning for the upcoming operating peak demand season;
- Reviewing system disturbances and transaction curtailments for "lessons learned" and compliance with NERC reliability standards;
- Recommending new or revised reliability standards; and
- Providing advice to the Operating Reliability Subcommittee as it debates new or revised reliability standards.[3]

These reliability standards are based on calculations independent of the triggering incident. Under some conditions, other simultaneous surrounding events and risks to society that exacerbate the effect of particular power outages must be considered. One example might be the greater harm to society were an extended power outage to occur during subfreezing weather or in conjunction with widespread terrorist attacks. Thus, in the implementation of these reliability standards, specific procedural mechanisms should take into account the likely particular nature of terrorist assaults, which may differ from customary triggering events. And as an example, were multiple simultaneous terrorist assaults to become likely, consideration might be given to changing the system's design criterion from withstanding any single insult to having the bulk power system impervious to two or even three simultaneous losses on the system.

Changes Introduced with the Enactment of the Energy Policy Act of 2005: New Requirements for Mandatory Reliability Standards

For decades, the electric power industry operated under voluntary compliance with NERC's reliability standards. But in the past few years, the restructuring changes described above led to a consensus within the industry that new

[3]See Reliability Coordinator Working Group (RCWG), available online at http://www.nerc.com/~oc/rcwg.html.

statutory authority requiring mandatory compliance with national reliability standards was needed. In August 2005, Congress passed the Energy Policy Act (EPAct), which authorized FERC to issue rules governing the certification of an electric reliability organization (ERO) and procedures for establishing, approving, and enforcing electric reliability standards. EPAct amended the Federal Power Act to include a new section requiring FERC to certify an ERO that would develop, administer, and enforce reliability standards, subject to FERC oversight.

FERC's new regulations, finalized in February 2006, require that the FERC-certified ERO must submit each proposed reliability standard to FERC for its approval. Only FERC-approved reliability standards are enforceable. In addition to the ERO, there are roles anticipated for regional reliability entities, which may propose reliability standards through the ERO and then administer and enforce such standards if delegated to do so by the approved ERO. The final rule applies to all users, owners, and operators of the bulk electric power system in the United States (other than Alaska and Hawaii).[4]

NERC applied in April 2006 to be certified to become the ERO, and in July 2006 that application was approved by FERC. NERC also filed with FERC for approval of a series of proposed reliability standards in 15 categories, most of which are the same as those that have already been in effect for several years on a voluntary basis. As of March 31, 2007, FERC had approved 83 reliability standards, and another 24 were pending (FERC, 2007). NERC has stated to FERC that the proposed reliability standards are consistent with ensuring acceptable performance with regard to operation, planning, and design of the North American bulk-power system. The reliability standards became effective on June 18, 2007.

Under Section 215, FERC must either (1) approve a proposed reliability standard if it determines the standard is just, reasonable, not unduly discriminatory or preferential, and in the public interest, or (2) remand a proposed standard back to the ERO for further consideration when FERC determines that the proposed standard fails to satisfy this test. FERC has stated its expectation that even after an initial set of reliability standards is approved, the process of proposing, reviewing, and approving standards will be continual in order to accommodate changes in the electric system and subsequent improvements in the standards. Additionally, FERC has stated that although uniformity across the United States is a goal, it expects a certain amount of regional variation in standards in order to accommodate regional differences and unique features of specific systems in the electric power industry. This would suggest there will be both greater stringency in the national standard and particular approaches as appropriate given the physical characteristics of a region. Since the United States is interconnected electrically with Canada and Mexico, FERC expects that it and the ERO will need to work directly with regulators and electric industry participants from these countries to ensure the successful implementation of mandatory reliability standards (Moot, 2006).

[4]Groups covered include regional transmission organizations and independent system operators, independent power producers, investor-owned electric utilities, public power and rural electric cooperatives, and other load-serving entities.

LONG-RANGE PLANNING

Long-range planning has always been essential to providing reliable, economic electricity service. Coordinated planning is still needed, even where wholesale markets prevail and investment decisions are profit-motivated. Three factors make coordinated planning essential: (1) the capital-intensity of the electric power industry, (2) the long lead times required to get new facilities online, and (3) the absolute necessity of having adequate facilities installed for reliability in recognition that electricity cannot be stored. A fourth important factor for large-scale systems is the interplay between decisions to construct transmission and generation facilities, since both are necessary to get power to market, or to provide supply alternatives.

Over time, the scope and identity of who does the planning for power supplies and who identifies the requisite investments as societal concerns have evolved. In the emerging quasi-market-supply structure that exists for the industry in many sections of the country today, the very nature of and responsibility for that planning are open questions.

Vertically integrated electric utilities, either private-regulated or government-run, are, by necessity, a planned industry with exclusive supply rights and obligations to serve in particular areas. These have been the predominant institutional forms for providing electricity service in the United States since 1900, so it is not surprising that each supply entity has engaged in careful strategic long-range planning, given its desire to maintain and enhance service reliability and thereby customer satisfaction. Over the past 100 years, however, the scope of those plans has gradually expanded in a number of ways:

1. Geographically, as the size of individual firms increased and voluntary power-pooling organizations were formed among firms;
2. Contextually, to reflect social concerns, as environmental quality, then public health and safety, and finally regional economic well-being were recognized as being linked in consequential ways with the operation of electricity supply facilities; and finally,
3. Economically, to consider the type and primary source of energy supply, following the oil supply shortages of the 1970s when "integrated resource planning" became the popular process for public involvement in a democratic society.

Thus, a long and ever-more comprehensive planning process has evolved both within and external to this industry. Supplying institutions have tolerated the increasing external intervention in their own internal planning processes because without that public approbation, the legal right to site new generation facilities, and generally, transmission facilities also, could be denied.

The time and the cost of acquiring necessary regulatory approvals have become the major impediments to the siting and construction of new facilities in many regions of the country. In some instances, those approval costs can be an appreciable portion of the total project costs, including those for land and construction. "Deciding how to decide" has become an institutional art-form, involving legal, political, economic and behavioral insights on how to design efficient and fair decision processes. It also can be used to effect for parties intent on using those processes to block particular projects.

In the wake of the restructuring and deregulation of the electric power industry, firms must now determine whether or not to invest based on market-related criteria, but also must bear the risk of public-policy-type decisions concerning siting. A regulated or public firm could be reasonably assured of recovering those decision-related costs sometime in the future; the prospects are far less certain for a firm in a competitive market. While firms in other competitive capital-intensive industries also face siting approvals before they can expand their capacity, they can minimize their risk simply by waiting to construct until supply shortages have driven prices in the marketplace high enough to warrant the risk. Because modern societies have an utter dependence on real-time delivery of reliable electricity supplies, they simply may not be willing to rely on market forces alone to determine whether suppliers are willing to invest in a siting decision. Some degree of public participation and subsidy in recognition of the public nature of the decision may be warranted.

However, in the current transition to market-based wholesale electricity supply in many regions of the country, the allocation of responsibility for and the sharing of the risk of this decision making in the planning process have yet to be worked out.[5] Rationalizing the private and public nature of these approval processes is particularly important for electric transmission lines where authorizations must be acquired from many political jurisdictions that might be spanned by the desired new facility. If those approvals are not granted simultaneously, there is a tremendous incentive for jurisdictions to delay their individual decisions so that they are last in line, and therefore able to extract the most favorable concessions. The private merchant builder must factor all of these considerations into a decision on whether or not to try to invest and to begin to seek the necessary approvals; they are also factors the public sector must consider if it desires a market-driven process that serves the public interest.

Problems to be resolved abound. With the traditional regulated vertically integrated industry structure, the utility would decide whether it was more efficient to build new transmission or new generation (as well as where, when, and of what fuel source) in order to minimize costs while meeting reliability standards. In this context, the entity might even consider the value in terms of the economic risk reduction of maintaining a stable of diverse generation sources, in terms of their primary fuels. In the evolving market context, a generator must decide whether and where to build based on the going market price in different locations. A competitive transmission company must base investment decisions on price differences in electricity between regions, plus any fixed delivery contracts it can assemble ahead of time from buyers and sellers. Note that decisions to invest by either type of firm are likely to reduce the original price levels or price gaps, and so each firm must take that market effect of its investment into account. Firms must also consider how the interaction between likely new generation and transmission investments will affect their revenues in the future. However, these firms have little incentive to consider the effects of their investment choices on system reliability or fuel diversity risk without public intervention. This is one reason why many jurisdictions are establishing subsidization mechanisms for bringing renewable-resource-based generation online—although in some instances the transmission requirements to bring that remote energy to the load locations are neglected.

These anomalies all suggest at least an equal need for planning under a wholesale market supply scenario. Such planning would be somewhat different in type and scope from that practiced in an environment of regulated, vertically integrated institutions. FERC has recognized this by mandating that one of the requirements for ISOs/RTOs is for each to establish a planning process to identify needs and to initiate market-driven investments that might be required first, and if these prove inadequate, to then initiate regulatory-based investments.

In many ISO/RTO jurisdictions, however, a legal semantic distinction is being made between facilities needed for reliability purposes and those that might further some economic benefit (e.g., lower wholesale electricity prices). Since both functions are served over the same transmission network, this distinction is arbitrary, in terms of both the laws of physics and economic principles. Almost any transmission line that is built to enhance reliability will most probably also reduce congestion at certain times of the year, thereby reducing wholesale costs. Similarly, any line constructed to facilitate economical transfers of power most likely will have effects on reliability somewhere on the system. It may also facilitate access to diverse sources of generation further away, thus enhancing reliability and security. In fact, FERC seems to have recognized these relationships through its recently

[5]As an example, in New York State, a one-stop siting law had been in place, requiring that all public permits be reviewed and provided through a single integrated process. Since the advent of competitive wholesale markets, that law has been allowed to lapse, compounding the risk for private investment as piecemeal approvals must be sought.

issued Order 890 that mandates economic-based planning in all jurisdictions.

If public concerns about robust resilience to possible terrorist attacks are also considered, the required public overview of the planning process becomes further complicated. Moreover, additional factors to be considered are whether a competitive wholesale marketplace for electricity is a decentralizing force for the ultimate evolving configuration of the system. If so, the system may be inherently more resilient to failures, whether due to natural or human causes. However, the first requirement is that an integrated planning process exist to guide and offer benchmarks for the future evolution of the industry.

INCENTIVES FOR TRANSMISSION AND DISTRIBUTION FACILITY INVESTMENT

Except for those areas served by public power agencies, transmission and distribution facilities in the United States are built under the expectation of earning a competitive rate of return on investment through the prices charged for using those facilities. In the case of transmission, FERC usually sets the target rate of return that is factored into the maximum allowable price, whereas in the case of distribution, the state regulatory bodies approve the allowable rates for service. Point-to-point merchant transmission might be constructed without a regulated rate set by public monitors if sufficient price-differentials exist between the end points, and if there is little likelihood that new lower-cost generation facilities might be built at the high-priced end of the line. However, in many areas of the country, the risks involved in getting the necessary simultaneous approvals by many property owners and municipal agencies to site a lengthy line are usually prohibitive to private capital investment. Even government-built facilities face prolonged political fights over siting, compounded by debates over who is to pay for the line and who is the beneficiary, if user fees do not completely cover the costs.

Because the usual practice by most state public utility commissions is to establish a uniform price for service throughout a particular company's service territory, an increased cost incurred by a regulated entity to build a new transmission line will usually raise the rates for all its customers, even though a small subset may be the only ones to benefit from lower energy charges as a result of the new line. The disincentives to utilities regulated in this traditional manner are compounded when another utility is located between the generator and its customers and that third utility would need to add a line to connect the two. The third utility's customers gain no immediate benefit from the new line, but they may bear the cost. As an incentive to undertake the risks, FERC may approve a price for transport over that new line that is substantially greater than what many state regulators have been offering. FERC may also authorize the line-building utility to pass those charges on only to the line's users. However, if this utility also owns substantial distribution assets that are governed solely by a state commission, it runs the risk of having the state regulators offset the higher award by FERC for its transmission venture by lowering its price for distribution services.

These equity and fairness issues associated with cost-recovery practices become even more complex when the planned transmission line spans the borders of several states. Consequently, planning for and gaining the political approval for the construction of new lines become even more difficult. Some jurisdictions like Texas have sought to reduce these contentious issues by effectively declaring all transmission a public good (like the interstate highway system) and recovering the costs over all customers in the state. In other regions like the Southeast, where the utilities have remained vertically integrated and the opposition to siting new facilities is less vehement than in older urbanized areas, costs are again "socialized" over all users and integrated with prices for all components of service. In still other regions of the country like the upper Midwest, separate transmission-only companies have been formed. Such entities do not have to worry about state regulators offsetting their FERC-approved transmission rates since they offer no state-jurisdictional services.

CONCLUSIONS

- There are major aspects of the electric system that are common to all parts of the country, but there are also those that differ considerably by region—electrically, institutionally, economically, and in terms of regulatory oversight. Many historical factors account for these differences, and it is unlikely that this situation will change any time soon.
- Although there is ultimately a single operator responsible for each portion of the electric system, there are many such operators around the United States, and there are many more participants in the whole electric power delivery enterprise. In many respects, this is a highly decentralized but interconnected system.
- Power systems have always faced multiple sources of routine and persistent threats to reliable operations. Some kinds of threats are harder to deal with than others because of their diffuse nature, because they are associated with new technological developments, because they arise from regulatory incentives misaligned with investment requirements, or because they spring from new and not-well-understood sources of terrorist ingenuity and motivation.
- The transmission system is much more stressed, and thus more vulnerable, than it was a few decades ago. This is principally the result of two factors: (1) years of underinvestment in system upgrades due in part to ambiguities and changed incentives introduced by electric power restructuring and associated changes in the regulatory environment; and (2) the growing

amounts of power that must be moved between sellers and buyers in new competitive power markets have added complexity in the operation of the bulk power system.

- Improving system reliability comes at a cost. Decisions to reduce the level of risks—through the adoption of stricter standards or through investment to protect against various types of risks—have to take into account (implicitly or explicitly) the question of whether the benefits of reducing a risk is worth the expense.
- Typically, customers of electric service end up paying the costs for reliable operations, although noncustomers also may benefit if there are external social effects or broader macroeconomic consequences. These aspects of reliability concerning the public good, including increased immunity from terrorist attacks, cannot be properly accounted for through market-based supplies of electricity, and standards must be set and enforced by a central authority such as the ERO. Once those supply standards are set, their actual provision can be decentralized through markets if the proper payments are made to the providers.
- As with all public goods where different individuals receive different levels of service or value reliability differently, who pays what is a contentious issue. Questions of fair cost allocations are one reason that investments in strengthening the transmission grid have lagged in many regions of the country. A compounding factor is the continual political pressure to keep electricity rates low, despite the demands by some customers for higher power quality and reliability.
- One mandate of the ERO is to establish regional advisory boards that might coordinate the different political perspectives of federal, state, and local governments and their regulatory bodies, but how that dialog is translated into capital investment and revised operating practice has still to be worked out.

REFERENCES

Constable, G., and B. Somerville. 2003. *A Century of Innovation: Twenty Engineering Achievements That Transformed Our Lives*. Washington, D.C.: Joseph Henry Press.

EPRI (Electric Power Research Institute). 2003. *Electricity Technology Roadmap: Meeting the Critical Challenges of the 21st Century: 2003 Summary and Synthesis*. Palo Alto, Calif.: EPRI.

FERC (Federal Energy Regulatory Commission). 2007. *Electric Reliability: NERC Standards*. Available at http://www.ferc.gov/industries/electric/indus-act/reliability/standards.asp. Accessed June 2007.

Functional Model Review Task Group. 2003. *NERC Reliability Functional Model: Function Definitions and Responsible Entities: Version 2*. Available at ftp://www.nerc.com/pub/sys/all_updl/oc/fmrtg/Functional_Model_Version_2.doc. Accessed August 2007.

Linke, S., and R.E. Schuler. 1988. "Electrical-Energy-Transmission Technology: The Key to Bulk-Power-Supply Policies." *Annual Review of Energy* 13: 23–45.

Moot, J.S. 2006. "Testimony of John S. Moot, General Counsel, Federal Energy Regulatory Commission" before the Committee on Energy and Natural Resources of the United States Senate, May 15, 2006. Available at http://www.ferc.gov/EventCalendar/Files/20060515151838-SENR%20EPAct%2005%20Electric%20Reliability%20Provisions%20(Moot)%2005-15-06.pdf. Accessed August 2007.

NEPDG (National Energy Policy Development Group). 2001. "America's Energy Infrastructure: A Comprehensive Delivery System." Chapter 7 in *National Energy Policy: Reliable, Affordable, and Environmentally Sound Energy for America's Future*. Washington, D.C.: U.S. Government Printing Office.

OTA (Office of Technology Assessment). 1990. *Physical Vulnerability of Electric System to Natural Disasters and Sabotage*. OTA-E-453. Washington, D.C.: U.S. Government Printing Office.

U.S.-Canada Power System Outage Task Force. 2004. *Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations*. Available at http://www.nrcan.gc.ca/media/docs/final/finalrep_e.htm. Accessed October 2007.

3

Physical Security Considerations for Electric Power Systems

From its earliest days, the electric power industry has been able to provide, or rapidly restore, essential services during various types of natural emergencies. Later, during World Wars I and II and the Korean War, the industry had to deal with the potential for sabotage. This sabotage threat continued at a reduced level through the Cold War, but the main physical security concerns during that period were domestic problems with vandalism, theft, and tampering. However, recent international developments have created a heightened threat to the nation's infrastructure from terrorist attack, including the electric power supply and delivery system.

THE THREAT

Osama bin Laden has stated that the objective of the al-Qaeda Islamic terrorist movement is to "target key sectors of the U.S. economy."[1] The so-called mastermind of the 9/11 operation, Khalid Sheik Mohammed, also stated that al-Qaeda's goal was "to launch spectacular attacks on vulnerable symbolic targets."[2] It is evident from the various attacks carried out by terrorists groups against power systems elsewhere in the world that many such groups consider electric power systems to be on their list of potential targets.

Potential terrorist attacks against electric power systems include sabotage; physical assault; disruption of sensors, information systems, and computer networks; tampering with process safety; disruption of fail-safe systems; and indirect attacks such as disruption of water, fuel, or key personnel.

Although al-Qaeda has received the greatest attention, the U.S. Department of State lists over 42 international terrorist groups operating around the world today (Department of State, 2006, p. 83). Approximately 2,500 attacks have been conducted by such groups against transmission lines and towers in various parts of the world over the past 10 years.[3] The (next most frequently attacked power transmission target for international terrorists has been substations, with more than 500 attacks over the same period.[4] In Iraq, terrorist and insurgent groups have skillfully used their resources and insider contacts to repeatedly attack national power transmission, to cause both disruption and social unrest and also to steal valuable materials such as copper conductors. Similarly, terrorists have been attacking Colombia's electrical grid at a rate of over 100 times a year.

As noted in Chapter 1, if economic damage and social disruption become primary objectives for terrorists in the United States, the electric power transmission and distribution system would be an attractive target.

POWER SYSTEM CHOKE POINTS AND VULNERABILITIES

Electric power transmission and distribution systems are susceptible to attack generally with little risk to the attacker, a fact well recognized by saboteurs and terrorists. The remote locations of many transmission power lines, substations, communications facilities, or natural gas supplies to generating facilities allow attackers to conduct their operations with little or no risk of detection. Selecting points for attack and estimating the consequences are within the capability of technically trained individuals in the terrorist community.

High-value choke points, those facilities which, if destroyed, will significantly degrade power system capabil-

[1]Statement by Usama Bin Ladin: Al-Jazirah Space Channel Television, Oct. 6, 2002, as quoted in Scheuer (2004), p.17.

[2]"Substitution for the Testimony of Khalid Sheikh Mohammed" pp. 11–14, Central Intelligence Agency [no report title, number, or date], as quoted in Lawrence Livermore National Laboratory (2006).

[3]From November 1, 1996, to November 1, 2006, 528 substations were attacked worldwide. This number includes substations and switchyards collocated with substations that were attacked with rocket propelled grenades (RPGs), mortars, small arms, etc., and were the targets of actual and attempted attacks. For the same 10-year period, 2,539 transmission towers were attacked worldwide (attempted attacks). Data from The Energy Incident Data Base, Robert K. Mullen, bezoar@earthlink.net.

[4]Data from Mullen; see footnote 3.

ity, are easily located either on the ground or from system maps. Detailed maps of U.S. power systems were once readily available in the public domain and on the Internet. Despite attempts to control access to such maps, they can still be easily obtained. Commercially available satellite data, as well as direct observation on the ground, can also be used to readily update and confirm system map information for potential attackers.

Facilities and equipment can be damaged or destroyed by a variety of means well known to international terrorists, surrogate agents, and special operations military forces. Physical facilities are vulnerable to mechanical intervention or from serious physical damage from stand-off attack projectiles and explosive devices. In addition some choke points on the electric systems of the modern world are vulnerable to cyber incursion. Chapter 4 discusses the cyber threat. Any attack could be considerably amplified if aided by insiders, whether voluntary or coerced. The insider issue is discussed in Chapter 5.

Most utilities are well prepared to handle outages caused by all but the largest natural events. However, the power industry is not capable of reliable performance if major components are severely damaged on a widespread basis by deliberately planned terrorist acts or natural phenomena. Virtually no utilities are equipped or staffed to mitigate the consequences of multiple attacks against major critical components or from widespread impacts of natural phenomena like Hurricane Katrina. National security planners have devoted insufficient attention to this fact or to the fact that electricity must be produced and delivered, through highly complex technological systems, at the instant of demand, and cannot be easily stored.

Points of Vulnerability

Specific points of vulnerability can be better understood by considering briefly each major element of power systems: generators, substations, transmission towers, distribution components, system control centers, and customers or users.

Generators

Although this report focuses on the power delivery system, it is important to note that in some parts of the world generators have been targets of terrorist attacks. In the United States generator units and ancillary equipment are installed within a power house that is manned by operational personnel, giving them some protection. Some are inside a perimeter fence with physical security equipment and trained security forces, and others are being upgraded. However, most generating stations except nuclear plants have very limited in-place security measures which could be circumvented by expert saboteurs, and lack supporting contingency plans to coordinate with local authorities.

BOX 3.1
Security Criteria to Be Considered in Evaluating Substation Security

- Potential threat and probability of attack
- Frequency and duration of past security breaches
- Severity of damage
- Cost of breaches
- Safety hazards in the substation
- Equipment types and design
- Number and types of customers served
- Substation location
- Criticality of load
- Overall cost of facility
- Quality of service at existing substations
- Exposure to vandalism, sabotage, and terrorist attack of control houses, control equipment, and key electrical system components

Transmission Substations

Bulk Transmission Substations have unique security concerns in that they are relatively soft targets; they are vulnerable to stand-off attack as well as penetration attacks by adversaries compromising the substation's perimeter fences. There is general agreement among security planners that key high-voltage substations are the most worrisome terrorist targets within the power transmission system. They are also difficult to protect. Their replacement parts are difficult to obtain, and damage to substations can separate customers from generation for long periods.

Box 3.1 lists security criteria that may be considered in evaluating substation security.

Transmission Lines and Towers

Transmission lines have been a desirable terrorist target in countries suffering from insurrection or civil unrest. A circuit can be temporarily disabled by fairly simple means. Shooting insulators on a tower can short a line. Severing the legs of the tower with explosives can bring it down, shorting all the lines it carries. On some transmission lines, taking out a tower can cause a domino effect, resulting in a cascade collapse of several adjacent towers.[5] Taking out a tower where two lines cross can disable both circuits at once.

[5]Transmission lines normally consist mainly of suspension towers that are intended to support the conductors, which are under tension to minimize sagging. These towers are held in place by the conductors and require little horizontal bracing under normal conditions. If the lines break in one direction, however, the tower may be pulled down by the tension on conductors in the other direction. Thus a cascading failure of towers can occur up to a

Transmission lines are often very long and in sparsely populated areas. They make easy targets and cannot be well protected. However, they can also be repaired quickly unless there is a coordinated widespread attack. Even then, the transmission lines can be repaired almost as soon as replacement towers can be delivered. Thus transmission lines are of less concern than substations.

System Control Center(s)

Major electrical systems rely heavily on their primary system control center. Computers, telemetry, fiber, radio, and dedicated telephone lines are continuously used to monitor major system elements and transmit vital information to the control center. As discussed in Chapter 6, when routine disturbances occur, the system is designed to take certain remedial measures instantly and to automatically report these measures and conditions to the control center staff. Major disturbances often require quick decisions and reactions on the part of the staff to prevent widespread outages.

System control centers contain highly technical control and communications equipment as well as experienced system operations personnel. Any attack, such as with a vehicle bomb that would destroy or severely damage such a center, would also significantly impair the operation or restoration of a system by eliminating vital command, control, and communications (C3) functions and capabilities. In most cases there are redundant control facilities, and the system could still be operated, but C3 would be significantly degraded.

Security is very uneven across the system. Some control centers have been extensively hardened and have excellent access control and other security. Other utilities provide nominal local security for these centers that could easily be overcome by a determined attacker. Control centers could easily be sabotaged by insiders either to affect C3 loss or to support a broader system attack by outsiders.

Control centers could be a desirable terrorist target, particularly if the redundant center is also targeted. Loss of a control center would make the continued operation of the power system difficult and might cause widespread outages.

Distribution Components

From the transmission substation networked medium-voltage lines and substations carry the power to all the users "downstream" from the transmission system. Distribution components are more numerous and of lower capacity than transmission system components, and spare parts are generally in greater supply. Storms take an annual toll on distribution systems. Utilities are prepared for such emergencies and often pool their resources to aid each other in restoring service. Targeting of distribution system components can cause troublesome outages, but the magnitude of the problems will usually be more manageable than those resulting from attacks on the "upstream" transmission systems or generation stations, unless of course they are targeted at disrupting supply to a critical facility in conjunction with some other attack.

Other Collective Targets

Other targets, although not system choke points, can be key terrorist targets. These include:

- *Key personnel.* Hostage taking usually places the attacker at greater risk than does the mere destruction of facilities or equipment. However, it should not be overlooked by security planners as a tactic historically employed when coercive control is desired. Contingency plans, security awareness training, and timely threat briefings for key personnel have proven effective in these situations.
- *Major materiel yards.* Central supply points, and sites where major repair vehicles and high-voltage spare components are stored, present valuable targets. Although such sites have a lower priority, security plans could include responses to the potential for attacks on these sites.
- *Customers (Users).* From heavy industries to households, the entire North American societal infrastructure is dependent in varying degrees on the reliable functioning of these electrical systems. As users' demands fluctuate moment-by-moment, generation must be increased or decreased to keep all elements of the system and the demand in precise balance. Attacking individual consumer electrical facilities would have limited overall impact on society, unless those facilities constituted part of a coordinated attack on targets such as chemical facilities or facilities providing essential community services.

Countermeasures

Countermeasures to attacks on physical infrastructure such as substations include improved security engineering techniques, such as calculations of blast effects; the use of hardened construction; and calculation of minimum stand-off ranges for threat weapons. Along with site hardening, new and improved surveillance equipment to allow rapid identification of and response to attacks could be installed at critical facilities. These improved electronic surveillance technologies include point vibration sensors, leaky coaxial cable sensors, seismic disturbance and electrostatic field disturbance sensors, microphonic cable, and microstain fiber option sensing systems (a new technology for perimeter protection) that could be employed as appropriate at sites depending on the level of threat and risk present.

dead-end tower (which is self-supporting even under one-sided tension) or a corner tower (which is used when the transmission line must make a turn, resulting in asymmetric loadings on the tower).

A capability for locking and controlling manhole covers remotely, and for monitoring at points of access to underground utility systems in urban cores, would help protect key distribution lines. Today, when underground access points are secured (e.g., for a visit of a head of state or other major event), it is typically by welding and/or bolting the covers shut. This current labor-intensive case-by-case approach both increases the likelihood that the system will not be secured as often as it should be, and increases the likelihood that key access points will be overlooked.

Improved and expanded security systems would be useful in protecting key underwater cable systems. This could include multi-zone motion detection, automatic alarmed calls, live and recorded video transmission, remote control via use of information technology, and simultaneous streaming video transmission to operation centers. Some newer cables are now well protected, but some older cables still need attention.

Highly critical facilities require perimeter protection systems—including cameras, sensors, intrusion devices, access controls, lighting, fencing, buffer zone security, and so on—that are specifically tailored to the substation environment described in Box 3.1.

The DHS is currently working with industry security officials to build cooperation with local law enforcement in order to map out potential attacker approach and egress routes as part of the DHS Buffer Zone Protection Plan effort.

REPAIR AND RESTORATION

Electric power providers in other countries have been challenged to restore service, especially when transformers at substations have been attacked. The availability of spare parts at remote areas, site access for needed repairs, and transportation of heavy, large-load high-voltage transformers to the sites all complicate the recovery process. These issues are discussed further in Chapter 7.

In assessing vulnerability, repair and restoration capabilities must also be considered. Electric utility systems have an outstanding record of reliability due to facilities' maintenance policies and ability to restore or bypass common outages quickly. The pooling of equipment and manpower contributes greatly to this record. Experience has proven that a vulnerability-risk analysis is applicable to any power system. The degree of risk is balanced against past ability to repair equipment and restore service in an acceptable length of time. Personnel and equipment inventories for making repairs are maintained to meet historic requirements. Many of these issues are discussed at greater length in Chapter 7.

Replacement of damaged equipment following a multi-site coordinated attack on major components could take many months or, in absolute worst cases, several years. For example, substation and generator step-up transformers can require as much as 12 to 16 months to manufacture even under ideal conditions. Transporting, installing, and testing them can take several more months. The availability of special transportation equipment itself could pose serious delays. Utilities have enough skilled personnel and equipment under their control for smaller emergencies, but having the skills required to safely repair a severe multi-site attack on electrical equipment requires extensive planning, the availability of spare equipment, and activation of already-in-place mutual aid agreements. Recent regional natural disasters have also pointed out that there is a clearly defined need for state and federal government support and coordination in recovery and restoration efforts.

It has taken many years to engineer and build the nation's electric power systems. It is likely that reconstructing them after widespread, intelligently planned damage will require many months of highly skilled effort, assuming that the capability exists to manufacture or acquire the requisite components. The U.S. domestic ability to manufacture these components has eroded and moved offshore over the past 30 years, and is not likely to return without government action to bring manufacture of critical equipment back to the United States. Chapter 8 elaborates further on system restoration and the need for a critical parts inventory, particularly power transformers.

CONSEQUENCE MANAGEMENT

Since our modern society is almost totally dependent on electrical systems, the widespread loss of choke points on systems that serve clusters of key defense bases, critical infrastructure assets, and major metropolitan areas would have a very detrimental effect. Pumping of potable water, sewage, and irrigation water; sewage treatment; food and fuel supply and storage; refrigeration; medical facilities, prisons, banking, communications, refineries, shipping, transportation, commerce, and home/commercial life-support systems (heating, ventilation, and air conditioning) all depend on a continuously operating power supply in an interoperable system. Should these interoperable critical infrastructures cease to function for an unacceptable length of time, the consequences to national security, public health and safety, and the economy would be huge.

The federal government is concerned about the existing level of domestic electric power system vulnerability primarily because of the threat posed by international terrorists. The White House has provided briefings to industry on its concerns. The DHS has been organizing relationships with industry. Efforts to integrate national security considerations into electrical system reliability planning continue to evolve, and the utility industry is integrating low-cost security measures to strengthen bulk power supply systems, particularly those that serve key national defense or critical infrastructure assets. These efforts are coordinated through the North American Electric Reliability Council (NERC) or the newly created Electric Reliability Organization (ERO).

Various organizations and agencies involved in homeland defense have been in the process of identifying the thousands of critical infrastructure assets across the nation that must be protected. An objective is to develop plans to ensure that critical infrastructure assets have adequate security for continued functioning. Planners must realize that no matter how well protection plans for critical infrastructure perform, when the day of emergency arrives, all of those infrastructure assets are dependent on electric energy.

A new dimension of "national security reliability" is being used in the planning for reliability of the electric power industry. The North American Electric Reliability Council, with the Federal Energy Regulatory Commission (FERC) providing the regulatory support stipulated in the reliability provision of the Energy Policy Act of 2005, is leading the effort. Additional support is provided through industry groups, such as the Electric Power Research Institute (EPRI) and the Edison Electric Institute (EEI). Industry is also working closely with various federal government agencies, such as the Department of Homeland Security (DHS), Department of Energy (DOE), Department of Defense (DOD), Department of Justice (DOJ), Department of Transportation (DOT), Federal Bureau of Investigation (FBI), DOD's Technical Support Working Group (TSWG), and the National Security Council (NSC). It is important that these efforts be well coordinated to avoid conflicts in recovery and restorations efforts.

New security protocols and mitigation measures are currently being developed and adopted through cooperation between government and industry to provide protection against the current terrorist threat. Examples of these are provided in Box 3.2. Pilot projects involve advanced security technologies that include digital CCTV, fiber optics, smart cards, and biometric IDs and card keys, as well as fencing design and manufacturing improvements.

Efforts have also been made toward understanding interdependencies, and how the power industry fits into the national critical infrastructure framework. Regional interdependency exercises have been conducted to consider the resiliency of utilities, the water supply, telecommunications, oil and gas, banking, financial services, and so on.

POST 9/11 POWER INDUSTRY PHYSICAL SECURITY ENHANCEMENTS

Many physical changes have been made and security enhancements implemented since the attacks on the World Trade Center. These include an increased awareness of the need to be more cautious with regard to access to information and facilities as well as to ensure that employees and contractors are not likely collaborators with terrorists. Box 3.3 lists the steps that most utilities have now taken to limit access to facilities and information. In addition, electric power industry security personnel have begun to develop a set of technical physical security skills and practices of the kind listed in Box 3.4.

BOX 3.2
Examples of Security Protocols and Mitigation Measures Intended to Provide Protection Against Current Terrorist Threats

- Utility coordination and information exchange programs in place at the North American Electric Reliability Council and the Edison Electric Institute
- Development of new risk assessment methodologies
- Risk-awareness management principles and practices in use by utility consultants
- Security vulnerability assessments
- Implementation of security upgrades and transitioning from security enhancements to comprehensive programs
- Recovery planning
- Security outreach programs including exchanges of best practices
- Top-to-bottom emergency plan reviews and updates
- Review and updating of mutual support agreements
- Improvement of security engineering of substations and control centers

BOX 3.3
Steps Taken by Most U.S. Utilities to Limit Access to Facilities and Information

- Requiring positive ID for all personnel visiting facilities
- Instituting access controls for all pedestrians and vehicles passing through entrance gates
- Hiring additional security officers
- Increasing the frequency of facility security checks
- Increasing aircraft patrols of transmission lines
- Increasing liaison relationships among local law enforcement, the FBI, and the National Guard
- Upgrading security policy and procedures
- Updating employee security and emergency response guides
- Developing new gate designs and standards
- Developing industry-wide baseline of security standards
- Conducting employee security awareness training
- Instituting a "no tours of the facility" policy
- Reviewing all internal and external Web pages and materials for information that could be used by terrorists

BOX 3.4
Examples of Technical Physical Security Skills and Practices Being Developed and Implemented by Electric Power Industry Security Personnel

- Protecting system technical operations
- Gaining familiarity with the latest risk and vulnerability analysis systems
- Ensuring the physical security of equipment and systems
- Providing perimeter protection including fences, lights, gates and access controls, entrance and equipments locks, protection force fencing, electronic security systems, video surveillance systems, and building alarm systems
- Physically protecting telecommunications systems
- Streamlining security command-and-control systems
- Working with the National Incident Management System
- Conducting contingency planning
- Accessing intelligence sources and sharing local information
- Forming liaisons with local law enforcement organizations
- Initiating tactical planning of response operations
- Planning for exercise/implementation of defensive operations during heightened alert periods

CONCLUSIONS

- While the electric power transmission and distribution systems are resilient and are designed for rapid restoration after failure caused by natural and accidental events, they are vulnerable to intelligent multi-site attacks by knowledgeable attackers intent on causing maximum physical damage to key components on a wide geographical scale. A few natural events, such as large hurricanes and ice storms, pose similar challenges, although in those cases some of the system components, such as high-voltage transformers (that are most difficult to replace or restore), are less likely to be damaged.
- Electric power transmission and distribution systems are vulnerable to attack generally with little risk to the attacker. As most systems are currently configured and operated, attackers can conduct their operations without detection. Because the transmission and distribution systems are by their nature inherently distributed, it is very difficult to completely protect all key components, or to harden them against possible attack.
- However, there are steps that could be taken to reduce the vulnerability of critical components. These include:
  - —A variety of design and engineering steps to harden substation sites and make key components less vulnerable to physical attack. These include further hardening of control facilities; selective use of walls and roofs at substations (especially in built-up areas and at high-consequence facilities in remote areas); and hardened enclosures for key transformers.
  - —Improved integrated electronic surveillance that uses sensor and monitoring equipment, along with information-processing equipment, to allow rapid identification of and response to multi-site attacks.
  - —System tools that can identify and localize physical and control system problems and potential incidents. These are further discussed in Chapter 6.
  - —Greater use of robust self-supporting towers for both transmission lines and communication systems. This includes more frequent use of dead-end towers in transmission lines that use guide towers, as well as integrated communication and power towers and self-supporting microwave towers.
- Substations are the most critical choke points, followed by control centers. For these facilities there is a need to develop specific physical security equipment such as cameras, sensors, intrusion devices, access controls, improved lighting and perimeter security fencing, buffer zone security, and surveillance of approaches, as well as a greater human presence and upgrades in protection force training and response, all of which would be used to decrease vulnerability.
- Improved personnel-related security measures are needed, including better screening of employees, better access control, more realistic simulations and security training, programs to reduce the threat to key workers from biological and other attacks with weapons of mass destruction, and upgraded capability to deal with the insider threats. Details on these and other personnel issues are provided in Chapter 5.

REFERENCES

Lawrence Livermore National Laboratory. 2006. "The Jericho Option: Al-Qa'ida and Attacks on Critical Infrastructure." UCRL-SR-224072, June.

Scheuer, Michael. 2004. *Imperial Hubris.* London: Brassey's.

U.S. Department of State. 2006. "Country Reports on Terrorism 2005." Washington, April .

4

Vulnerabilities of Systems for Sensing, Communication, and Control

The operation of a modern electric power system depends on complex systems of sensors and automated and manual controls, all of which are tied together through communication systems. While the direct physical destruction of generators, substations, or power lines may be the most obvious strategy for causing blackouts, activities that compromise the operation of sensors, communication, and control systems by spoofing, jamming, or sending improper commands could also disrupt the system, cause blackouts, and in some cases result in physical damage to key system components. Hacking and cyber attacks are becoming increasingly common.

Most early communication and control systems used in the operation of the electric power system were carefully isolated from the outside world, and were separate from other systems such as corporate enterprise computing. However, economic pressures created incentives for utilities to make greater use of commercially available communications and other equipment that was not originally designed with security in mind. Unfortunately, from a security perspective, such interconnections with office and electronic business systems through other layers of communications have created vulnerabilities. While this problem is now well understood in the industry and corrective actions are being taken, the industry is still in a transition period during which some control systems have been inadvertently exposed to access from the Internet, intranets, and remote dial-up capabilities that are vulnerable to cyber intrusions.

Many elements of the distributed control systems now in use in power systems are also used in a variety of applications in process control, manufacturing, chemical process controls and refineries, transportation, and other critical infrastructure sectors and hence vulnerable to similar modes of attack. Dozens of communication and cyber security intrusions, as well as penetration red-team attacks, have been conducted by DOE, EPRI, electric utilities, commercial security consultants, and others. These "attacks" have uncovered a variety of cyber vulnerabilities including unauthorized access, penetration, and hijacking of control.

While the committee is unaware of any successful hostile cyber attack on the systems that control the operation of a power system, the risks posed by such attacks are sufficiently large to warrant serious consideration, continued improvement of key systems, and high levels of vigilance including careful attention to personnel training and operational procedures.

EPRI has conducted a survey of electric utilities to identify their concerns about grid security, cyber security, and communications security (EPRI, 2000). Figure 4.1 ranks the perceived threats to utility control centers. The most likely threats identified were bypassing controls, integrity violations, and authorization violations, with 40 percent of respondents rating the seriousness of each as either a 5 or a 4 on a scale of 0 to 5. Concern about the potential threats generally increased as the size of the utility peak load increased.

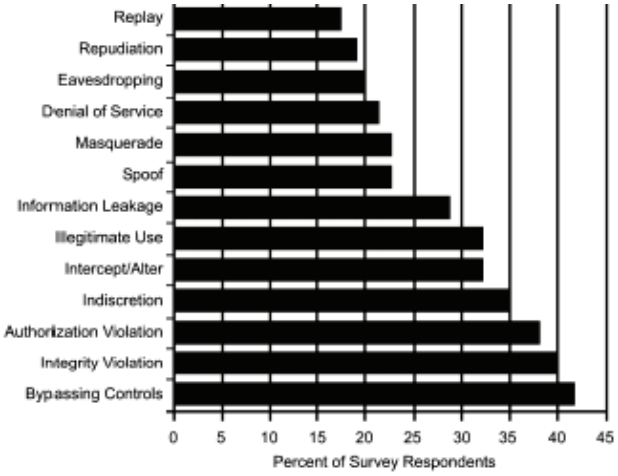
SENSING, COMMUNICATION, AND CONTROL SUBSYSTEMS

Functions of Sensing, Communication, and Control Elements of a Typical Power System

Figure 4.2 provides a simplified schematic diagram of the sensing, communication, and control elements of a modern power system. The elements of the system depicted in Figure 4.2 are defined and described below. Further details on the operation of many of these elements are provided in Chapter 6.

Energy Management System

The objective of the Emergency Management System (EMS) is to analyze the real-time measurements gathered by the supervisory control and data acquisition (SCADA) system (see next paragraph) to determine the reliability of the present operating condition of the grid, to alert the operators to any vulnerabilities to possible disturbances (contingen-



NOTES:

Authorization violation: Access by an entity that lacks the proper access rights.

Bypassing controls: Exploitation of system flaws or weaknesses by an authorized user in order to acquire unauthorized privileges.

Denial of service: Deliberate impedance of legitimate access to information.

Eavesdropping: Acquisition of information flows, sometimes by "listening" to radio or wireline transmissions, sometimes by analyzing traffic on a local area network.

Illegitimate use: knowingly or unknowingly intruding on system resources.

Indiscretion: Indiscriminate opening of information files and so on.

Information leakage: Unintentional provision of information to a disguised third party.

Integrity violation: Messages and the computer infrastructure subjected to unauthorized modification or destruction.

Intercept/alter: Intercepting and altering information flows, usually by accessing databases and modifying data.

Masquerade: Posing as an authorized user on a network, the most common method used by hackers to gain access to networks, often enabled by having other users' passwords. A masquerader can view secret information, alter or destroy data, use unauthorized resources, and deny legitimate users access to services.

Replay: Use of information previously captured without necessarily knowing what it means.

Repudiation: Denial by an entity that it undertook some action such as sending a message or receiving information.

Spoof: Occurs when a user or application believes it is using one of the legitimate computer services, while actually performing some different function.

FIGURE 4.1 Perceived threats to power system control centers as reported in a survey of electric utilities conducted by EPRI in 2000. SOURCE: Adapted from EPRI (2000).

cies), and to calculate possible operational changes that could improve the operational condition (i.e., more optimized in terms of cost and less vulnerable to contingencies). A very important automatic function of an EMS is automatic generation control (AGC), which involves measurements of system frequency interchange power flows, and power plant outputs to regulate system frequency and net power interchange via commands sent to power plants. An EMS always works in concert with a SCADA system, with the SCADA as the front-end component connected directly to the grid and the EMS as the back-end component with the heavy computational capabilities; this combination is referred to as the EMS-SCADA (or just EMS) or simply, the control center. Communication connections between EMSs in neighboring grids are common for the exchange of data describing the real-time conditions in the nearby interconnected system. More details on EMSs and their use in systems monitoring and control are provided in Chapter 6 of this report.

Supervisory Control and Data Acquisition

SCADA systems provide three critical functions in the operation of an electric power system: data acquisition, supervisory control, and alarm display. It consists of computers and display units with appropriate applications software, and is connected by a communications system to remote terminal units (RTUs) placed at substations that collect data and perform control of electrical system devices. The SCADA system polls the RTUs periodically to gather the real-time measurement data from all the substations and sends out control signals to the RTUs to control specific equipment. These supervisory control signals can be automatically generated by the SCADA computers or be manually initiated by the operator. The controls can be for operations of many types, such as the opening and closing of circuit breakers and the adjustment of control set points for transformer taps, generation of unit power outputs and voltage levels, DC transmission line flows, and so on. (It should be pointed out that SCADA is a generic name for this class of equipment, which is used for similar applications in many industries, including natural gas pipeline transmission and chemical plants.)

Most power system legacy SCADA systems operate in a several-second sample or polling rate. A separate SCADA system may be used for AGC. Modern SCADA systems may be networked using private Internet protocols, and may use faster sampling rates.

Remote Terminal Unit

RTUs are special-purpose microprocessor-based elements that are located at substations or power stations to interface with all the substation equipment. An RTU is connected to the SCADA system through a communication channel that

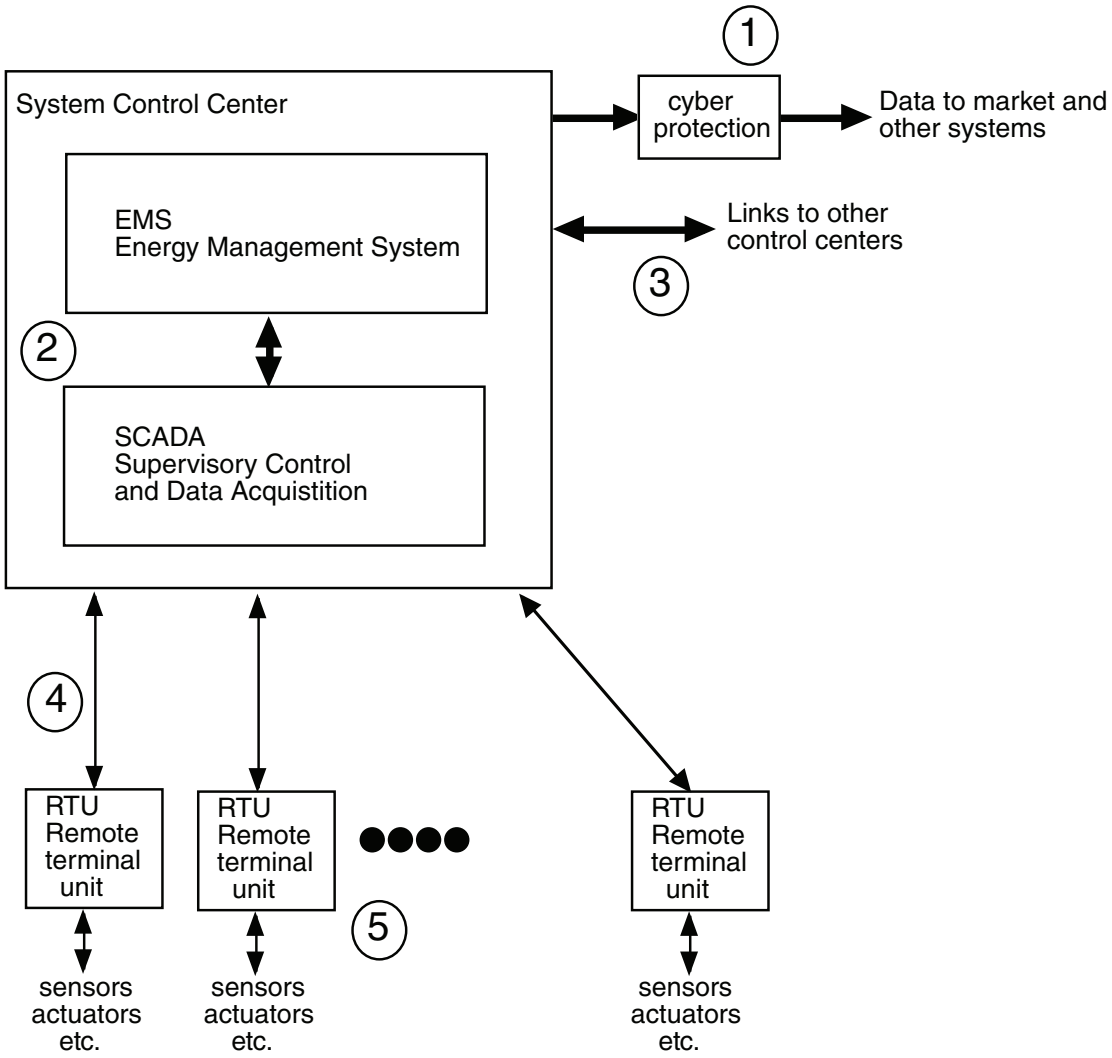


FIGURE 4-2 Simplified diagram of the sensing, communication, and control systems associated with a typical power system. Programmable logic controllers, protective relays, systems to control transformer tap settings and capacitor banks, automated metering systems, and distributed control systems as well as a variety of field devices all operate at this level. NOTE: Numbers refer to points of vulnerability discussed in the text.

uploads measurement data from the station and downloads control orders from the SCADA system. Within the station, the RTU is either directly connected to the equipment being controlled, or (because the new equipment is increasingly being controlled by microprocessors) through intra-station local communication networks. RTUs contain analog-to-digital and digital-to-analog converters, digital inputs for status, and digital or analog output for control.

A newer development is the intelligent electronic device, which often implies a built-in network capability such as Internet Protocol. Networked devices are, of course, more susceptible to cyber attacks. Sensors and the devices discussed below may also be considered intelligent electronic devices.

Programmable Logic Controller

Programmable logic controllers (PLCs) have been used extensively in manufacturing and process industries for many years and are now being used to implement relay and control systems in substations and power plants. PLCs replace binary (Boolean) logic networks of series and parallel combinations of electromechanical coils and contacts. They are used in mission-critical applications such as the special protection systems described in Chapter 6, sometimes in fault-tolerant configurations (e.g., triply redundant with two out of three required to agree for an output decision). PLCs have extended input/output (I/O) systems similar to those of transmission substation RTUs. The control outputs can be controlled by software residing in the PLC

and via remote commands from a SCADA system. In some applications, PLCs with RTU-reporting capability may have advantages over conventional RTUs. PLCs can have many real-time communication links inside and outside substations or plants.

A step beyond PLCs are programmable automation controllers (PACs), which include data acquisition, signal processing, monitoring, monitoring/display, and feedback control. In one manufacturer's product line of hardware and software, for example, the hardware can be either a PC or one of several real-time, embedded control devices.

Protective Relays

Protective relays are mission-critical electromechanical, analog, electronic, or digital controllers designed to respond to system faults and short circuits. When faults occur, the relays must signal the appropriate circuit breakers to trip and isolate the faulty equipment. Distribution system relaying must be coordinated with fuses and reclosures for faults while ignoring cold-load pickup, capacitor-bank switching, and transformer energization. Transmission-line relaying must locate and isolate a fault with sufficient speed to preserve stability, reduce fault damage, and minimize the impact on the power system. Modern digital protective relays can be networked, and settings can be changed remotely. Chapter 6 of this report discusses applications and the functional reliability of the control and protection systems.

Automated Metering

Automated metering is designed to upload residential and/or commercial gas and/or electric meter data. These data can then be automatically downloaded to a PC or other device and transmitted to a central collection point. With this technology, real-time communication links exist outside the utility infrastructure.

Plant Distributed Control Systems

Plant distributed control systems (DCSs) are plant-wide control systems used for control and data acquisition. The I/O count can be higher than 20,000 data points. Often, the DCS is used as the plant data highway for communication to and from intelligent field devices, other control systems (such as PLCs), RTUs, and even the corporate data network for enterprise resource planning applications. DCS technology has been developed with operating efficiency and user configurability as drivers, rather than system security. In addition, technologies have been developed that allow remote access, usually via a PC, to view and potentially reconfigure the operating parameters.

Field Devices

Examples of field devices are process instrumentation such as pressure and temperature sensors and chemical analyzers. Other standard types of field devices include electric actuators. Intelligent field devices include electronics to enable field configuration, upload of calibration data, and so on. These devices can be configured offline. They also can have real-time communication links between plant control systems, maintenance management systems, stand-alone PCs, and other devices inside and outside the facility.

Threats and Risk

As noted above, perhaps the most serious vulnerability to the various sensing, communication, and control subsystems that has developed in recent years, and which is now being rapidly rectified, has been lack of attention to connections from system control centers to the outside world (labeled as 1 in Figure 4.2). If these connections are not treated with great care, and if proper cyber security protection is not provided, they can in principle become a route for attackers from the outside world to create disruption, take control, and cause damage. Recent steps to dramatically improve the security of these links are discussed below.

While some of the operations of an electric power system are automatic, ultimately human operators in the system control center make decisions and take actions to control the operation of the system. Physical threats to such centers and the communication links that flow in and out of them are described in Chapter 3. But it is also essential to be concerned about two other factors: the reliability of the operators within the center, and the possibility that insecure code has been added to one of the programs in a center computer. The threats posed by "insiders" are discussed in Chapter 5. The risk of a "Trojan horse" or other deleterious program being intentionally embedded in the software of one or more of the control centers is real, and this can only be addressed by careful security measures both within the commercial firms that develop and supply this software, and careful security screening of both utility and outside service personnel who perform software maintenance within the center. Today software security upgrades often are not always supplied to end users, or users do not promptly apply the upgrades for fear of impacts on system performance. Current practice is to apply upgrades after SCADA system vendors thoroughly test and validate them, sometimes delaying deployment by several months.

A third source of vulnerability can arise from the essential links to other system control centers (labeled as 3 in Figure 4.2). Such links are essential for the operation of a large interconnected grid. However, even if the control center (shown as 2 in Figure 4.2) has taken all the necessary steps to protect itself from unauthorized access, either by external electronic logic or direct human intervention, if other control

centers have not taken similar steps, the entire system is vulnerable. That is, the system is no stronger than the weakest link in the chain.

The communication links between the system control center and various devices in the field labeled as 4 in Figure 4.2 are perhaps less worrisome than the items labeled as 1, 2, and 3 but still constitute a source of vulnerability. While obtaining access to the electronic logic of these communication channels and spoofing (i.e., sending a false signal) is always a possibility, a greater concern is jamming, or physical disruption, that would prevent system operators from knowing what is going on in key parts of the system, or from issuing needed commands.

Finally, the myriad devices that sense and control the power system in the field present vulnerabilities. Of particular concern are wireless and dial-up connections that could be monitored, spoofed, jammed, or reprogrammed. For example, if it were possible to reach and reprogram relays that control circuit breakers, considerable physical harm could be inflicted on some devices under some circumstances. However, today such relays can no longer be reached from the outside on most major systems, and new mandatory security regulations are rapidly resulting in corrective action in those few (typically smaller) utilities where it is still possible. Similarly, while wireless systems are seeing greater use, they are typically not employed in vital control systems. Nevertheless, because wireless is often much cheaper to implement than secure hard-wired controls, this is a potential source of vulnerability that warrants continued attention.

None of the protective strategies discussed will be effective without regular programs of staff training, and careful adherence to thoughtfully developed procedures designed to avoid the inadvertent introduction of alien software into SCADA systems, or the creation of interconnections to outside systems that may not be secure, or can be accessed via the Internet or similar means.

TOWARD SECURE SYSTEMS FOR SENSING, COMMUNICATION, AND CONTROL

During the past few years there has been a notable increase in the level of activity and interest in security for SCADA and control system communications both within the U.S. government and within the electric power industry. For example, DOE has created the National SCADA Test Bed, which includes the Idaho National Laboratory, Pacific Northwest National Laboratory, Sandia National Laboratories (SNL), and the National Institute of Standards and Technology (NIST). Work performed by these laboratories includes development of retrofit solutions, testing of vendor products, validation of encryption techniques and algorithms, vulnerability assessments for industry, and assessment of threats to SCADA and control system communications.

The January 2006 "Roadmap to Secure Control Systems in the Energy Sector" (Eisenhauer et al., 2006), the result of an effort co-sponsored by the U.S. Departments of Energy and of Homeland Security in cooperation with Natural Resources Canada, was developed through a collaborative process led by energy owners and operators. The authors explain that the purposes of the roadmap effort were to:

- Define a consensus-based strategy that articulates the cyber security needs of owners and operators in the energy sector;
- Produce a comprehensive plan for improving the security, reliability, and functionality of advanced energy control systems over the next 10 years; and
- Guide efforts by industry, academia, and government and help clarify how each key stakeholder group can contribute to planning, developing, and disseminating security solutions.

The authors note:

> [The] Roadmap builds on existing government and industry efforts to improve the security of control systems within the private sector by working through (1) the Electricity Sector Coordinating Council (coordinated by the North American Electric Reliability Council) and (2) the Oil and Natural Gas Sector Coordinating Council (coordinated by the American Petroleum Institute and the American Gas Association). The Roadmap is also intended to help coordinate and guide related control system security efforts, such as the Process Control Systems Forum (PCSF), Process Control Security Requirements Forum (PCSRF), Institute for Information Infrastructure Protection (I3P), International Electricity Infrastructure Assurance Forum (IEIA), Control System Security Center, and National SCADA Test Bed. (Eisenhauer et al., 2006)

Figure 4.3 provides a graphical summary of the results of this effort.

The U.S. Department of Homeland Security's Advanced Research Projects Agency (HS-ARPA) has recently funded several innovative technology development efforts. These efforts have the potential to yield new and effective tools to help secure SCADA and control systems for the electric power sector as well as for other sectors such as gas and oil, water, and transportation.

Individual companies and industry research organizations have also been active. Two examples are the American Gas Association (AGA) and the Electric Power Research Institute (EPRI). AGA has developed a specification for retrofit security of SCADA and control system communications. EPRI maintains several programs to provide member companies with security solutions for operational systems. However, utilities' interest in investing in major new initiatives in this area has been modest.

The North American Energy Reliability Council (NERC) Critical Infrastructure Protection Committee (CIPC) develops security standards and guidelines for the electric power

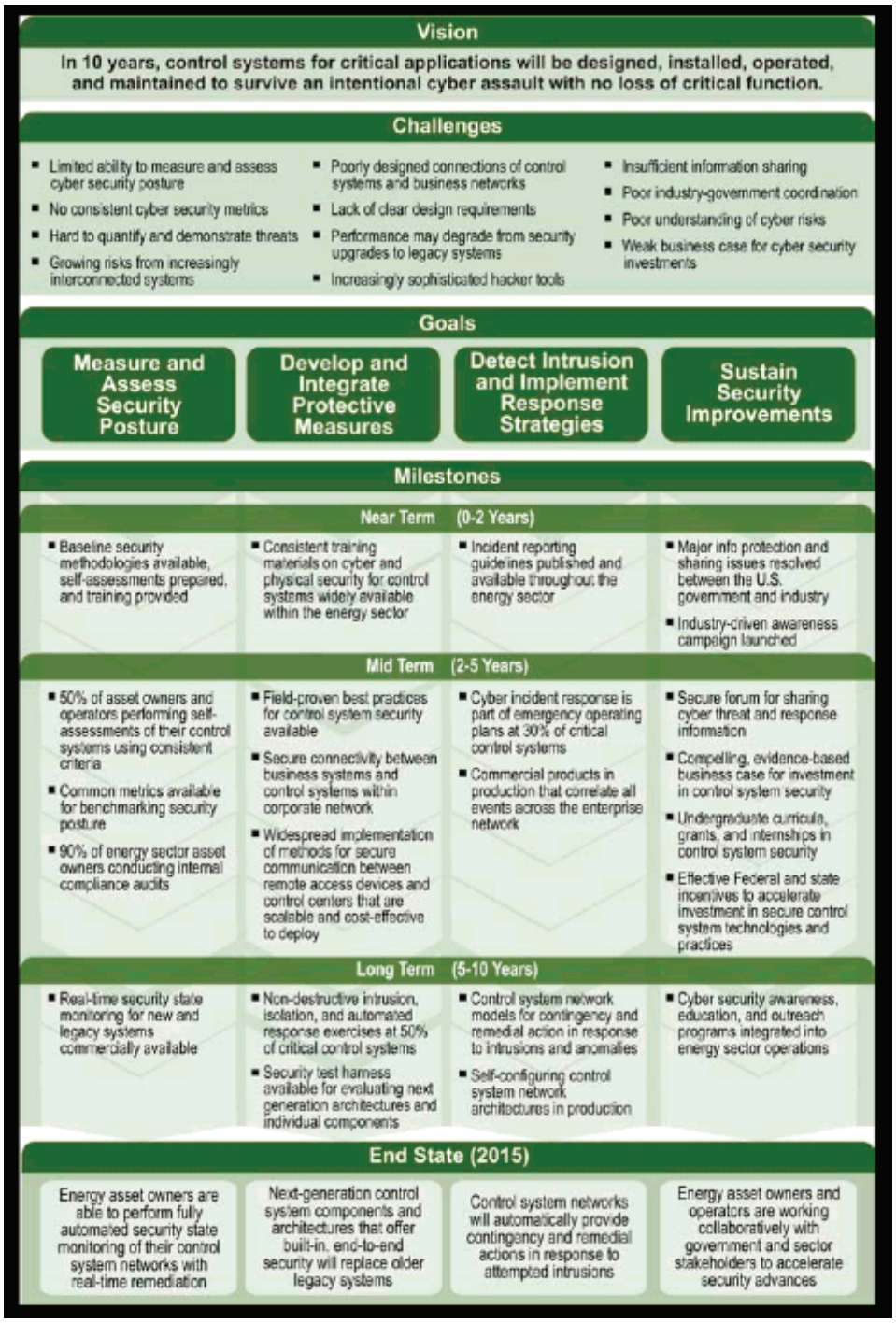


FIGURE 4.3 Road map for achieving secure control systems in the energy sector. SOURCE: Eisenhauer et al. (2006), p. 3.

industry. Formal CIPC representation is determined by the NERC regions, but meetings can be observed by any qualified industry member. A March 2006 report (NERC, 2006) by the NERC Control Systems Security Working Group (CSSWG) and the U.S. Department of Energy National SCADA Test Bed (NSTB) program highlights potential risks that can apply to some electricity sector organizations, describes practices that can help mitigate the risks, and provides a nonprioritized list of the 10 most common and threatening vulnerabilities to control systems in the electric sector based on the combined expertise of the NERC CSSWG members. The list, prepared by the CSSWG, is updated annually. As of March 2006, the top vulnerabilities of control systems and potential mitigation strategies were assessed to be:

- Inadequate policies, procedures, and culture governing control system security;
- Inadequately designed control system networks that lack sufficient defense-in-depth mechanisms;
- Remote access to control systems without appropriate access control;
- Auditable system administration mechanisms (system updates, user metrics, etc.) that are not part of control system implementation;
- Inadequately secured wireless communication;
- Use of a nondedicated communications channel for command and control, such as Internet-based SCADA, and/or inappropriate use of control system network bandwidth for noncontrol purposes (e.g., voice over Internet Protocol, or VoIP);
- Lack of quick and easy tools to detect and report on anomalous or inappropriate activity; inadequate or nonexistent forensic and audit methods;
- Installation of inappropriate applications on critical control system host computers;
- Software used in control systems that is not adequately scrutinized; and
- Control systems command and control data not authenticated.

Electric power utilities typically own and operate at least parts of their own telecommunication systems, which often consist of a fiber-optic or microwave backbone connecting major substations, with spurs to smaller sites. Historically, the energy industry operated closed, tightly controlled networks. Deregulation and the resulting commercial influences have placed new information-sharing demands on the industry. Traditional external entities like suppliers, consumers, regulators, and even competitors now must have access to segments of the network. The definition of the network must be expanded to include the external wide-area network connections for these external entities. This greatly increases the security risk to other functional segments of the internal network that must be protected from external connections. This is true whether a private network or the Internet is used to support the external wide-area network.

The external entities already have connections to the Internet, and as such the Internet can provide the backbone for the external wide-area network. Duplicating this backbone to create a private network requires not only large startup costs but also ongoing maintenance costs and potentially higher individual transaction costs than using the Internet. Nearly all control centers have multiple communication links. To understand the data security issues in the communication routes into the centers, more effort is required to determine how key data are routed before it gets to the center and where vulnerabilities exist (see Box 4.1).

In addition, standards for future solutions are being developed in several arenas, including, but not limited to, the International Electrotechnical Commission, the Instrumentation, Systems, and Automation Society, and, of course, the IEEE and ASME.

To address known vulnerabilities, the industry has worked diligently for the last 5 years to develop mandatory cyber standards through the NERC standards process. These mandatory standards will require a variety of preventive actions by all firms operating electric power facilities connected to the electric grids in North America. It is important to note that to effectively address the evolving spectrum of cyber threats, cyber standards should allow new technology solutions to be rapidly implemented and integrated to keep pace with these dynamic threats. Appendix E summarizes these new standards, which should be fully adopted within 3 to 5 years.

In summary, given the dynamic nature of cyber and communication threats, the long-term issue of cyber security and the hardening of the communications networks that provide mission-critical information to the energy control centers will require more investigation to enable dealing effectively with the threat.

CONCLUSIONS

- Minimizing penetration pathways to critical cyber systems is essential. The use of information/cyber systems makes more complex operation possible but also introduces new vulnerabilities. Any interconnection of the control systems with various corporate business systems, and thus to public networks, adds to the system vulnerability. Stand-alone autonomous systems are ultimately the most secure. Isolation of the critical systems must be the basic principle of cyber security for the power grid.
- Judicious interconnection is unavoidable. Although interconnection with public communication networks should always be avoided, control systems do need data from other systems, and vice versa. For example, energy management systems (EMSs) often need data from neighboring control centers or from market computers. Similarly, some engineering systems need data from the SCADA system or the EMS or from substation control or monitoring equipment. Such interconnections represent security risks and should be designed with care using high-quality security tools and the best available management practices. Firewalls with proper authentication and verification procedures, together with the use of unidirectional data transfer when appropriate, should be utilized.
- Best practices for security provisions always apply. Cybersecurity is part of FERC/ERO mandatory reliability standards. “Basic” security protocols and architecture must be standardized and adopted. SCADA/control system protocols should include elements to assure authentication and integrity. The

BOX 4.1
Addressing Control System Vulnerabilities

An article by Welander (2007) summarizes recent progress and work led by the North American Electric Reliability Council (NERC) in addressing 10 control system vulnerabilities highlighted in 2006 by the Control Systems Security Working Group of NERC (NERC, 2006). The article quotes a NERC official as stating that the 2006 version "'has grown from a simple listing of vulnerabilities in 2004, to include three levels of mitigations for each of the documented vulnerabilities'" (Welander, 2007, p. 38). Excerpts regarding 3 of the 10 listed vulnerabilities are given below:

- ***Inadequately secured wireless communication*** (including microwave technologies)

  Before installing wireless, it's important to do a complete assessment to identify the best areas for wireless use and ensure that leakage out of the plant is minimized. Wireless leakage occurs when you have transmitters or wireless-enabled workers walking around with tablet PCs or handheld devices. Those devices may be transmitting in an area outside a plant. (Welander, 2007, p. 42)

  On the wireless network side, technologies such as 802.11 b and g are often in place, operating in the 2.4 GHz spectrum. Often they have been deployed without a suitable site survey to determine if coverage is adequate and to evaluate if spurious emissions are limited so that people external to the facility must work hard to find these networks. (Welander, 2007, p. 42)

- ***Use of a nondedicated communications channel for command and control***

  [An example of this] would be the case with Internet-based SCADA. This vulnerability also could include inappropriate use of control system network bandwidth for non-control purposes, such as VoIP (voice over Internet Protocol). . . . IT [information technology] professionals typically look at application performance, and near real time for control is a foreign concept. Taking 300-500 ms extra to receive e-mail or a Webpage is largely unnoticeable; 300-500 milliseconds for control messages or safety messages could be disastrous. Often, what is an acceptable level of saturation or utilization from an IT perspective can spell disaster for controls. (Welander, 2007, p. 42)

- ***Unauthenticated command and control data***

  Not all controllers out there today authenticate who's making the change and authorize that the change is allowed for that user through the controller. This security step on most control systems is performed at a layer in the control system above the controllers. This leaves the controllers vulnerable, and that's why defense-in-depth is absolutely required. You've got to make sure the controllers are deep down in the security infrastructure, with multiple layers of defense above them. If you're not doing that, then your controllers are basically wide open on the Web. (Welander, 2007, p. 44)

Mitigation strategies for all 10 of the vulnerabilities range from using software packages to changing corporate culture. The online version of Welander's article (at http://www.controleng.com/article/CA6433393.html?text=welander) includes the full text of the NERC document (NERC, 2006) with three-tiered strategies for addressing each vulnerability.

process of developing, testing, and applying software security patches, and related upgrades, should be accelerated and requires careful and continuing management attention.

- Substation cyber security requires defense at several levels. Assuring security of communication between a growing multitude of microprocessor-based devices at substations and other distributed systems is a challenge that must be met with various levels of defense. All modern relays and other monitoring equipment have processors, and data capture and communications interfaces, which need to be connected, but this must be done with security as a strict requirement. Minimizing connectivity, requiring/ensuring strict authentication, and conducting regular testing are all important. Although wireless communication usage is increasing for various applications within substations, wireless links should not be used to implement critical control functions.
- Protection against human error is critical. Many controls are still manual and even the automatic control systems require manual testing and maintenance, thus allowing many human interfaces. In addition to limiting access and requiring strict authentication to screen out unauthorized personnel, systems should be hardened against human error. For example, testing equipment (laptops) has been known to have introduced viruses into substation equipment. Hardening

against human error automatically raises the barrier against malicious attack.

- Investment in process and personnel must be a priority. There has been a serious lack of investment in power system infrastructure in recent years, and market-based priorities are unlikely to support strategically increasing security in power systems. Cyber security, like the reliability of the grid, probably has to be mandated by the FERC/ERO process, which usually means that the mandatory standard (i.e., the minimum required) will lag behind best practices. Because cyber security weaknesses tend to provide highly opportunistic windows for would-be attackers, and mandatory standards processes tend to be slow, the industry must continue to look for ways to facilitate rapid and the reliable implementation of security upgrades and patches and to ensure that its personnel are well trained and applying best practices. Simply conforming to the last round of standards will often not be sufficient to provide adequate protection.

BIBLIOGRAPHY

AGA (American Gas Association). AGA-12 *Cryptographic Protection of SCADA Communications*. Available at http://www.gtiservices.org/security/aga12_wkgdoc_homepg.shtml. Accessed August 2007.

Amin, M. 2000. "Toward Self-Healing Infrastructure Systems." *IEEE Computer Magazine* 33(8): 44–53.

Amin, M. 2001. "Toward Self-Healing Energy Infrastructure Systems." *IEEE Computer Applications in Power Magazine* 14(1): 20–28.

Amin, M. 2001 and 2002. Special issues on control of complex networks. *IEEE Control Systems Magazine* 21(6) and 22(1).

Amin, M. 2002. "Security Challenges for the Electricity Infrastructure." *IEEE Computer Magazine* 35(4)(Part Supplement): 8–10.

Amin, M. 2003. "North America's Electricity Infrastructure: Are We Ready for More Perfect Storms?" *IEEE Security and Privacy Magazine* 1(5): 19–25.

Amin, M. 2004a. "Balancing Market Priorities with Security Issues: Interconnected System Operations and Control Under the Restructured Electricity Enterprise." *IEEE Power and Energy Magazine* 2(4): 30–38.

Amin, M. 2004b. "Electricity." Pp. 116–140 in *Digital Infrastructures: Enabling Civil and Environmental Systems Through Information Technology*, R. Zimmerman and T.A. Horan, eds. London, U.K.: Routledge.

Amin, M. 2004c. "North American Electricity Infrastructure: System Security, Quality, Reliability, Availability, and Efficiency Challenges and their Societal Impacts." Chapter 2 in National Science Foundation (NSF), *Continuing Crises in National Transmission Infrastructure: Impacts and Options for Modernization*. Arlington, Va.: NSF.

Amin, M. 2005a. "Energy Infrastructure Defense Systems." *Proceedings of the IEEE* 93(5): 861–875.

Amin, M. 2005b. "Scanning the Issue." *Proceedings of the IEEE* 93(5): 855–860.

Amin, M. 2005c. Special issue on energy infrastructure defense systems. *Proceedings of the IEEE*. May.

Amin, M., and C.W. Gellings. 2006. "The North American Power Delivery System: Balancing Market Restructuring and Environmental Economics with Infrastructure Security." Energy 31(6–7): 967–999.

DHS (U.S. Department of Homeland Security). 2006. "National Infrastructure Protection Plan." June. Available at http://www.dhs.gov/nipp. Accessed August 2007.

DOE (U.S. Department of Energy). 2002. "National Transmission Grid Study." Available at http://www.pi.energy.gov/documents/TransmissionGrid.pdf. Accessed August 2007.

DOE. 2003. "Annual Energy Outlook 2003." Energy Information Administration.

Dy Liacco, T.E. 1967. "The Adaptive Reliability Control System." *IEEE Transactions on Power Apparatus and Systems* 86(5): 517–531.

Eisenhauer, J., P. Donnelly, M. Ellis, and M. O'Brien. 2006. "Roadmap to Secure Control Systems in the Energy Sector." Report prepared by Energetics Incorporated, Columbia, Md., sponsored by the U.S. Department of Energy and the U.S. Department of Homeland Security in collaboration with Natural Resources Canada, January. Available at http://www.controlsystemsroadmap.net/.

EPRI (Electric Power Research Institute). 1999. *Electricity Technology Roadmap: 1999 Summary and Synthesis*. Technical Report CI-112677-V1. 160 pp. Palo Alto, Calif.: EPRI.

EPRI. 2000. *Communication Security Assessment for the United States Electric Utility Infrastructure*. EPRI Report 1001174. Palo Alto, Calif.: EPRI.

EPRI. 2001. *Electricity Infrastructure Security Assessment*. Vol. I–II. Palo Alto, Calif.: EPRI.

EPRI. 2003a. *Complex Interactive Networks/Systems Initiative: Final Summary Report—Overview and Summary Final Report for Joint EPRI and U.S. Department of Defense University Research Initiative*. Palo Alto, Calif.: EPRI, 155 pp.

EPRI. 2003b. *Electricity Technology Roadmap: Synthesis Module on Power Delivery System and Electricity Markets of the Future*. Palo Alto, Calif.: EPRI.

EPRI. 2004. *Supervisory Control and Data Acquisition (SCADA) Systems Security Guide*. EPRI Report 1002604. Palo Alto, Calif.: EPRI. Available at http://www.epri.com.

EPRI. 2005a. *Guideline for Securing Control System and Corporate Network Interfaces*. EPRI Report 1010714. Palo Alto, Calif.: EPRI. Available at http://www.epri.com.

EPRI. 2005b. "Strategic Insights into Security, Quality, Reliability, and Availability" (co-authors: M. Amin et al.). Report 1008566. Palo Alto, Calif.: EPRI, 128 pp.

Fink, L.H., and K. Carlsen. 1978. "Operating Under Stress and Strain." *IEEE Spectrum* 15(March): 48–53.

Gellings, C.W., and K.E. Yeager. 2004. "Transforming the Electric Infrastructure." *Physics Today* 57(12): 45–52.

Hauer, F.F., and J.E. Dagle. 1999. *Review of Recent Reliability Issues and System Events*. Consortium for Electric Reliability Technology Solutions, Transmission Reliability Program, Office of Power Technologies, U.S. DOE, August 30.

House Committee on Energy and Commerce. 2003. *Blackout 2003: How Did It Happen and Why?* Committee hearing September 3–4, 2003. Available at http://energycommerce.house.gov/reparchives/108/Hearings/09032003hearing1061/print.htm. Accessed August 2007.

Kropp, T. 2006. "System Threats and Vulnerabilities: An EMS and SCADA Security Overview." *IEEE Power and Energy Magazine* 4(2): 46–50.

Kundur, P. 1994. *Power System Stability and Control*. EPRI Power System Engineering Series. New York: McGraw-Hill.

Marburger, J. 2002. Testimony before the House Committee on Science, June 14.

National Science Foundation, Division of Science Resources Statistics. 2003. *Research and Development in Industry: 2000*. NSF 03-318. Available at http://www.nsf.gov/statistics/nsf03318/pdf/taba19.pdf. Accessed August 2007.

NERC (North American Electric Reliability Council). Undated. Disturbance Analysis Working Group database. Available at http://www.nerc.com/~dawg/. Accessed November 2007.

NERC. 2002. "NERC Security Guidelines for the Electricity Sector." Available at http://www.esisac.com/library-guidelines.htm. Accessed August 2007.

NERC. 2006. "Top 10 Vulnerabilities of Control Systems and Their Associated Mitigations—2006." North American Electric Reliability Council, Control Systems Security Working Group, U.S. Department of Energy, National SCADA Test Bed Program, March 16, 8 pp.

President's Commission. 1997. *Critical Foundations: Protecting America's Infrastructures.* Report of the President's Commission on Critical Infrastructure Protection. Washington, D.C., October.

Samotyj, M., C. Gellings, and M. Amin. 2003. "Power System Infrastructure for a Digital Society: Creating the New Frontiers." Keynote address. Pp. 1–10 in Proceedings of the CIGRE/IEEE PES International Symposium on Quality and Security of Electric Power Delivery, Montreal, October 7–10.

SNL (Sandia National Laboratories). 2005a. *A Reference Model for Control and Automation Systems in Electric Power*. SAND2005-1001C. Albuquerque, N.Mex.: Sandia National Laboratories. Available at http://www.sandia.gov/scada/documents/NSTB_Ref_Model_V1_2.pdf. Accessed August 2007.

SNL. 2005b. *Framework for SCADA Security Policy*. SAND2005-1002. Available at http://www.sandia.gov/scada/documents/sand_2005_1002C.pdf. Accessed August 2007.

US-CERT. 2005. "Control Systems Cyber Security Awareness." Pittsburgh, Pa.: Carnegie Mellon University, Software Engineering Institute, July 7, 7 pp.

Weiss, Joseph. 2004. "Control Systems Cyber Security—Maintaining the Reliability of the Critical Infrastructure." Testimony before the House Government Reform Committee's Subcommittee on Technology, Information Policy, Intergovernmental Relations, and the Census, March 30.

Welander, P. 2007. "10 Control System Security Threats." *Control Engineering* 54(4): 38–44. Available at http://www.controleng.com/article/CA6433393.html?text=welander.

5

Vulnerabilities Related to the People Who Run the Electric Power System

The employees and contractors who operate and support the U.S. power system have a remarkable record of dedicated and reliable service. However, just as physical substations, transmission lines, and information and communication systems can all be sources of vulnerability, so too, either inadvertently or intentionally, human activities can create or exacerbate disruptions in the operation of the transmission and distribution system.

It is obviously important to ensure that employees, contractors, and others who have access to critical physical assets and information systems are carefully and regularly screened for reliability. But, as with the other issues addressed in this report, it is also important to understand the broader context within which the issues of human reliability arise. Many jobs in the industry are becoming more technically demanding at the same time that the industry faces problems of an aging workforce, recruiting difficulties, and training needs that are among the most challenging of any major industrial sector.

In this chapter, the issue of ensuring the reliability of existing employees and contractors who have access to critical facilities is examined. Then, several broader issues are explored that complicate the problem of training high-quality staff and minimizing the chances that staff will inadvertently make mistakes that place the system at greater risk. Problems posed by the industry's aging workforce and the declining pool of qualified new entrants are also examined. This is followed by some discussion of vulnerabilities that could arise from an accidental or intentionally introduced pandemic.

SECURITY THREATS FROM INSIDERS

Employees and contractors with legitimate reasons for access to the electric power system could do great harm should they ever decide to do so. Implicitly, such insiders have the capability to damage physical assets such as transformers and switch gear even more effectively than from attacks by outsiders. Great damage could also be done by system operators who intentionally took actions to place the system in vulnerable conditions. As noted in Chapter 1, disgruntled employees pose some risk but would typically be expected to operate alone. In contrast, one or several insiders working in conjunction with outsiders bent on inflicting major damage and disruption could likely do far more damage. While similar damage could also be done either directly or indirectly by contractors with access to utility equipment, a more subtle and troublesome concern is the possibility that contractor personnel who were charged with maintaining and updating critical software and intent on doing damage might insert "Trojan horses" or other destructive computer programs that could later become activated and wreak havoc in control systems at some future time.

Background security checks on all potential employees and periodic reviews of critical employees are essential. So, too, are such checks on all contractor personnel with direct or indirect access to critical elements of key physical or information and communication systems. Reviewing the quality of these security checks is also essential. Today, background checks are often outsourced to security service companies that begin the background checks as part of the initial employment process. Thorough, competent background checks must be conducted to ensure that electric utility personnel remain trustworthy and law abiding, with no links to terrorist organizations or criminal activity. Additionally, in today's environment, it is important that key employees have government security clearances so that they can work with and obtain intelligence information from government and law enforcement officials.

Standardized credentialing of utility and contractor personnel for security purposes is thus important and should utilize modern ID card technologies that use photographs, card readers, proximity access, and, where appropriate, RFID (radio frequency ID) capabilities. Standardized enterprise-wide credentials allow employees to function and gain access, in a manner that allows them to respond to a wide variety of incidents as well as to operate across a wide geographic area. While there has been much progress

in background checks of operational and security personnel, there is still much work to be done in this area, both within operating companies and in the contractor community.

PLANNING, TRAINING, AND REHEARSAL

Preparatory Activities

The first important step to ensuring readiness in the face of unplanned events is by preparation through the planning process. The ability to identify key "what-if" scenarios and then develop the appropriate response plans to deal with such contingencies is the first key step in developing a comprehensive emergency response plan. Once plans have been developed, the next step is to test their effectiveness. The best way to accomplish this objective is through careful training and the use of drills and exercises. A well-constructed drill can test the ability of personnel to respond to simulated real-life situations as well as test their understanding of the overall plan. Well-designed drills test the ability of personnel to understand their roles and responsibilities as well as test the overall effectiveness of the plan in resolving the emergency situation. Crucial elements for a successful exercise include establishing clear objectives, providing realistic scenarios that simulate real-life conditions, and establishing expected actions or outcomes. Perhaps the most valuable component of a drill is an after-action review of the exercise. This allows for modifications to the plan to be discussed and implemented and an opportunity to avoid the risk of overgeneralizing from the results of a specific scenario or exercise. As further discussed in Chapter 7, many drills should include participants from outside local, state, and federal agencies.

There is also a need to reduce the vulnerability of key workers to both conventional security threats (e.g., from the use of firearms and explosive devices) and potential chemical/biological attacks. Employees serving as first responders should be provided with chemical and biological awareness training. The scope of this training should include threat and agent recognition, protection and first-aid training, personnel protection equipment, detection and sensor equipment, and training in emergency decontamination procedures.

Lastly, there is also a need for better and more realistic simulations and security training. While much has been done by industry in the security training area, better and more frequent simulation and red-teaming security exercises will improve the readiness of security personnel.[1] Dramatic improvements in personnel readiness can result from introducing a comprehensive security training program that systematically includes emergency notification exercises, security training seminars, tabletop exercises, red-team exercises, force-on-force exercises, command-post exercises, and full field exercises. Training simulations and exercises such as these can:

- Provide insights into potential problem areas;
- Encourage a team approach to meeting security challenges;
- Improve organizational teamwork; and
- Audit the status of security preparedness.

First Responders

It has sometimes proved important even in the aftermath of natural catastrophes to provide police protection for line crews working to restore power systems.[2] In the event of a terrorist action, restoration workers themselves may become targets. Workers on poles and towers and in open areas in substations are particularly vulnerable, especially if the surrounding area is complex and offers cover in which it is easy for assailants to go undetected. Further complications arise if terrorist attacks involve chemical, radio nuclear, or biological agents. Workers must be able to determine if such an attack has occurred, the nature and extent of contamination, and what protective measures need to be taken before they can enter and work in an area where power system damage has occurred.

Restoration of a system in the context of a crime scene, as might be the case in a post-terrorist event, can also lead to involvement by personnel from myriad local, state, and federal law enforcement, security, and emergency agencies. In such situations, it is important to have previously established lines of communication. Clear manuals to explain the assignment of first responders, the roles of assisting utility teams, the jurisdiction of different law enforcement agencies, and so forth can provide a presumptive roadmap for action. As discussed in Chapter 7, carefully clarifying ahead of time the chain of command for restoration practices, for work rules, and for operational expectations on the ground will be very helpful in promoting efficient recoveries during the stress of an actual terrorist event.

ERRORS AND AUTOMATION

The Electric Power Research Institute (EPRI) recently studied about 100 North American power outages that occurred in recent years and concluded that 12 of them were attributable to human error, either by operators in control rooms or by maintenance workers in the field (EPRI, 2000).[3]

[1]Red teaming is the use of a group of specialists to conduct a mock attack on a power system. It is frequently used to test facility and cyber security strength against attack. It is intended to uncover vulnerabilities and weaknesses and to assist in hardening the system.

[2]For example, in the aftermath of Hurricane Katrina several line crews were shot at before police protection was introduced.

[3]For example, improper maintenance of relays contributed to cascading events, thus worsening the New York City blackout in July 1977. Improper maintenance at a San Mateo substation triggered a December 8, 1998, blackout in the San Francisco Bay Area, which cascaded from San Mateo, affecting 2 million people for up to 7 hours. Control room operator errors were a key factor in the Northeast blackout of August 2003.

Similarly, the London blackout in August of 2003 has been attributed to an incorrect relay setting.

Improved procedures and system designs can help avoid errors. With good surveillance and training, many errors can be detected and corrected before they lead to problems. But errors do happen. If they were to occur in the face of an unfolding terrorist attack, they could considerably complicate an already serious situation. This prospect further strengthens the importance of contingency planning, training, and simulated exercises.

The explosion in available information has made attention time an extremely valuable commodity for all workers. Most automated networks require some human intervention not only for routine control, but also especially when exhibiting anomalous behavior that may suggest actual or incipient failure. Progress continues to be needed in the design of interfaces that help users retain good situational awareness while allowing them to focus on the most important factors in a complex and rapidly evolving dynamic situation. Improved displays of the state of the electric power grid are being installed in control centers (Christie and Mahadev, 1994, Overbye and Weber, 2001), but there is room for a great deal of imaginative innovation in this area.

Humans have cognitive limitations that can cause them to make serious mistakes when they are interrupted. While actual or imminent local failures can be detected automatically, operators can easily be distracted by other tasks—including responding to multiple systems warnings. In the worst case, a detected failure can set off a multitude of almost simultaneous alarms as it begins to cascade through the system. Under this scenario, system operators may be unable to accurately determine the real source of the problem, which in turn could lead to the whole network shutting down automatically.

In recent years, systems have been designed that allow users to delegate tasks to intelligent software assistants ("softbots") that operate in the background, handling routine tasks and informing the operators in accordance with some protocol that establishes the level of their delegated authority to act independently. In this arrangement, the operator becomes a supervisor, who must either cede almost all authority to subordinates or be subject to interruption by them. At present, there is very limited understanding of how to design user interfaces to accommodate interruption.

Two products developed by EPRI for substation operations and maintenance (O&M) could lead to tools for analysis of human performance. The first is the Maintenance Management Workstation (MMW), a data integration, analysis, and display tool that is used to guide decisions on equipment maintenance and replacement. Since it can connect to any database and data source, it could be adapted to analyze operational decision making. The other tool is the Planning and Resource Optimizer (PRO), which is a planning tool to assist in task scheduling and resource allocation (including labor). It allows for consistent and efficient work planning, optimized schedule and resource allocation, and facilitation of unexpected changes, and it can be used for backlog management. It also integrates with the MMW.

The degree of field information available to operators is also an area of concern. In many cases, there is little feedback from the maintenance crews to operations engineering and design engineering personnel with regard to the actual work done during a maintenance task and the as-found condition of the asset being maintained. Insufficient coordination and communication among these various personnel can result in a lack of information that can lead to less than optimal configurational control of the system and to incorrect decision making in responding to a system alarm or failure. As one example of attempts to address this issue, ConEd is evaluating a hand-held reporting system that requires specific feedback that can be uploaded to the work order management system. Such a system could enable an operator to quickly assess field work performed in evaluating the implications of an alarm. Despite the progress made to date in addressing the shortcomings of automation and human performance, the following challenges remain:

- *Application of statistical methods to extract information and trending on human performance.* These analytical techniques can be combined with enhanced visualization and techniques to improve situational awareness of the state of the system (perhaps using multimedia user interfaces and virtual reality) to assist the human operator.
- *Network visualization and situation awareness.* The exact nature of the information needed by operators, managers, users, and the general public may vary, but all need to understand what is going on in the infrastructure network. Adequate visualization of the state of the system is required for situation awareness. The proliferating new technology for multimedia user interfaces, and for virtual reality in particular, needs to be evaluated and fitted into this context of human performance. Such technology also should be incorporated into existing training simulators having adequate modeling and database capabilities at a regional transmission operator or an independent system operator level so that any entity in the region could use the same setup for its training facilities.
- *Interface design.* Little use has been made of esthetic considerations in the design of interfaces, yet it is clear that humans are attracted to, and seek to use more frequently, that which is esthetically pleasing. Such considerations may also be important if means are provided (e.g., on cable or broadcast television) to pass disaster mitigation information to the general public.

AGING WORKFORCE, RECRUITING, AND TRAINING

A skilled workforce is critical to continued reliable operation and resilience of the nation's electric power system. Maintaining a skilled force is increasingly challenging for utilities, manufacturers, and consultants to the power industry.

The average age of all power system employees has increased significantly over the last decade. A serious shortage is developing, and will continue for several decades, as many of today's employees reach retirement age. The loss of this expertise is a serious concern. Unless this issue is resolved, the nation's electric power system will become less reliable and more vulnerable to external threats, including terrorist intrusion and disruption from natural phenomena. Preparation for, and an effective response to, a terrorist attack can only be achieved with a highly skilled and flexible workforce that is adequately sized.

For most of the past century, before the more recent widespread restructuring, the corporate culture of utilities focused on effective—perhaps liberal—use of human resources to ensure excellent performance and function. Jobs were seen as highly secure. Many professional and skilled workers remained with a company for their entire career. The complexity of managing investments, conducting system planning, running operations, running plant engineering, managing construction, and conducting maintenance required workers who were both highly trained and knowledgeable, but able to balance the needs of all stakeholders, including regulators and customers.

Industry restructuring, pressures from Wall Street and regulators, mergers and acquisitions, and the evolution of wholesale markets have led to massive reductions in the U.S. electric utility workforce. Similar to other industries, the goal of increased productivity has been largely realized, albeit with greater risk of insufficient human resources. Ashworth (2006) notes that 2005 employment levels in the U.S. power industry have "declined by 23.7 percent [compared] to pre-1975 levels, while output has continued to grow by 30 percent over the same 15 year period" (p. 1661). This substantial downsizing has made electric utility jobs far less secure and has made many jobs in the industry more stressful. Skilled laborers now often find that employment in other sectors is less demanding and more rewarding.

Ashworth (2006) also reports that the median age of the electric utility workforce is 3.5 years older than the U.S. national average of 43.9 years. Approximately 50 percent of electric utility workers are 45 or older. The average age of line workers is approximately 50. Analysis by Reder has shown a significant problem with the age distribution of engineers in the power industry (Reder, 2006). Many companies have less than 10 percent of their workforce below age 35, with the average age of employees increasing each year. The age distribution shown in Figure 5.1 projects an unsustainable and unhealthy increase in the average age of power industry employees over the next 10 years.

As many as 200,000 of 400,000 electric utility workers will be eligible to retire in the next 5 to 10 years. Ashworth (2006) reports results from a survey of top human resource executives in which 45 of the 65 respondents placed "aging workforce" in the highest category of problems facing the industry. This was followed by "skilled workforce" and "cost of employee benefits," both of which were ranked in the top category by 11 of the 65 respondents. Clearly, with a substantially older workforce that will retire sooner, the loss of critical skills and the training of replacement workers are significant problems for the electric utility industry.

It is clear from these demographics that disruptive changes in the electric utility workforce are imminent. Many utility engineers report a substantial broadening of work assignments without the necessary time to become "experts" in the new areas of responsibility. They cover more functions and technical areas at less depth, primarily due to reductions in the available pool of engineers and other workers to cover the tasks at hand. Both because of the much smaller research investments being made by industry and government in power-related topics, and because students view opportunities for upward mobility and flexible life styles to be greater in "hot" fields such as information technology and microelectronics, many engineering schools have completely dropped power engineering as an area of study. Venkata (2004) estimates that today only 1.5 percent of engineering students select power engineering as a focus area. Clearly, the available pool of power engineering bachelor's and master's degree students is small, and competition by employers for future graduates will be intense.

University power engineering programs are key to the availability of sufficient numbers of engineers for the power industry. However, power engineering educators generally agree that electric power engineering education is facing a crisis. The educators on the committee that prepared this report concur that there are fewer than 12 truly viable power engineering programs in universities in the United States. Several power engineering programs have only one or two remaining faculty who are near retirement and will likely not be replaced.

The reduction in the number of viable power engineering programs in universities can be attributed to several factors. Many utilities stopped recruiting new students as they reduced their workforce. As a result of mergers, competitive forces, and deregulation, industry support of university programs in the form of scholarships, fellowships, and research funding has significantly declined. The level of funding from electric utilities to universities is significantly lower then it was 20 years ago.

Deans and department heads in universities must make decisions about the technical areas where new faculty will be hired. Generally, new faculty are hired to focus on industries that provide a strong demand for students and heavy R&D support. The electric utility industry has not demonstrated either of these characteristics over the last two decades.

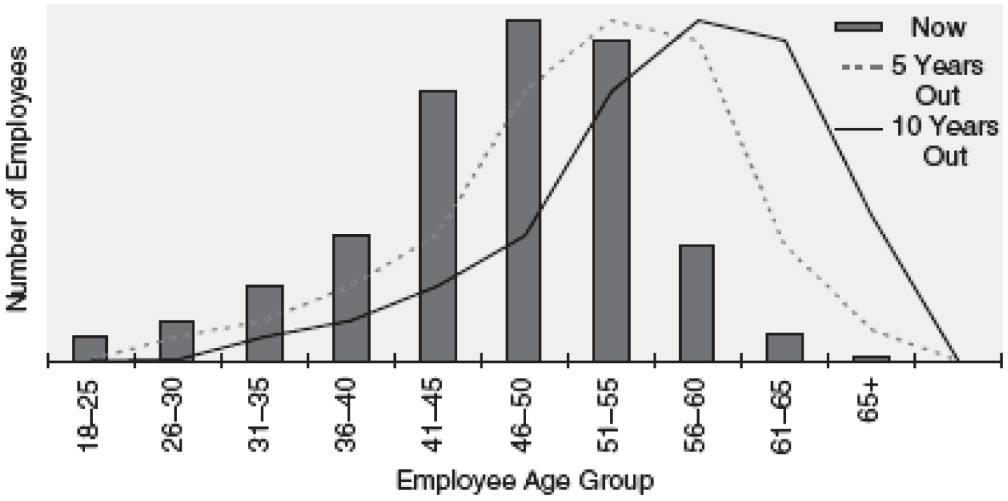


FIGURE 5.1 Typical power industry employee age distribution. SOURCE: Ashworth (2006).

Faced with the choice of limited faculty resources, many department heads replace retiring power engineering faculty with faculty working in "hot" technology areas with strong industry funding. Often these industries provide endowed professorships and chairs to support faculty positions, which guarantees the retention of faculty in these technical areas. By contrast, there are few endowed professorships and virtually no fully endowed chairs designated in electric power engineering in universities in the United States.

The widespread perception that the utility industry does not offer career opportunities that are as exciting as other industries is increasingly untrue. Technology advances are altering the nature of the technologies being deployed in the industry. Going forward, the electric power industry will need increasingly more eclectic workers with skills to address digitization and the complexity of electronics, communications, computers, and highly integrated systems; the integration and operation of renewable energy sources; the operation of sophisticated chemical processes for providing clean coal and for controlling other pollutants and carbon dioxide; and perhaps a new generation of nuclear power. Much of this modernization will be driven by consumers' increasing demands for near-perfect reliability and quality of supply at a reasonable cost and by ever tighter environmental constraints.

As the workforce population declines through retirement, attrition, and down-sizing, a precipitous loss in institutional knowledge is occurring. This knowledge is often not documented, and frequently it is known only to a very few people. As today's employees leave the workforce, this knowledge leaves with them. EPRI and others have worked to develop tools to capture this knowledge before it is lost.

New advanced training and worker support tools may help to provide tomorrow's employees with the knowledge and skills they will need. For example, multimedia and virtual reality tools may help with training workers in critical areas and in high-hazard tasks such as live-line work. The National Aeronautics and Space Administration is already using virtual reality tools in place of replica training simulators for team building and training with members in distributed locations. Improved haptics (the science of the sense of touch) is the most obvious requirement both in virtual reality and in multimedia in general, and there is a significant amount of research and development being done in this area.

Over the last 15 years, the response of the utility industry to a shrinking and overstressed workforce has been to turn increasingly to consultants and to outsourced engineering and information and communication technology service providers. This system is not sustainable. Many of the employees of consulting and engineering service companies are older and are therefore not a solution to the manpower needs 10 years hence. Furthermore, the majority of the experienced employees of these firms were trained in the electric utility industry as utility employees before joining service providers. The electric utility industry is no longer a training ground for skilled engineers and will not provide the increasing number of employees needed by service providers.

The conundrum is obvious. As engineers and other skilled workers retire, electric utility companies either will need ever more external support from consultants and engineering and information and communication technology service providers, or they will need to mount major new initiatives to recruit, train, and retain new workers in a competitive environment in which other power companies (and other industries) will be working vigorously to hire the same well-trained men and women.

All of this raises significant security concerns. As new employees charged with a range of responsibilities replace older workers with deep, specialized knowledge, the risk grows that people will make mistakes that compromise

security, or that exacerbate the consequences of attacks on the system. Clearly, regaining some of the workforce stability that characterized this industry in years past, while also adding to the technical depth and knowledge of the future workforce, will be an essential part of reducing the risks that terrorism poses to the electric power delivery system.

A partial solution to the workforce issue that is relevant to DHS and other federal agencies, at least in the short term, concerns the severe H1-B visa limits, currently 65,000 per year—with high competition from many industries. Electric power in the United States has greatly benefited for over 100 years from the talents of tens of thousands of immigrant engineers, including those from industry giants such as Tesla and Steinmetz. A very high proportion of U.S. graduate students in electric power today are not U.S. citizens, but many would choose to work in the U.S. power industry following graduation if allowed. Assuming that appropriate and timely background security checks can be conducted for immigrant students and others with the necessary skills, they could provide needed talent and expertise in both academic and industrial environments. Obviously, adequate numbers of student visas are also required.

WORKFORCE VULNERABILITY TO PANDEMICS

Recently, the threat of a pandemic has become an area of much concern because of both the threat to life and the disruption of the services provided by those afflicted. The threat presents unique implications, and it exposes many points of vulnerability across the electric power system infrastructure. Should a pandemic occur—whether naturally or by malicious action—it will touch every part of the electric system in ways few have considered. Recognizing the potential societal and economic impact of a pandemic, the U.S. government and the North American Electric Reliability Council (NERC) have issued advisories to the electric industry on the need for preparedness plans.

Many businesses today have implemented business continuity and emergency preparedness plans. Those plans that address high absentee levels are an important tool to ensure that critical business activities are sustainable in the event of various possible extreme situations, including health emergencies. This is particularly relevant to an industry that has relied on mutual assistance agreements in responding to catastrophic events.

Since 2003, of the 270 people known to be infected with avian flu, 164 have died (WHO, 2007). To date, 10 countries across three continents have reported confirmed human cases of avian flu. As a result, avian flu is now being described by health officials as a possible pandemic. The late Lee Jong-wook, former director-general of the World Health Organization (WHO) noted, "It is only a matter of time before an avian flu virus . . . acquires the ability to be transmitted from human to human, sparking the outbreak of human pandemic influenza. We don't know when this will happen. But we do know that it will happen" (Knox, 2005). As with other catastrophic events (e.g., hurricanes, earthquakes, flooding), that the risk exists is known; however, the full impact is difficult to predict. Unlike the effects of other catastrophic events, the damage caused by a pandemic will not, by definition, be limited to a single geographic region. A pandemic can affect businesses nationally and internationally, with a primary impact on both staff and the public at large. Yet as a business continuity risk, the prospect of a pandemic can best be approached by organizations acting on a regional basis.

When a pandemic does occur, it has both social and economic impacts. The private sector and government must be prepared to manage both. The social impacts directly relate to the health and well-being of employees, customers, and business partners. Understanding how to manage the social impacts of this threat is critical and should be the focus of planning for a pandemic. A pandemic can also have major financial consequences as a result of disruption of operations or loss of key vendors or suppliers. These can directly affect an organization's ability to recover from the event and resume normal operations. Understanding and managing both aspects of the business impact is a prerequisite to effectively and efficiently dealing with the threat of a pandemic.

In the event of a pandemic, the electric power industry, unlike some organizations, cannot completely shut down if a high percentage of the workforce is absent. Essential services such as health care, water and sewer systems, as well as basic economic activity depend on electricity to operate. Thus it is essential that the electric industry continue to develop and refine plans to address the business and human capital risks associated with a pandemic. These plans will help to ensure business continuity in the event of a pandemic and can be a natural extension to existing business continuity plans.

It should be recognized that no organization has unlimited resources to tackle a pandemic scenario. The only rational way to prepare for a pandemic is to focus on those operations that are mission critical and people-dependent. Such plans should create a leadership succession process, cross-train people to perform multiple critical business functions, include a crisis health and sanitation plan, provide for advance employee training, and include a communication and information dissemination plan.

CONCLUSIONS

- Robust background screening programs for all personnel need to be uniformly implemented across the electric power industry. These programs not only should apply to new employees but also should include members of the existing workforce who are staffing critical operational positions and to all contractors and others with direct or indirect access to such facilities.
- Pre-event training programs need to be developed to ensure that utility workers, as first responders, are

adequately trained to respond to a terrorist event. Training should include instruction on how to detect and operate within an area that has been contaminated by radioactive, chemical, or biological agents. The training at the engineering workforce level should also include aspects of organizational theory, risk communication, and risk perception. It should also recognize the high likelihood that such areas will be classified as a crime scene. It is important to note that such training is specifically intended to expose utility workers to probable scenarios that are a consequence of malicious attacks, and it should be clearly separated from the training utility workers receive for day-to-day system operation and maintenance.

- The electric power industry faces serious and growing security and other challenges as a result of more rapid churning of employees in utilities and among contactors. This change is resulting from workforce aging, the attrition of skilled workers, the loss of core competencies and institutional knowledge, and competition for the declining supply of electrical engineers and other skilled professionals. A detailed analysis of workforce issues in the U.S. electric power industry, including a careful examination of associated security issues, is needed and should be a priority activity for organizations representing the industry. Appropriate organizations in the public and private sector (e.g., the Edison Electric Institute CEO Committee) must engage utilities at an executive level to create and implement a set of systematic solutions to these problems.
- Mid-term and long-term solutions to the shortage of an educated power engineering workforce are dependent on the health of electric power engineering programs in universities—programs that, in many cases, have been eliminated or undergone major contraction. The utility industry must find a systemic, coordinated solution for the support of those universities that have maintained power engineering faculty and are capable of expanding power curricula and increasing student numbers over the near term. While direct student support is important in the form of scholarships and graduate fellowships, endowed chairs and professorships are needed to secure power faculty positions in electrical engineering departments. The key to the success of power engineering programs is a significant increase in direct research support for faculty and students. Increased research funding must be targeted to universities in order to provide incentives to deans and department heads who must decide which technical areas will be emphasized and where new faculty will be hired. To date, no industry organization has provided adequate leadership and "ownership" of the crisis facing power engineering education in universities.
- All utility service providers should develop business continuity plans that ensure that power can continue to be reliably supplied in the face of a pandemic. Such plans should create a leadership succession process, cross-train people to perform multiple critical business functions, include a crisis health and sanitation plan, provide for advance employee training, and include an internal and an external communication and information dissemination plan.

REFERENCES

Ashworth, M.J. 2006. *Workforce Aging in the U.S. Electric Power Industry*. Briefing to the workshop on the same topic, Carnegie Mellon Electricity Industry Center, Pittsburgh, Pa., April 17.

Christie, R.D. and P.M. Mahadev. 1994. "Case Study: Visualization of an Electric Power Transmission System." IEEE Proceedings of the Conference on Visualization '94.

EPRI (Electric Power Research Institute). 2000. *Power Delivery Reliability Initiative: Phase One Summary Report.* EPRI Report 1000200. Palo Alto, Calif.: EPRI, December.

Knox, N. 2005. "'Matter of Time Before Bird Flu Pandemic Strikes,' WHO says." *USA Today*, November 8.

Overbye, T.J., and J.D. Weber. 2001. "Visualizing the Electric Grid." *IEEE Spectrum* 38(2): 52–58.

Reder, W.K. 2006. "The Technical Talent Challenge (and Implications of Our Maturing Workforce)." *IEEE Power and Energy Magazine* 4(1): 32–39.

Venkata, S. 2004. "Human Resource Needs in Electric Energy/Power Engineering." Presentation. Clarkson University, Albany, N.Y., May 17.

WHO (World Health Organization). 2007. "Cumulative Number of Confirmed Human Cases of Avian Influenza A/(H5N1) Reported to WHO, 29 January 2007." Available at http://www.who.int/csr/disease/avian_influenza/country/cases_table_2007_01_29/en/index.html. Accessed January 2007.

6

Mitigating the Impact of Attacks on the Power System

Power systems are routinely designed and built to resist a variety of natural disruptions and continue to operate (NERC, 2006a,b). For example, they can often withstand, or rapidly recover from, events such as lightning strikes, wind and ice storms, fires, and various equipment malfunctions. Some of the features that have been designed into systems to enable them to withstand such "normal" events also offer protection against attacks of modest scale by terrorists. As the sophistication of various technologies grows, the evolving electric power system can be guided toward an even more resilient configuration.[1]

Simply adding generation and transmission capacity does not always make the system more robust. Furthermore, unless carefully planned, such additions can sometimes cause added congestion and decreased reliability in other parts of the system (Blumsack, 2006; Clark, 2004).

As described in Chapters 1 and 2, the nation's electrical grid is highly stressed due to the growth in new generation and load without a concomitant increase in transmission capacity. An intelligently planned and well-coordinated terrorist attack could result in local or regional outages of significant duration and disrupt activities for a large segment of the population. The catastrophic failure caused by the 2005 hurricanes Katrina and Rita in several southern states resulted in widespread damage to system components, and it took several months to restore certain portions of the system.

If terrorist attacks targeted large critical components such as high-voltage transformers, for which spare parts are limited, restoration to pre-event levels of operation could take much longer (see Chapters 3 and 8). This chapter explores ways in which the electric system can be made resilient in the face of some attacks, and how any failures that do occur can be minimized. The reader also is referred to Chapter 3 for a discussion of physically protecting key facilities and Chapter 4 for cyber protection. Much of this chapter is necessarily technical, but the findings and recommendations at the end are intended to be understood without reading the entire chapter.

The chapter covers several technical topics:

1. Planning and operational design of the system to withstand simultaneous multiple outages;
2. Monitoring and protection systems, which play a critical role in mitigating the impact of an attack on the system;
3. Mechanisms to enhance the "graceful degradation" of the system in the event of an actual action or disturbance; and
4. Measures to increase the robustness and resilience of the distribution system[2] through networked distribution system architecture and other means such as distributed generation.

Together, these types of system design and operational approaches can help to mitigate the effects of an attack, and may in fact make it less attractive to attack the electric system.

BULK POWER SYSTEM ENGINEERING

Interconnected bulk power systems[3] are planned and operated in accordance with reliability criteria designed to ensure survivability following a range of plausible disturbances. The criteria are currently developed by NERC (as ERO) and regional reliability council processes (NERC, 2006a). Until recently, they have been voluntary but are

[1]For example, new technologies for diagnosis and control of disruptions and the widespread use of distributed generation could considerably strengthen the ability of the system to continue to provide service to most customers in the face of even fairly large-scale attacks (Benner and Russell, 2004).

[2]In the United States, distribution voltage is typically 4–34.5 kV.

[3]The term "bulk power system" generally applies to large central generation stations and those portions of the transmission system operated at voltages of 100 kV or higher.

becoming mandatory as a consequence of energy legislation enacted in 2005.

A key feature of the FERC-approved reliability standards is a performance table showing planning and operating criteria for normal operations (Category A) and three categories of disturbances.[4] For single or multiple outages, the following apply:

5. *Category B, events such as a short circuit causing loss of a single element or component in the system* (i.e., an *N*–1 event with outage of a single generator, transmission line, or transformer).[5] The power system must remain stable (no cascading) and within thermal and voltage limits. Loss of load or curtailment of firm transfer (i.e., sales of energy that have been agreed upon by contracts) is not allowed. For operations, the system must be readjusted within 30 minutes to withstand another outage.
6. *Category C, certain related (non-independent) events causing outages of multiple elements.* An outage of two circuits of a multiple circuit is one example. Similar performance to Category B is required except that planned/controlled load shedding and/or firm transfer curtailment are allowed. Cascading must be prevented.
7. *Category D, extreme events resulting in multiple elements removed or cascading out of service.* Selected events may be evaluated for risks and consequences.

To date, NERC standards have given little consideration to scenarios in which multiple facilities are destroyed by terrorists. In the future it may be prudent to design and operate bulk power systems to withstand multiple outages (Category D) that have some likelihood or history of occurring, or that are vulnerable to well-thought-out terrorist attacks. Such a standard would likely be expensive to implement and might reduce transfer capacity until additional facilities are added, but some movement in this direction is probably warranted.[6]

For Category D events, controls may be applied to prevent or mitigate cascading and massive loss of load. These are sometimes termed *safety nets*. For example, underfrequency load shedding is universally applied for controlled or uncontrolled separations (islanding). Undervoltage load shedding may be applied in areas where voltage collapse is a concern. These and other automatic controls attempt to restore equilibrium conditions within the electric power system or portions thereof. Loss of components due to malicious attacks would also cause imbalances and, if necessary, such controls would also be activated to mitigate the detrimental effects.

According to the NERC performance table, actions such as reduced power transfers and canceling of planned outages (e.g., for maintenance) may occur during abnormal conditions such as storms or forest fires. Similar actions should be taken during elevated terrorist threats resulting in a DHS red alert status.

The U.S.-Canadian power system currently consists of four large regions (see Chapter 2) within which all connected generators operate synchronously. Asynchronous connections between the regions are accomplished with DC tie lines or back-to-back AC-DC-AC converters (asynchronous links). Large synchronous regions evolved for economic power transfers and for the mutual support inherent with AC transmission.[7] Under some operating conditions, however, large synchronous interconnections are vulnerable to large cascading failures when certain faults occur.[8] (For examples, see Table 1.1.) Upgrades of AC transmission capability to improve the strength of the existing interconnections, the selective addition of advanced controls, and power electronics-based equipment, and other solutions such as prioritized modernization of power plant and substation equipment, including emergency control and protection are urgently needed.[9]

Substation Design and Modernization

A critical component of the bulk power system is the design and layout of transmission substations and switchyards. Substations are designed for reliability, flexibility of operation (including access), and cost. Substations provide the ability to safely switch equipment out of service during either scheduled or unscheduled outages while maintaining service. Several substation configurations have evolved to

[4]See Table 1 at ftp://www.nerc.com/pub/sys/all_updl/standards/rs/TPL-001-0.pdf.

[5]Simulations for *N*–1 planning/operating criteria often involve a rarely occurring three-phase fault at a critical location with outage of a key line or transformer during peak load or transfer. The three-phase fault "umbrella" events are more severe than many multiple outages, especially those occurring during less stressed (off peak) operating conditions.

[6]Recall also that an *N*–2 event is defined as one in which the system would continue to operate reliably without two elements. Note, however, that there is no requirement for the frequent *N*–2 event of a short circuit with line outage, and with simultaneous outage of a parallel line or line with common termination because of a protective relay mis-operation. Storms, fires, airplanes, and terrorists may also cause loss of parallel lines on the same right-of-way. However, moving to N–*n* reliability standards in which *n* is larger than 2 should only be undertaken after a careful quantitative probabilistic assessment of costs and benefits.

[7]For example, for an outage in one line, power automatically shifts to other parallel lines in a fraction of a second. With DC links, special controls are needed.

[8]One theoretically possible approach to containing the extent of such outages would be to reduce the size of synchronous regions. For example, the large Eastern and Western interconnections could be restructured into regions similar in size to the Quebec and the Texas interconnections. This would require breaking up these two large interconnections into smaller ones connected by asynchronous links. Such a change would prevent the propagation of disturbances across very large areas. However, this approach would have serious limitations. It would undermine the kind of automatic support now provided by a large interconnected AC grid when large loads or generators are tripped. Further, asynchronous links are expensive.

[9]Such control equipment may include selective conversion to asynchronous links, such as a link proposed between Ontario and Michigan that might have reduced the extent of the August 14, 2003, blackout.

achieve reliability and flexibility. The configurations consist of different bus and circuit breaker schemes which, when switched, provide alternate network paths.[10] The bus configurations could have a significant impact on maintaining reliability in the event of a malicious attack on the power system, especially if a transformer, circuit breaker, instrument transformer, or bus work fails violently. For example, a buswork or circuit breaker failure can cause complete substation outage with one bus configuration, but no loss of connectivity with another. Appendix F compares four common bus configurations and indicates their relative advantages and disadvantages. Older, usually lower-voltage, configurations and protection schemes tend to be less reliable.[11]

Whether it is caused by a terrorist attack or some natural cause, once a transmission or substation short circuit has occurred, circuit breakers must interrupt tens of thousands of amperes to isolate the faulty equipment and protect equipment that is not yet damaged. If the circuit breaker fails, additional breakers may be required to open, and, depending on bus configuration, may cause outage of multiple additional lines and transformers. Furthermore, a circuit breaker failure may be explosive, damaging nearby equipment and causing a fire. Breaker failure protective relaying is often nonredundant or may not be installed, potentially resulting in even larger disruption and possible cascading blackout. Breaker failures have initiated large-scale power interruptions.

Modern circuit breaker technologies are available to replace underrated or unreliable breakers.[12] Prioritization of breaker replacements is relatively straightforward, and, as budgets permit, power companies replace underrated breakers. Prioritization is based on breaker type and reliability, interrupting rating relative to short circuit currents, bus configuration, and the potential system impact of a failure. Difficulties with cost recovery must be overcome in order for such modernization to occur.

For major new transmission line construction, it may be preferable to construct new substations rather than enlarging existing substations to a size that jeopardizes reliability if those substations completely shut down. Likewise, bypassing substations in a hopscotch fashion along a multi-line transmission path reduces the effect of a complete substation shutdown, and reduces choke points.

Power System Protective Relaying

The electric power system consists of expensive generators, apparatus, and lines that can quickly be damaged or destroyed as a result of short circuits (faults), thermal overload, or other abnormal conditions. Protection systems are designed to automatically detect and isolate lines and apparatus following electrical faults or disturbances in order to protect equipment from damage due to voltage, current, or frequency excursions outside the design limits. Primary protection devices include relays, reclosers, fuses, circuit breakers, and switches. In response to short circuits, protective relays detect abnormal electrical signals and open circuit breakers to isolate faulty equipment.[13]

Protection systems are critical to ensuring safe and reliable operation of interconnected transmission networks and should have the characteristics shown in Figure 6.1. A protection system must be dependable and secure in all its operations. Dependability means that protection devices properly respond when changes in electrical conditions indicate an abnormal or dangerous condition. Security means that protection systems will not mis-operate under normal conditions or for conditions outside the operational design of the protection system. Usually an increase in system dependability means a decrease in security or vice versa. For example, protection system dependability can be enhanced by incorporating device redundancy. Increased redundancy through the use of multiple relays to monitor a transmission line for abnormal conditions improves the probability that an event will be detected and thus improves reliability. However, multiple relays acting in parallel can also decrease security through greater complexity and greater exposure to component failure and mis-operation. Consequently, reliability requires a fine balance between dependable operation and security against inappropriate operations.

Many design issues and approaches can affect the characteristics of protection and control systems, including the following:

[10]Most switchyards and substations have open-air bus work. At *much* higher cost, bus work may be placed in pipes insulated with SF6, rather than open air. Switchgear is incorporated in the gas-insulated equipment. The substation is then much more compact and can be installed indoors or underground. Gas-insulated substations are commonly used in urban areas, particularly in Europe and Japan, where land prices are high. Obviously, stations that are indoor or underground can be more secure against attacks.

[11]As an example, a bus fault at an old 400-kV substation led to a massive cascading power system blackout in Brazil on March 11, 1999. Lack of local bus protection and an unnecessary zone 3 relay operation at another station contributed to the failure. Following the blackout, potential system improvements were prioritized considering risk to the system, cost, and other factors. Many of the changes involved relatively low cost substation configuration improvements, and protection modernization.

[12]A recent Fitch report states that 60 percent of circuit breakers in the bulk power system are now more than 30 years old (Anderson et al., 2006). Many may be underrated or marginally rated for present day short-circuit currents. Modern circuit breakers are technically superior and much more reliable, and are available at about the same cost as old circuit breakers, despite general inflation.

[13]In the August 14, 2003, blackout event, lines sagging into trees caused a short-circuit current that was detected by relays and cleared by proper operation of breakers. The transmission line remained undamaged and capable of being placed into service. In other words, the protection devices correctly operated in response to faults caused by external factors (i.e., contact with trees). However, in that case, successive loss of multiple lines due to short-circuit or overload conditions resulted in instability and successive protection system operations that ultimately gave rise to a cascading failure and a blackout.

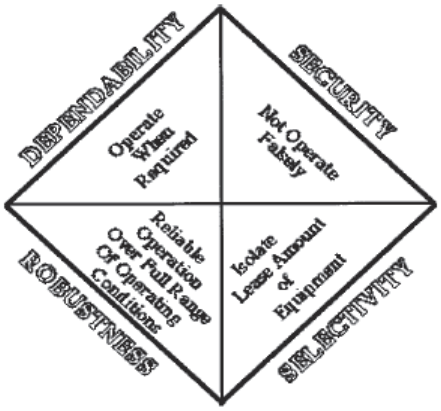


FIGURE 6.1 Protection and control system characteristics.

- *Speed at which protection systems operate.* A rapid decision to trip a breaker may prevent instability and permanent damage to lines or apparatus under fault conditions. However, disturbances and system dynamics may create electrical signals that emulate fault or overload conditions that can only be distinguished with sufficient analysis time. Consequently, a quick decision to trip may be required under certain conditions, but also may result in an improper decision under different dynamic conditions.
- *Testing and maintenance practices.* These can result in improper protection settings or inadvertent changes in protection logic. These have also caused large-scale blackouts. For example, even a cursory analysis of the August 2003 blackout shows several areas of concern with respect to protection system design, as integrated with system operations and communications. The loss of the first transmission line was caused by the correct operation of relays to clear a fault caused by the line sagging into trees. This resulted in heavier loading of parallel lines with the effect of subsequent loss of multiple lines due to faults and overload conditions. The lines associated with these events were properly protected and preserved and could have immediately been placed back in operation had operators had adequate knowledge and awareness of the dynamic events that were occurring.
- *Systems to enhance awareness of operating conditions.* New digital relays with advanced communications and information sharing capability coupled to control and information systems can decrease the probability of cascading failures as a consequence of multiple protection system operations.
- *Proper settings of relays.* Improper settings have resulted in cascading blackouts caused by the tripping of transmission lines under nonfault conditions. An improper setting of a "zone 3" impedance (distance) relay was a proximate cause of the November 9, 1965, Northeast blackout. The relay performed correctly based on its setting, but it had not been reset as system load grew. High load but nonfault electrical conditions caused the relay to operate. Emphasis should be given to remote monitoring of protective relay settings and improving maintenance and test procedures that mitigate the possibility of improper and insecure operation of relays.
- *Addressing the "overreach" of protection systems.* Overreaching distance protection, mainly in the form of zone 3 relays, has caused or contributed to many blackouts. Overreaching protection is generally applied as backup protection in the case of breaker failure in a distant substation. In other words, if a local protection system fails to detect a fault, surrounding substations "overreach" to detect the fault and eliminate fault current in-feeds to the local substation. Sensitive settings are required, and so the relays are prone to operate on nonfault conditions of overload, depressed voltage, or electromechanical swings among generators. There are several solutions to this problem, including redundant local relays, breaker failure relays, bus protection, and restrictions on the reach of impedance relays. NERC and the industry have addressed the backup relay problem in response to the 2003 blackout. Thousands of changes were made by North American power companies. (Reports are available at www.nerc.com.) Eternal vigilance, however, is required to ensure that relays respond only to short circuits.

The above approaches do not address all of the protection issues that can cause or exacerbate a cascading blackout. With millions of protective relays and protection schemes in place, undesirable or unnecessary operations cannot be prevented. However, fruitful areas of investigation and improvement include the following:

- *Improvement in intelligent, digital relays allowing for self-evaluation and remote evaluation* of settings and relay health to ensure reliable operation.
- *Integration of protection systems with other control and operation systems* to ensure that operators have full operational awareness as conditions change and deteriorate during a cascading event.
- *Improved control philosophies and strategies for multiple contingency events occurring in close time proximity.* Such improvements could address situations in which the proper operations of relays in response to changing conditions, when taken as a whole, can create unrecoverable instability in the power system.
- *Methods to prioritize modernization of protection relays and schemes,* including communications such as by fiber optics between stations.

Sensors

As noted in Chapter 4, supervisory control and data acquisition (SCADA) provides two-way communication and control capability for control centers, power plants, and substations. Every few seconds, control centers receive massive amounts of data, most of it reflecting electrical conditions across the grid. However, determining what it all means, and what exactly happened following a natural event or a terrorist attack, may be difficult.

There are various sensor-related strategies to improve the situation. One, for example, is to increase the amount of data by using and analyzing data from a large number of distributed sensors.[14] These enable detection of potential intrusions and sabotage, and postmortem studies after failures. Although it is very difficult to avoid or predict terrorist acts, quick assessment of the situation can help operators take actions in order to avoid cascading events and the consequent partial or total blackouts.

The mechanical failures resulting from malicious attacks on a transmission line are similar to extreme natural events affecting a transmission line. Thus, work done in the latter area can also help to guide preventive and corrective action for acts of sabotage. A basic method to assess damage caused by any physical event on the transmission grid is visual inspection, but this is difficult for transmission lines dispersed over hundreds of kilometers.[15]

Various techniques can address this issue. For example, digital distance relays can report approximate fault location based on the impedance calculation for a fault. Transmission fault locator devices based on traveling wave propagation or other methods can more precisely determine fault location. Real-time determination of the fault location (e.g., as a percentage of line length), and then communication of this information to the control rooms and reliability coordinators, allows the operators to take appropriate control actions, and if terrorism is suspected to quickly alert law enforcement about the exact location of the problem. The mapping of the fault location as a percentage of line length to a particular geographic location is usually straightforward, provided that global information system models of the line are available. Single-phase switching or three-phase automatic reclosing attempts provide information on the type of fault and whether it is transient (e.g., lightning caused) or permanent. In situations where information is limited, operators in control centers may attempt manual (SCADA) line reclosure to determine if the fault is permanent. For permanent faults, crews are dispatched, possibly including aircraft for visual inspection.

Monitoring the structural integrity of transmission lines is helpful in assessing the effects of mechanical events. Equipped with adequate cryptographic and security features, wireless sensors for collecting structural information can provide a seamless sensing environment thanks to their main characteristics: ease of installation and replacement, low cost, networking, and small size.

Innovative technologies should be employed for detection of failures in power systems before they become catastrophes. Novel approaches that involve the implementation of a sensor network design for the national electric energy infrastructure combined with the use of nonconventional mechanical sensors may significantly improve the robustness of power systems against catastrophic failures. This would include wireless sensor network technology for detection of mechanical failures in transmission lines, such as conductor failure, tower collapses, hot spots, extreme mechanical conditions, and so on. It also involves the installation of mechanical sensors in predetermined towers of a transmission line, communicating via a wireless network. Sensors include accelerometers, tension/strain gauges, and tilt and temperature sensors. The main goal is to obtain a complete physical and electrical picture of the power system in real time and determine appropriate control measures that could be automatically taken and/or suggested to the system operators.

A variety of nontraditional sensors should also be considered and evaluated. These include sensors for mechanical motion; sound; visual spectrum (e.g., closed-circuit television and automatic processing of closed-circuit television signals); infrared; chemical, gas, ozone, nitrate, CO, and CO_2 sensors; electromagnetic radiation, Poynting vector (based on electric and magnetic fields), partial discharge detectors; biological sensors; conduit continuity/resistance; incipient fault detection; and vibration. Also, the use of unmanned aerial vehicles (UAVs) could be considered. Sensor additions will require new software to process (filter and prioritize) the data for presentation to operators who may already be overwhelmed with data and alarms following events.

Automatic Controls for Power Systems

While there has been much discussion regarding the actions of operators, particularly after the August 14, 2003, failure, terrorist attacks and other disturbances can evolve into instability in a few seconds or tens of seconds, in many cases too fast for operators to determine what is happening and take appropriate corrective actions. During certain relatively familiar events in which alarms become activated, operators may act within a few minutes. In new situations, 15 to 30 minutes may be required for assessment and operator

[14]These might include nonconventional sensors and innovative instrumentation located in the power system by some prioritized strategy. Metrics include system observability, power usage, enhancement of communication capabilities, and size of data for operations and enhanced operational decision making.

[15]Problems occurring in concentrated environments (substations or generating plants) are not difficult to find and assess with a small crew, or through video surveillance. Recent blackouts in the United States and Italy have shown that failure to assess and understand the condition of the power system, and the delay in taking appropriate corrective actions after just a single outage, can lead to blackouts across large areas.

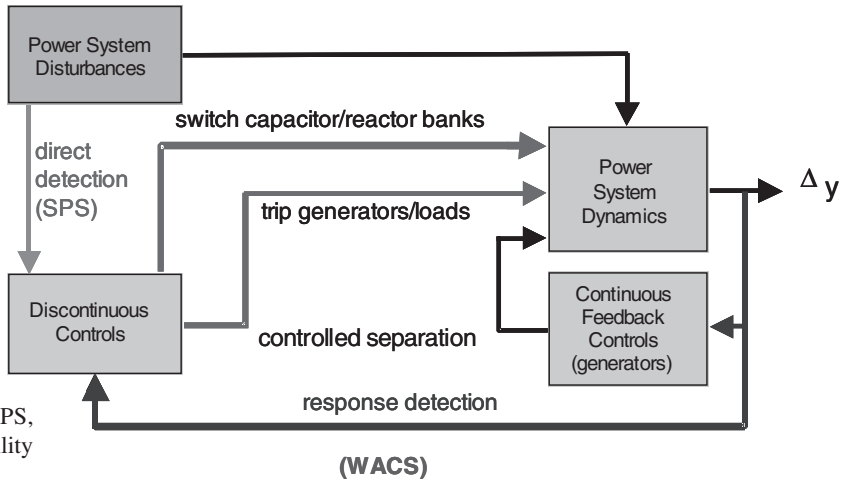


FIGURE 6.2 Power system stability controls. SPS, special protection systems; WACS, wide-area stability and voltage control system.

actions, especially if load shedding is required. Thus, various types of automatic controls are required.

The following are some of the examples of automatic controls the committee has identified:

- Techniques for shedding load and generation to enhance power system dynamic response capabilities, including simple and low-cost approaches to avoiding voltage collapse;
- Techniques for maintaining proper transmission network voltage profiles;
- Primary automatic controls to prevent cascading instability that are located mainly at power plants;
- Transmission-level power electronic devices and mechanical devices;
- Local load-shedding practices and techniques;
- A class of controls termed special protection systems (SPSs) or remedial action schemes;
- Wide-area feedback/response-based controls, either continuous or discontinuous; and
- Sophisticated control algorithms (using various techniques such as adaptive or "intelligent" control) as part of digital control and communication capabilities.

Appendix G provides further descriptive details concerning each of these types of controls. Figure 6.2 illustrates a possible configuration of power system stability controls. The special protection systems path is feedforward. The continuous feedback controls are normally local and mainly at generation facilities, but could be wide area. The feedback (response-based) discontinuous controls are often wide area, but could be local (e.g., underfrequency or undervoltage load shedding).

In summary, power system robustness, resilience, and survivability in the face of major disturbances, including modest terrorist attacks, can be increased significantly and economically through the use of automatic controls. What is required is implementation of industry best practices, prioritized upgrading of old analog controls, and development and implementation of wide-area controls.

POWER SYSTEM OPERATIONS AND ENERGY MANAGEMENT SYSTEMS

In North America, the bulk power system is monitored and managed at energy control centers, also called SCADA-EMSs or simply energy management systems (EMSs). Data acquisition and remote control are performed by computer systems called SCADA systems. Figure 6.3 shows a schematic of a modern EMS. Note that a SCADA system communicates with generating plants, substations, and other remote devices.

Because of the historical evolution of the electric utilities in the different geographic regions, these EMSs are functionally similar but not identical. All these different EMSs result in significant additional complexity. Of the four synchronous interconnections in North America, the Quebec and Texas interconnections each constitute a "balancing area"—an organizational jurisdiction responsible for balancing its load and generation and each requiring its own EMS with automatic generation control. By contrast, the two other interconnections (the Western and Eastern) are too large to have only one balancing area each and, instead, have dozens of them.[16] With so many EMSs in these two interconnections, it is difficult to monitor all that is happening in a large interconnection, and so reliability coordinators or independent system operators that coordinate large portions of the interconnection have been set up and sometimes have

[16]The Eastern Interconnection has about 100 and the Western about 40, with the numbers fluctuating over time as organizational jurisdictions change. Note that some balancing areas in these two interconnections are so large that the EMS is hierarchical, with some of the functions distributed over several control centers.

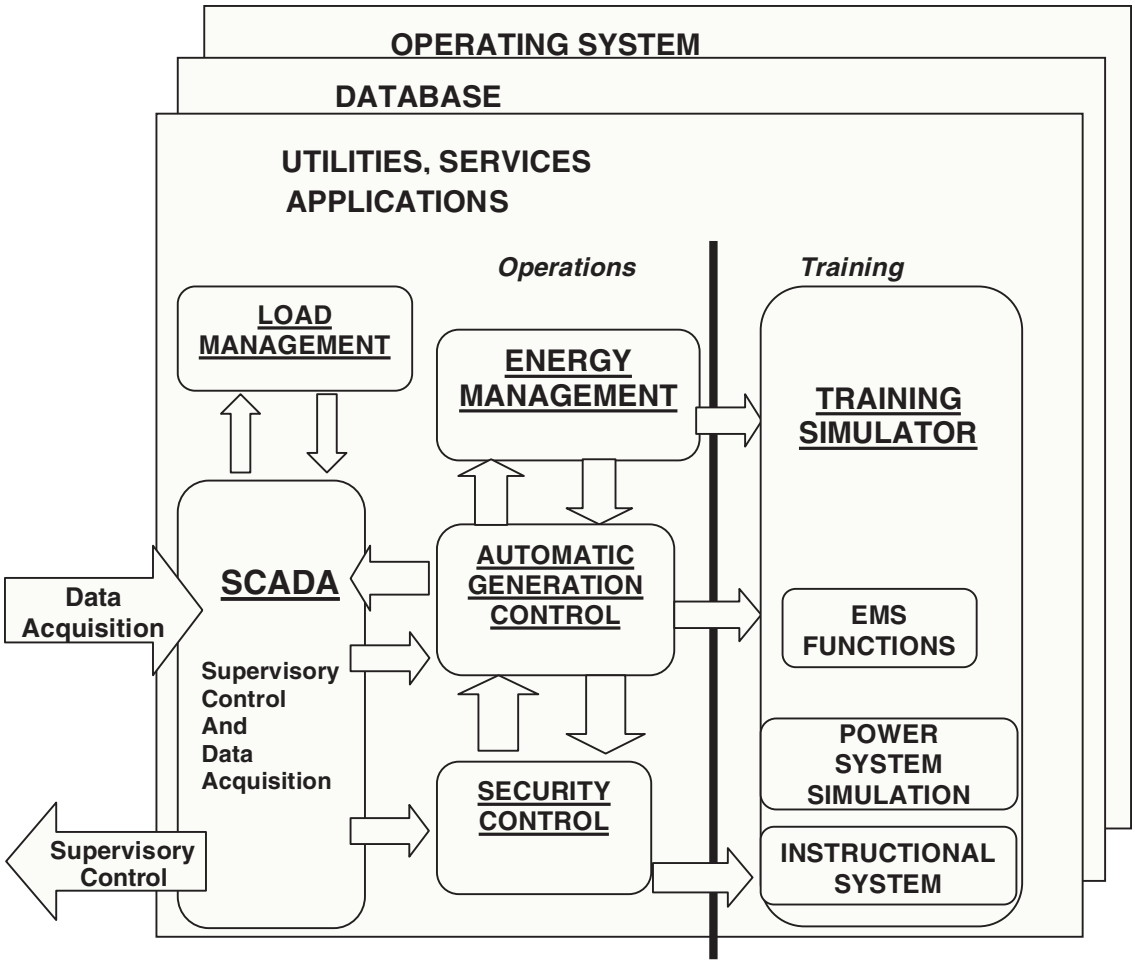


FIGURE 6.3 Modern emergency management system.

footprints covering many balancing areas. Figure 6.4 shows the balancing authorities in North America. Figure 2.1 in Chapter 2 shows the four interconnections.

Thus, the control center EMSs that represent the balancing areas have the most control of the grid, but each can control only a small portion of the Western or the Eastern Interconnection. The reliability coordinators have a wider view of the grid but no coordinator covers the whole Western or Eastern Interconnection, and coordinators do not always have direct control of their portion of the grid. No single entity has the full real-time view of either the Western or the Eastern Interconnections, but some balancing authorities and reliability coordinators do exchange real-time data with their neighbors to increase their situational awareness beyond their own borders. More such data exchange will be needed and even a central monitoring center for these large interconnections has been suggested in the 2005 EPAct and elaborated further by USDOE and FERC (DOE/FERC, 2006).

Because the balancing area control centers have the ability to switch breakers and control other parameters, these could be main targets for cyber attacks.[17] Historically, the communication systems between these EMSs and remote terminal units (RTUs), and between EMSs, have been dedicated redundant channels and are not paths for intrusion. However, connections between the EMSs and other information systems have increased in recent years, and such connections need to be secured and made trustworthy.

Although some automatic controls, like automatic generation control, are part of an EMS, the main function of the EMS is to allow the operator to monitor the present condition of the system (including alarming and analysis of the present conditions) and to take manual control actions as necessary to reliably operate the grid. Because the final cascading, like that in the 2003 Northeast blackout, can happen too fast for the operator to intervene, it is important for the operator (with the help of the EMS software) to recognize developing patterns that endanger the system. An operator in an EMS can observe the electrical performance of the system and take appropriate actions. However, neither the operator nor the

[17]Cyber security is discussed in more detail in Chapter 4.

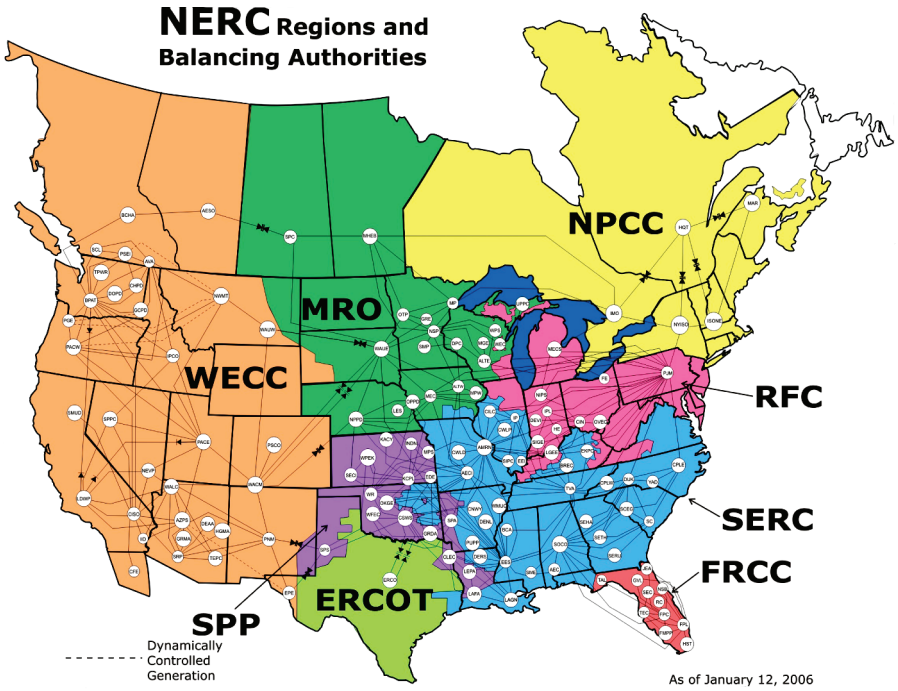


FIGURE 6.4 Balancing areas (also called control areas). For definitions of acronyms, see Appendix D. SOURCE: NERC. Available at http://www.nerc.com/regional/NERC_Regions_BA.jpg. Accessed October 2007.

automated control system can distinguish between a physical disruption in the system and an electrical disturbances (e.g., if the base of a transmission tower is bombed and the line goes down causing a contact with the ground, the circuit breakers will operate to isolate the transmission line from the rest of the system). For an operator in the control center, the primary indication is that the circuit breakers operated to open and isolate the transmission line. The operator, however, cannot distinguish whether this is a temporary situation or a permanent one. If this information was available, then the operator in all probability would make decisions to maneuver the system to a more secure state. The ability to provide this additional information is the primary focus of the steps needed to protect, mitigate, and enhance graceful degradation. In order to facilitate these steps, various initiatives would be needed to harden the system against malicious disruptions. These steps are outlined and discussed below.

Especially after the 2003 U.S.-Canada blackout, the "situational awareness" of the operator has emerged as a major concern. Operators at the EMS where the power system conditions were deteriorating were not aware of these conditions. Although trending and alarming for limit violations and abnormal conditions of individual measurements are commonplace in control centers, the recognition that abnormal patterns are developing (e.g., the depression of voltage over a large region as opposed to voltage limit violations at individual buses) is dependent on the experience and alertness of the operator. Automatic capture of such disturbing trends by the EMS computers would be an enormous help to alarm the operator. Such alarm processing using advanced methods of pattern recognition is needed.[18] It also would be valuable to coordinate, in real-time, the display of line outage information across reliability coordinator boundaries. If a group of terrorists were to strike a number of electrical targets distributed across a large geographic region, the sooner the malicious nature of the event was uncovered, the quickly protective actions could be taken. Currently there is only limited sharing of real-time information across reliability coordinator boundaries (Figure 6.5), with no one seeing the big picture for a grid such as the Eastern Interconnection. Hence, there would likely be a delay in determining that the near simultaneous loss of multiple lines in multiple regions was likely due to malicious activity.

Just as redundancies are needed in the design of the power grid to increase its reliability and its ability to withstand physical attacks, so also are redundancies needed in the EMS, in both the hardware and the software, to ensure reliability of this critical function. Redundancies in the communication channels to the RTUs and redundancies in the computer hardware (including automatic checkpointing and failover) have been common practice. Redundancies in software and its graceful degradation have been less common. The loss of the alarming system in a key EMS during

[18]For example, it is likely that multiple attacks on the transmission system will not occur precisely simultaneously even if planned that way. Even small differences in the time of failures could give important indications that an attack is occurring and allow remedial actions before the full effect of multiple failures would be felt.

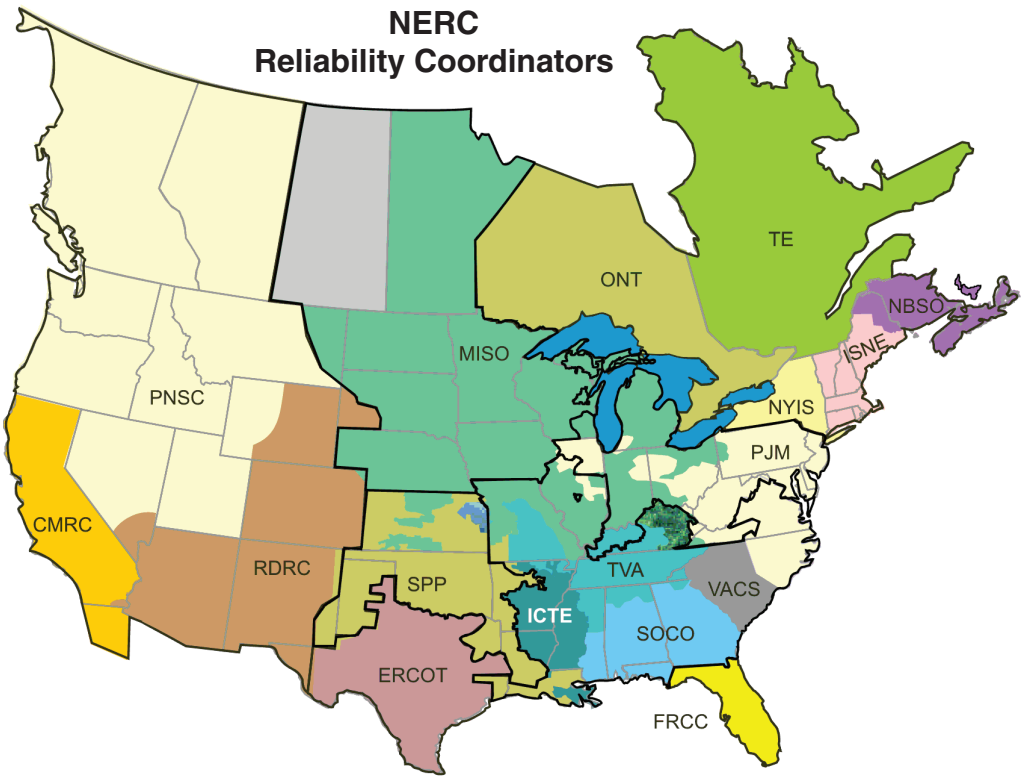


FIGURE 6.5 Reliability coordinators. SOURCE: NERC. Available at http://www.nerc.com/~filez/Logs/relcoors.htm. Accessed October 2007.

the 2003 U.S.-Canada blackout was a critical element in the operator not being aware of the deteriorating conditions in the power system. Better design of software redundancy and degradation should be a critical part of EMS design, as discussed in Chapter 4.

In addition to technology improvements, it is necessary to ensure that the operators themselves have the training to understand and deal with rapidly deteriorating situations. High-quality system simulators are now available to train operators to understand and manage complex disruptions of the transmission system. Much greater and more uniform use should be made of such systems during the training of system operators.

DISTRIBUTION ENGINEERING

Another area where there are design and operational strategies to mitigate the effect of attacks is the engineering of the distribution system. Once electric power has been transmitted in bulk over transmission lines, it is delivered to distribution or bulk power delivery substations where it is distributed to customers. Distribution substations consist of multiple step-down transformers that reduce the relatively high voltage of transmission lines to lower distribution voltages. Although some large industrial customers take electric power at higher voltages, more than 90 percent of all the electric power distributed in the United States is delivered at less than 15,000 volts.

The majority of distribution subsystems in the United States consist of overhead feeders typified by the common wood pole construction and pole-mounted transformers found in rural and most urban areas. A growing number of distribution customers are served by underground cables. Whether built as overhead lines or with underground cable, the majority of distribution is of a radial "single-feed" nature, meaning that the loss of the distribution feeder results in a customer interruption, since there is no alternative source of power.

Conventional overhead lines in a radial configuration usually are the least expensive way to distribute electric power to customers. However, overhead lines are vulnerable to natural and man-made attack. While any one line can be repaired quickly, multiple outages, such as after a hurricane, can result in long periods of service interruption. The use of underground cable, multiple feeds to the customer with automatic switching, loop circuits whereby customers can be switched from one feeder to the next, and other forms of redundancy significantly improve reliability at additional expense. In the case of critical loads such as a manufacturing facility or a hospital, distribution designers often provide a twin or dual feed, namely, an alternative feeder that provides redundancy in case the primary feeder is lost. Obviously, the cost to

provide such redundancy makes similar wholesale structural changes to the existing distribution systems unlikely.

Some use is made of "network" distribution, primarily in high-density urban areas. The low-voltage outputs of multiple distribution transformers are connected to create a network to which customers are attached. This inherently creates multiple feeds to customers. While these networks are more complex to operate than a simple radial distribution, they have certain advantages in both efficiency and reliability. The cost is greater than radial distribution but can be generally justified for serving the dense loads of a downtown area.

The loss of a distribution feeder results in the immediate loss of electric power to several hundred to several thousand customers—but such a disruption is often relatively small in the context of the entire utility system. Distribution will most likely be subject to physical attack when specific customers or critical industry are targeted. The distribution apparatus used today is operationally rugged and relatively easy to repair, but because the distribution system is rarely monitored, the only notice the utility receives that power has been lost to a customer is the customer calling to complain. Often distribution power outages last for several hours simply because the utility is initially unaware of the problem, and then it takes substantial time to dispatch the repair crew to locate a fault and identify and replace damaged equipment.

Through the use of automated distribution, significant opportunities exist to improve the reliability of electric power distribution without rebuilding the existing distribution system. In general, these include:

- *Automation of distribution systems, including SCADA systems.* This approach consists of the use of advanced sensors with communications infrastructure so that an electric utility can monitor and remotely control distribution. SCADA systems as part of distribution substations allow electric utility dispatchers to monitor feeder information, such as voltage level and feeder loading, with the coincident ability to open and close feeder breakers remotely. Systems for automated distribution and control can be incrementally introduced and are already in place in some parts of the country. Compelling arguments concerning economic development can be advanced for at least some such improvements, since distribution-system disturbances account for most of the power outages experienced by customers. State regulators should require local companies engaged in distribution to undertake studies that explore the potential benefits and costs of such upgrades, and then to mount programs of improvement that have clear positive net benefits.
- *Use of RTUs scattered throughout the distribution system.* Such systems would be installed at the feeder level, allowing a distribution dispatcher to sectionalize a feeder or perform switching operations to restore power by isolating faults. This action restores power to a large number of customers, minimizing the duration of an outage by quickly locating and isolating the faulted section. New developments include automated sectionalizing and restoration of healthy feeder sections, after a fault, using intelligent, distributed RTUs.
- *Advanced communication systems.* Advanced communications systems are being introduced into distribution systems, including radio and cell communications, to acquire data and to control remote devices. The distribution feeder itself is used as a communication medium in power-line communication systems. As communications improve, the functionality and the complexity of distribution automation grow.
- *Other advances in distribution automation.* These include the use of intelligent electronic devices, automatic meter reading, and continuous high-frequency monitoring of distribution feeders to identify the incipient failure of distribution equipment and to detect very-low-current, arcing faults. If failing equipment can be detected and repaired or replaced before catastrophic failure, the number and length of outages can be reduced. Computer-based intelligent electronic devices can be applied to monitor and protect distribution feeders, resulting in a wealth of information that supports system restoration and improved reliability (Benner and Russell, 2004; EPRI, 2005).

It is obvious that the existing electric distribution system in the United States is vulnerable to attack because it is highly distributed geographically. But the huge investment already made in electric distribution makes significant structural changes both expensive and long term. Consequently, efforts must focus on maintaining the health and robustness of distribution with an emphasis on restoring power after outages and maintaining the continuity of electric service to critical customers.

Over the next decade, efforts can prudently be concentrated on the following areas:

1. Critical customers should be identified and specific attention given to ensuring service continuity and maintenance of critical functions during a terrorist attack. This level of protection can be accomplished by providing multiple power feeds to distribution customers and by providing onsite generation in case of the loss of bulk transmission. Recent experiences in large-scale blackouts have shown that many critical loads are vulnerable and do not have adequate auxiliary power backup.
2. Distribution automation can be applied at reasonable cost, significantly improving the reliability of

distribution and making system restoration more deterministic and rapid. Emphasis should be given to applying improved SCADA, intelligent electronic devices, advanced communication, and sophisticated (broad-bandwidth) monitoring that provide continuous control and high-quality data concerning the operation of distribution. These devices can provide immediate notice of an outage, confirmation of the cause of the outage, and the specific information necessary to restore service as rapidly as possible.

3. Robust distribution is needed, which requires careful attention to system upgrades and maintenance. Distribution systems operating at close to design limits or systems operating with degraded equipment fail more easily and make restoration of service more difficult. Consideration should be given to the applications that monitor and diagnose the health and robustness of distribution, and to supporting condition-based maintenance and repair. Such continual maintenance also provides the opportunity for upgrading not just to new power equipment but also to the distribution automation technologies mentioned above.

DISTRIBUTED GENERATION/ENERGY SOURCES

One way to mitigate the effects of attacks on the electric power delivery system is to make end uses more resilient, as well as capable of operations when disconnected from the grid. Distributed generation refers to the use of relatively small generators spread throughout the electrical system, and typically connected at distribution primary voltages, or perhaps at the subtransmission level. The generators may be operated either by a utility or by other parties that have connected to the grid. Although widely used in some parts of Europe, such as the Netherlands, distributed generation has been slow to develop in the United States.

Because of the economics, regulatory barriers, and other factors, the technology has not really expanded yet, but there is a prospect for widespread use of distributed generation. Because there are now so many types of distributed generation systems,[19] as their use becomes more widespread, they should be introduced in a way that aligns with—rather than undermines—key Institute of Electrical and Electronic Engineers (IEEE) standards (Standards 1159, *Recommended Practice for Monitoring Electric Power Quality* and 1547, *Interconnecting Distributed Resources with the Electric Power System*). Some of the key technical issues in integrating distributed generation systems into the grid are as follows.

- *Distributed generation at substations.* The placement of distributed generation at transmission/distribution substations has been used in the past to provide emergency power. There are proposals to increase the level of distributed generation at substations to take advantage of the space and facilities at many of these substations.
- *IEEE standards, recommended practice, and guides for emergency power generation*[20] (Daley and Siciliano, 2003a,b; Davis and Stratford, 1988; IEEE, 1987), and certain other specialized systems.[21] These standardized procedures are largely in place in commercial and industrial applications in the United States today. At the time this report was prepared, there were no recommended practices for residential systems.
- *Back-up power installation.* The technology of back-up power is well known and commercialized. The appropriate IEEE standards for emergency and standby power technology are IEEE 446 (*IEEE Recommended Practice for Emergency and Standby Power Systems for Industrial and Commercial Applications*) and 141 (*Recommended Practice For Electric Power Distribution for Industrial Plants*).
- *Considerable volume of material on case studies for distributed generation.* A sampling in the literature of materials that relate to the potential of this technology, especially in the arena of emergency supply, include Ault et al. (2000, 2003). Daly and Morrison (2001), and Golshan and Arefifar (2006). In Daley and Siciliano (2003b), the specific case is made for distributed generation for emergencies. In Dugan et al. (2001), some cautions are outlined for cases of high penetration (i.e., high installed power levels) of distributed generation.
- *Safety.* Perhaps the greatest fear in installing distributed generation is the safety issue of circuits being fed from the load end (Dugan et al., 2001). During restoration of power after large disturbances, this safety issue could be very important (Barker and De Mello, 2000; Caire et al., 2002).
- *Interest in renewable energy sources to alleviate dependence on natural resources.* Renewable sources appear to be well suited for low-power scenarios, and the public acceptance of these sources is high. If the economics can be made favorable, there is a real prospect for the increased use of renewable sources.

[19]Some distributed generation is categorized as 60-Hz synchronous generation and its conventional controls. Other distributed generation may be interfaced with the distribution system through an electronic converter. Penetration levels in the time span 2006–2010 are not expected to exceed 10 percent of the total demand. However, localized high penetration levels may occur.

[20]Additional recent developments for emergency generation are discussed in Daley and Siciliano (2003a,b) and in Davis and Stratford (1988).

[21]IEEE Standard 141 (1986)—Recommended practice for electric power distribution for industrial plants; IEEE Standard 241 (1983)—Recommended practice for electric power systems in commercial buildings; IEEE Standard 493 (1980)—Recommended practice for the design of reliable industrial and commercial power systems; and IEEE Standard 602 (1986)—Recommended practice for electric systems in health care facilities.

The main nonhydroelectric renewable source is wind power. Photovoltaic panels coupled with battery storage have considerable potential for distributed generation as prices drop.

- *Energy storage to allow for increased use of renewables and to improve resiliency of the entire grid.* Improving the system load factor and utilizing renewable sources that are time and weather dependent require the use of energy storage. Prospects include batteries, pumped storage, compressed-air storage, and supercapacitors.

FINDINGS AND RECOMMENDATIONS

Findings

Findings on the Transmission Network—Short to Medium Term

Finding 6.1 Any increase in the reliability of the power grid makes the system more capable of withstanding terrorist attacks, more able to mitigate the impacts of such, and less interesting as a target of terrorists.

Finding 6.2 In many cases, increased performance of the electric power system may be achieved through stronger ERO reliability criteria and additional controls such as special protection systems. For example, the ERO and FERC could require NERC Category C performance for the common *N*–2 event of a short circuit on a line with line outage, and with simultaneous outage of a parallel line or line with common termination because of protective relay misoperation. Meeting this requirement would improve system robustness and help protect against terrorist actions on lines on the same right-of-way. As an example of new operating procedures, the DHS red-alert condition could require more conservative system operation similar to storm-watch procedures.

Finding 6.3 The robustness and resilience of power systems can be significantly improved by prioritized modernization of power plant and transmission infrastructure and deployment of technological advancements. Many power plant and substation enhancements can be rapidly implemented at low cost compared to the construction of new transmission lines. Potential upgrades include modern circuit protection systems, communications, generator excitation equipment, and shunt capacitor banks to increase generator reactive power reserve.

Finding 6.4 The control center is the nerve center of the power system, and its resiliency is extremely important. The computer hardware and software in the EMS should be designed to withstand failures and to degrade gracefully when necessary. The control center as a whole must be protected from physical as well as cyber attacks, and a backup control center should be available. Adjacent control centers (e.g., PJM Interconnection and Midwest Independent Transmission System Operator [MISO]) should partially back each other up.

Finding 6.5 Much greater and more uniform use should be made of simulators during the training of electric power system operators.

Finding 6.6 Undesirable and unnecessary operations of protective relays during power system disturbances have contributed to many cascading power failures. These relays are intended to detect short circuits or other specific conditions in a protection zone, but can operate inappropriately during other conditions such as overload and/or voltage sag. While commendable industry-wide improvements were implemented following the August 14, 2003, blackout, continual vigilance and careful design are required. Coordination among various control and protection devices is essential to system reliability.

Findings on Transmission Research and Other Long-term Needs

Finding 6.7 The electric power transmission system should move toward large-scale use of sensors that provide a complete physical and electrical picture of the power system in real time, and appropriate control measures that could be taken automatically and rapidly or suggested to system operators. Research needed to make such a system a reality is discussed in Chapter 9. With today's digital control and communication capabilities, there are many opportunities for application of sophisticated local, distributed, and high-level control algorithms using various techniques such as adaptive or "intelligent" control coupled with wide-area measurements and adaptive islanding.

Finding 6.8 Improved intelligent, digital relays are needed that allow for self-evaluation and remote evaluation of settings and status to ensure reliable operation.

Finding 6.9 Improved control philosophies and strategies are needed for multiple contingency events occurring in close time proximity. The proper operations of relays in response to changing conditions, when taken as a whole, can create unrecoverable instability in the power system.

Finding 6.10 Consideration should be given to redesigning some critical substations using buswork in pipes insulated with SF_6 with switchgear incorporated in the gas-insulated equipment. This approach allows more compact substation design, and the critical facility could then be relocated indoors or underground to provide more security against attacks.

Finding 6.11 As advanced storage technologies become available, strategies should be explored to use them to increase the performance and the resiliency of power systems.

Findings on the Distribution System

Finding 6.12 Being able to reduce load, and to focus on serving critical customers, can make the power delivery system far more robust in the face of natural disruption or terrorist attack. In many distribution systems, it is currently difficult or impossible to serve only a subset of customers on a distribution feeder. However, the technology is readily available to facilitate such selective service through distribution automation and intelligent load shedding.

Finding 6.13 Distribution systems operating at close to their design limits or systems operating with degraded equipment fail more easily and make restoration of service more difficult. State regulators should require distribution companies to assess the status of their systems and, where appropriate, require the installation of systems that monitor and diagnose the health and robustness of distribution, and support condition-based maintenance and repair. Systems that are operating with adequate capacity margins, and with all apparatus in good condition, are clearly more robust in the face of attacks or outages.

Finding 6.14 Greater use of automated distribution and load-shedding management holds the potential to reduce the vulnerability of the existing power system. Increased deployment of distributed generation and planning for the use of these facilities in the event of contingencies could greatly reduce the impact of an extended outage. Most of the needed technology for these concepts already exists.

Recommendations

Recommendation 6.1 The electric reliability organization (ERO) should require power companies to reexamine their critical substations to identify serious vulnerabilities to terrorist attack. Where such vulnerabilities are discovered, physical and cyber protection should be applied. In addition, the design of these substations should be modified with the goal of making them more flexible to allow for efficient reconfiguration in the event of a malicious attack on the power system. The bus configurations in these substations could have a significant impact on maintaining reliability in the event of a malicious attack on the power system. Bus layout or configuration could be a significant factor if a transformer, circuit breaker, instrument transformer, or bus work is blown up, possibly damaging nearby equipment.

Recommendation 6.2 The ERO and FERC should direct greater attention to vulnerability to multiple outages (e.g., *N*–2) planned by an intelligent adversary. In cases where major, long-term outages are possible, reinforcements should be considered as long as costs are commensurate with the reduction of vulnerability and other possible benefits.

Recommendation 6.3 The ERO and FERC should develop best practices and standards in improving system-wide instrumentation and the ability of near-real-time state estimation and security assessments, since otherwise operators are at a disadvantage trying to understand and manage system disruptions as they unfold. System operators should be able to observe what is going on well beyond their own borders whenever necessary. Reliability coordinators can oversee larger areas, maybe comprising several balancing authorities, but new entities should be established to oversee the whole Western and Eastern interconnection.

Recommendation 6.4 Local load-serving entities should work with local private and public sector groups to identify critical customers and plan a series of technical and organizational arrangements that can facilitate restricted service to critical customers during times of system stress. DHS could accelerate this process by initiating and partially funding a few local and regional demonstrations that could provide examples of best practice for other regions across the country.

BIBLIOGRAPHY

Anderson, K.L., D. Furey, and K. Omar. 2006. "Frayed Wires: U.S. Transmission System Shows Its Age." Available at www.fitchratings.com. Summary available at http://tdworld.com/news/fitch-electric-transmission-report/. Accessed August 2007.

Ault, G.W., A. Cruden, and J.R. McDonald. 2000. "Specification and Testing of a Comprehensive Strategic Analysis Framework for Distributed Generation." Pp. 1817–1822 in *Proceedings of the 2000 IEEE Summer Power Engineering Society Meeting*, Vol. 3. New York: IEEE.

Ault, G.W., J.R. McDonald, and G.M. Burt. 2003. "Strategic Analysis Framework for Evaluating Distributed Generation and Utility Strategies." *IEEE Proceedings—Generation, Transmission and Distribution* 150(4): 475–481.

Barker, P.P., and R.W. De Mello. 2000. "Determining the Impact of Distributed Generation on Power Systems. I. Radial Distribution Systems." Pp. 1645–1656 in *Proceedings of the 2000 IEEE Power Engineering Society Summer Meeting,* Vol. 3. New York: IEEE.

Benner, C.L., and B.D. Russell. 2004. "Investigation of Incipient Conditions Leading to the Failure of Distribution System Apparatus." Pp. 703–708 in *Proceedings of the IEEE PES Power Systems Conference and Exposition*, Vol. 2. New York: IEEE.

Blumsack, S.A. 2006. *Network Topologies and Transmission Investment Under Electric-Industry Restructuring*. Ph.D. Thesis, Department of Engineering and Public Policy, Carnegie Mellon University, Pittsburgh, Pa.

Caire, R., N. Retiere, S. Martino, C. Andrieu, and N. Hadjsaid. 2002. "Impact Assessment of LV Distributed Generation on MV Distribution Network." Pp. 1423–1428 in *Proceedings of the 2000 IEEE Power Engineering Society Summer Meeting*, Vol. 3. New York: IEEE.

Clark, H.K. 2004. "It's Time to Challenge Conventional Wisdom." *Transmission & Distribution World*. October 1. Available at http://tdworld.com/mag/power_time_challenge_conventional/index.html. Accessed August 2007.

Daly, P.A., and J. Morrison. 2001. "Understanding the Potential Benefits of Distributed Generation on Power Delivery Systems." Pp. A2/1–A213 in *Proceedings of the Rural Electric Power Conference*. New York: IEEE.

Daley, J.M., and R.L. Siciliano. 2003a. "Application of Emergency and Standby Generation for Distributed Generation. I. Concepts and Hypotheses." *IEEE Transactions on Industry Applications* 39(4): 1214–1225.

Daley, J.M., and R.L. Siciliano. 2003b. "Application of Emergency and Standby Generation for Distributed Generation. II. Experimental Evaluations." *IEEE Transactions on Industry Applications* 39(4): 1226–1233.

Davis, W.K., and R.P. Stratford. 1988. "Operation of UPS on Emergency Generation." Pp. 11–14 in *Proceedings of the Industrial and Commercial Power Systems Technical Conference*. Piscataway, N.J.: IEEE.

Dugan, R.C., T.E. McDermott, and G.J. Ball. 2001. "Planning for Distributed Generation." *IEEE Industry Applications Magazine* 7(2): 80–88.

EPRI (Electric Power Research Institute). 2005. *Distribution Fault Anticipator: Phase II Algorithm Development and Second-Year Data Collection*. Final report prepared for the Electric Power Research Institute. Publication 1010662. Palo Alto, Calif.: EPRI. November, 58 pp.

Golshan, M.E.H., and S.A. Arefifar. 2006. "Distributed Generation, Reactive Sources and Network-Configuration Planning for Power and Energy-Loss Reduction." *IEEE Proceedings—Generation, Transmission and Distribution* 153(2): 127–136.

Hsu, S.-M., H.J. Holley, W.M. Smith, and D.G. Piatt. 2000. "Voltage Profile Improvement Project at Alabama Power Company: A Case Study." Pp. 2039–2044 in *Proceedings of the 2000 IEEE Power Engineering Society Summer Meeting*, Vol. 4. New York: IEEE.

IEEE (Institute of Electrical and Electronic Engineers). 1987. IEEE Recommended Practice for Emergency Standby Power Systems for Industrial and Commercial Applications. Std. 446. Piscataway, N.J.: IEEE.

Nedwick, P., A.F. Mistr Jr., and E.B. Croasdale. 1995. "Reactive Management: A Key to Survival in the 1990s." *IEEE Transactions on Power Systems* 10(2): 1036–1043.

NERC (North American Electric Reliability Council). 2006a. Reliability Standards. Available at https://standards.nerc.net/. August 2007.

NERC. 2006b. Operating Manual. Available at http://www.nerc.com/~oc/operatingmanual.html. Accessed August 2007.

Taylor, C.W. 2001. "Power System Stability Controls." Chapter 11.6 in *The Electric Power Engineering Handbook*. Boca Raton, Fla.: CRC Press/IEEE Press.

U.S.–Canada Power System Outage Task Force. 2004. *Final Report on the August 14, 2003, Blackout in the United States and Canada: Causes and Recommendations*. Natural Resources Canada and the U.S. Department of Energy. April. Available at http://www2.nrcan.gc.ca/es/erb/erb/english/View.asp?x=690&oid=1221.

DOE/FERC (U.S. Department of Energy and Federal Energy Regulatory Commission). 2006. *Steps to Establish a Real-time Transmission Monitoring System for Transmission Owners and Operators within the Eastern and Western Interconnection—A Report to Congress Pursuant to Section 1839 of the Energy Policy Act of 2005.* February.

Yang, B., V. Vittal, and G.T. Heydt. 2006. "Slow-Coherency-Based Controlled Islanding—A Demonstration of the Approach on the August 14, 2003 Blackout Scenario." *IEEE Transactions on Power Systems* 21(4): 1840–1847.

Zerriffi, H. 2004. *Electric Power Systems Under Stress: An Evaluation of Centralized Versus Distributed System Architectures*. Ph.D. Thesis, Department of Engineering and Public Policy, Carnegie Mellon University, Pittsburgh, Pa.

7

Restoration of the Electric Power System After an Attack

Utilities have considerable experience with the problems of restoring electric service after massive disruptions caused by natural events such as ice storms or hurricanes, in which damage may be widespread. Such experience would be useful in restoring service after a terrorist attack, but the aftermath of an attack is likely to be quite different from a natural disaster. Terrorists can be expected to choose targets and inflict damage in order to impose maximum disruption and make speedy restoration difficult. Major substations and transmission lines are the most likely targets. Damage to key substations could be much greater and more extensive than that caused by most natural events,[1] requiring replacement of many large transformers, circuit breakers, and other equipment. Depending on the availability of spares, restoration could take weeks, months, or even longer.

Moreover, even given advance planning and preparation such as stockpiling of equipment, terrorists might compound damage by mounting a staged attack on additional or replacement facilities. After an attack, law enforcement and intelligence agencies will want to carefully study the damage in order to determine what was done and who did it. Unless prior arrangements have been carefully worked out ahead of time, the conflict between rapid restoration of service and careful study of a crime scene could result in considerable chaos and seriously delay the restoration process. Utilities and their contractors might also have to deal with a much higher level of physical, chemical, and biological threats after a terrorist attack than would be expected to arise as a consequence of any natural disruption.

Simply blowing up or knocking down a transmission tower can cause problems, but typically repairs can be done quickly. Transmission lines are most vulnerable when there are long stretches of suspension towers interspersed with only a very few dead-end or stop-loss structures.[2] In such cases the destruction of a few carefully chosen towers can result in a domino effect (cascading collapse) that can bring down many kilometers of line and towers.

In most cases, restoration after a cyber attack is likely to go more rapidly than after a well-planned and well-executed physical attack. However, if software has become widely infected with a pernicious virus, it may be necessary to reinstall large numbers of systems. If timed Trojan horses or worms have infected the system, there could be recurring problems. Some cyber attacks could also result in physical damage to important components in the power system. In most cases, however, this would likely be more limited than the damage caused by an all-out physical attack. Restoration could still be slow if key replacement equipment is not readily at hand.

PLANNING FOR THE AFTERMATH OF A TERRORIST ATTACK

As noted in previous chapters, to ensure continuity of service, utilities currently incorporate various degrees of contingency design into the design and operation of generating stations, substations, and transmission and distribution systems. The purpose of contingency design is to ensure that the loss of one or more components up to a defined design level should neither result in loss of service to customers nor lead to remaining in-service equipment exceeding designed operating specifications or ratings. Utilities have generally developed contingency designs based on the failure of single pieces of equipment or of a common support structure (such as a common transmission tower) rather than damage to multiple pieces of equipment at a given location or even the loss of multiple key facilities.

For example, a large urban area substation may be designed to operate under peak load conditions even with the loss of one or two of the power transformers supplying that particular station. However, in the face of a carefully designed terrorist attack, such $N-1$ or $N-2$ design criteria are not likely to be adequate to ensure continued operation.

[1] One possible exception could be a very large earthquake.

[2] Suspension towers are designed to support the cable vertically. They have little capability to withstand horizontal loads, which are usually balanced. If an adjoining tower comes down, however, the loads are unbalanced, and a line of towers may cascade down like a row of dominos.

Thus, utilities need to develop emergency response plans. Although it is not possible to cover all possible emergency scenarios, the planning and drill process is invaluable in building a capability in responding to actual events because it provides a basic framework and foundation. The following should be considered as part of future contingency response development:

- Evaluation of existing facilities based on their criticality and development of plans for recovery in the event of the loss of all key equipment in several of these facilities (e.g., the loss of entire substations or loss for an extended period of one or several key transmission lines). Such contingency analysis should be conducted to determine the impact of this loss on other facilities.
- For new designs or upgrades, a planning/engineering process that considers how to make facilities more robust in the face of possible attack, and development of strategies to quickly restore or bypass such facilities if they sustain significant damage.
- Sharing by utilities of ideas and designs that may improve performance. Organizations such as the Edison Electric Institute (EEI) and the Association of Edison Illuminating Companies (AEIC) are excellent forums for such sharing. Benchmarking with other utilities, especially those in countries that have had experience in addressing terrorist threats and attacks, will provide valuable lessons and ideas. For example, the Infrastructure Security Initiative sponsored by the Electric Power Research Institute (EPRI) produced *Counterterrorism Measures and the Protection and Restoration of an Electric Grid* (EPRI, 2005a), a report that describes Israel Electric Corporation (IEC) programs and procedures for maintaining the integrity of Israel's power transmission and distribution system, as well as related restoration efforts. However, there is a decided limit to how much special investment private utilities can be expected to make to protect against low-probability threats to every key element of their system.

To prepare for the possible need to mount a restoration of service, utilities should carefully address several important issues:

- Black-start capability (that is, the ability to supply limited amounts of power to generators and other power-system equipment before they can be brought back online);
- Line/cable charging strategies and other means of voltage and reactive power control;
- Need to disable or adjust certain protective systems, such as those for undervoltage, underfrequency, synchronization checks, and so on;
- Use of restoration panels; and
- Development of restoration policies, including islanding requirements and monitoring of voltages, frequencies, and phase angles.

In anticipation of catastrophic events leading to a system-wide blackout, utilities are required to develop plans that will enable their operators to break up the normally synchronized grid into "isolated" islands that are self-supportive. Such advanced planning can be valuable, but in the event of any specific outage, these plans will require real-time adjustments based on existing conditions, such as availability of equipment, load conditions, reactive power supply/control capability, availability of synchronizing equipment, and governing control while maintaining voltages and frequency at acceptable operating levels.

Plans for the restoration of a transmission and distribution system should consider two basic approaches. One is based on the availability of power from other external providers through tie lines. A second, or "island," approach considers restoration of the system from generation internal to its service territory. The latter approach could be significantly strengthened with the greater deployment of various types of distributed generation, including micro-grids. Today, however, there are considerable regulatory impediments[3] to the deployment of such systems, and distribution system operators typically do not have plans to make use of such resources in emergency situations.

With some important exceptions, many distribution circuits serve both socially critical facilities such as police stations, schools, and filling stations, together with many less critical facilities. If the supply of power were to become seriously limited, it would be highly desirable to temporarily restrict service to just critical loads. Advanced distribution automation (see Chapter 6) could make it possible to rapidly and selectively supply service to a few such key facilities. However, many systems still do not have distribution automation, and in the case of those that do, most have not been configured to facilitate such selective load shedding within a single distribution feeder. In the absence of such capabilities, reconfiguring distribution feeders to serve just a few loads would typically be a slow, labor-intensive operation (sending line crews out to open or close breakers at customer service drops), as would be restoring service to dropped customers along such feeders as power supplies once again became more plentiful.

[3]These impediments include informal difficulties that many distributed resources still experience when trying to connect to the utility system (Alderfer et al., 2000), interconnection rules that currently require all distributed resources to disconnect from the grid the moment any problems arise (IEEE, 2003), and laws that grant legacy utilities exclusive service territories, making the installation of small micro-grids that serve several customers difficult or impossible in much of the country (King, 2006; Morgan and Zerriffi, 2002). There is additional discussion of some of these issues in Chapter 9.

The use of emergency generators can also provide a quick and cost-effective response to restore critical loads. Many utilities have in-house emergency mobile generation or access to mobile generators through contracts with vendors. Utilities should make every effort to talk with critical customers about the importance of procuring their own backup generation to be able to respond to prolonged, unplanned outages to ensure that their critical services are available to the public in a timely manner following an attack. Utilities should also evaluate the critical loads they serve to help develop a prioritization plan for emergency generator dispatch. In addition, utilities should discuss this priority list with local governmental officials to get their input on the overall emergency response plan.

When a month-long outage hit the central business district in the city of Auckland, New Zealand, in February 1998, significant demand reduction during the restoration phase was achieved with rotating blackouts and through direct communication with customers, who were asked to remove a portion of the lamps in florescent fixtures (load reduction from 40 to 15 MW); run air conditioners on fresh air only, with reduced chiller banks and pre-cooling during off-peak hours (load reduction from 70 to 30 MW); turn off office equipment when not in use (load reduction from 25 to 20 MW); and employ various similar strategies (load reduction from 15 to 10 MW). The result was a reduction in these loads by 50 percent (Walker, 1999).

Although time-of-use meters are still rare in the United States, as they become more widespread it might be possible, with prior agreement of public utility commissions and with proper customer notification, to limit load during restoration by applying very high rates.

ENSURING ACCESS TO PHYSICAL EQUIPMENT FOR RESTORATION

After any disruption that results in the physical destruction of equipment, access to replacement parts is of critical importance. Thus, for example, utilities that operate in hurricane-prone regions routinely stock large supplies of distribution poles, distribution transformers, and similar equipment and have mutual support agreements with other utilities in the event that supplies run low. Utilities also routinely provide support to each other by supplying line crews and other critical human resources in the event of such large emergencies.

The situation after a major physical terrorist attack would be similar, but the equipment needs could be quite different. Terrorists would most likely seek to destroy many large high-voltage transformers. These devices are hard to move. Most are custom designs to meet specific needs. Because such devices are very expensive, and also very reliable under normal operating conditions, most utilities have only limited numbers of spares. With few exceptions, most such transformers are no longer made in the United States, and because of large demand across the developing world, lead times at factories are very long. Thus, the greatest vulnerability in the event of terrorist physical attack on the power system will likely be securing needed replacements of high-voltage transformers.

EEI is currently spearheading the Spare Transformer Equipment Program (STEP) to catalog available spares across the industry. Over 50 utilities participated in the negotiation of a binding contract, the Spare Transformer Sharing Agreement (EEI, 2006). Any investor-owned, government-owned, or rural electric cooperative utility in the United States or Canada may participate in the program, and currently 47 utilities, representing more than 60 percent of the Federal Energy Regulatory Commission (FERC) jurisdictional transmission systems, are members. The sharing agreement provides considerable flexibility for utilities to operate and utilize assets as they normally would during the course of business, but binds utilities to share their committed transformers if an event that triggers the sharing obligations should occur. A "triggering event" is defined as an act of terrorism that destroys or disables one or more substations and results in a state of emergency as declared by the President of the United States. The Spare Transformer Sharing Agreement also provides that any participating utility may voluntarily transfer spare transformers to a participating utility or to a nonparticipating utility regardless of whether a triggering event occurs. But each participating utility that disposes of a spare transformer through "permitted transfer" is obligated to obtain a replacement transformer as soon as practical, but in no event later than 18 months after the spare transformer is disposed of. In committing spare transformers under this binding agreement, participating utilities agree to sell committed transformers to any other qualified participating utility pursuant to a properly exercised "call right" and at a set purchase price. A commitment formula utilizing "needed megavolt," "connected megavolt," and available spares in defined voltage classes will be utilized to determine necessary commitments for each participating utility. The needs of each participating utility will be based on the impact of losing its five most critical substations within an equipment class. The basic obligations are to:

- Obtain qualified number of spare transformers equal to its commitment;
- Replace spare transformers that are used in order to continue to meet its commitment;
- Report necessary information to calculate its commitment;
- Maintain committed spare transformers in accordance with good utility practices; and
- Qualify for certification by an executive officer that the participating utility is complying with its commitment.

In some cases, a utility participating in the Spare Transformer Sharing Agreement may need to acquire, or acquire the right to, less than a whole transformer. Such utilities may choose to join with a small group of other utilities to acquire spare transformers. The utilities working on the development of the sharing agreement recognized that a joint procurement program might be helpful to some utilities and considered creating a special, not-for-profit entity for that purpose. One example of such a program is the nonprofit Pooled Inventory Management (PIM) program. Since 1980, this program has operated to acquire, store, and maintain long-lead-time spare parts for the nuclear industry. The PIM program has agreed to pursue development of a PIM spare transformer equipment program.

Technical meetings to work out the actual design specifications and required commitments for participating utilities will be held at least annually as part of this process. Also, the North American Electric Reliability Council has a listing of spare transformers that could be made available to a utility faced with a significant loss due to terrorist activity.

Participants in STEP recognized that FERC approval would be required for transfers of transformers under the sharing agreement. Under Section 203 of the Federal Power Act of 2005, FERC must approve the sale or disposition of jurisdictional assets in excess of $10 million. To expedite the process of transfers, participants petitioned FERC and received pre-approval of the transfer of spare transformers from one utility to another in the event of a terrorist attack. In its approval, FERC also determined that the sharing arrangement is prudent, which will support participants that seek to recover the costs of participation through rate setting. FERC believes that participation in STEP will increase transmission owners' emergency recovery capabilities by providing access to more spare transformers at lower cost. Participating utilities will also be seeking similar approval from their respective state commissions to ensure that they are able to recover the costs of acquiring spare transfers under the program.

As promising as STEP may be, it alone is not sufficient to address the vulnerabilities that the United States faces in the event of a large physical attack on the high-voltage substations of the power grid. There are not enough spares available to replace all those that might be lost in a terrorist attack. Furthermore, because of their size and variations in design, sufficient spares cannot be moved rapidly enough to provide needed recovery. With this in mind, EPRI (2006) has undertaken a project to build and test a compact "restoration transformer" that would be small enough to easily transport.[4] In order to reduce the size so that the device can fit into large cargo aircraft and move on trucks through underpasses, the transformer would run hot (and thus waste more energy than a conventional transformer). That would make operation too expensive for routine use, but it would allow much more rapid restoration of service than is now possible. EPRI describes the recovery transformer as:

> a new type of emergency spare high-voltage network transformer that is lighter than existing transformers, smaller, easier to transport, and faster to install and energize during recovery from severe high-voltage transformer outages induced by equipment failure, weather, earthquakes, or terrorist acts.
>
> After the terrorist attacks of September 2001, EPRI started the Infrastructure Security Initiative (EPRI 2005b), which identified the need to determine the technical feasibility of developing and testing a new high-voltage network transformer that is easier to transport and install than existing spares. The design was completed during Infrastructure Security Initiative work efforts and included tradeoff studies of capacity, impedance, and dielectric withstand strength, and voltage transformation ratios. These efforts resulted in the development of detailed specifications and electrical designs that covered a variety of North American network transformer voltages and megavolt ampere (MVA) ratings. The work also identified all mechanical components and field installation processes necessary to support the expedited transport and installation of the transformer. . . . Compared to existing transformers, this new type is characterized by the following:
>
> - Cost: about 20 percent lower
> - Weight: about 25 percent less
> - Size: about 25 percent smaller
> - Efficiency: about 99.0 percent (vs. 99.8 percent)
> - Operating temperature: about 155°C (vs. 110°C)
> - Installation time: about 48 hours (vs. weeks)
> - Design life: 35 years
>
> The time to install the transformer can be dramatically reduced through specialized storage and preparation-for-shipment techniques, specialized processing equipment and techniques, rapid deployment and transit, trained installation personnel, preparation of the installation site, and installation testing. Specifically, transformer condition should be carefully maintained during storage so that there are no "condition surprises" during installation. Oil monitoring systems will detect moisture and harmful chemicals to verify transformer readiness for use and conduciveness of the storage condition to immediate energizing. Prior recovery transformer work determined that careful management of relocation and reassembly is critical to reducing the total recovery time. For example, the use of draw lead or draw rod bushings (for higher current applications) will save many hours of installation time by eliminating the need to enter the transformer and reconnect primary current-carrying joints. Modularization of the cooling and oil expansion systems will reduce installation time: single cooling and oil expansion modules allow for module location at multiple storage sites and shipment and combination to serve various sizes of recovery transformers. (EPRI, 2006, p. 1)

[4]See also NRC (2002) and Stiegemeier and Girgis (2006).

Because the terrorist threat that any single utility faces is typically modest, even if the collective national risk is not, EPRI has had difficulty getting sufficient support from the electric power industry to move forward aggressively with this project. This is a classic case of "tragedy of the commons." Clearly, some sharing of the costs by all of society, through support by the federal, state, and local governments, is needed. This issue is discussed further in Chapter 9.

ORGANIZING FOR RESTORATION

Coordination of Essential Services

To ensure effective management, command, and control of an emergency situation, it is imperative that an organized command structure be used. The Incident Command System (ICS)[5] outlines effective management principles for control as well as the assignment of specific functions and responsibilities. This widely recognized organizational process is also used by federal, state, and local emergency response and governmental agencies. Advantages of using ICS include:

- Clear understanding of who is in charge,
- Defined roles and responsibilities for individuals,
- Improved communications with responding agencies,
- Greater sense of cooperation with outside stakeholders, and
- Overall enhanced and efficient response to emergency mitigation.

Although each utility's process might vary slightly from the standard ICS structure in order to meet specific needs, the core functional areas should remain intact. These functions include the incident commander and his or her staff for oversight and overall control (command) in operations, planning, logistics, and administration/finance. ICS is scalable and is equally effective for managing incidents that range from simple (routine) to complex (full scale). The incident commander's staff should also include representation in the following areas:

- Legal matters;
- Communications and media relations;
- Environmental, health, and safety issues;
- Liaison with government agencies and other involved organizations; and
- Customer outreach.

To fully integrate the use of ICS into the corporate culture, first responders should utilize it for both small- and large-scale emergencies.

[5]See, for example, http://www.training.fema.gov/EMIWeb/IS/ICSResource/assets/reviewMaterials.pdf.

While most of the focus on the impacts to utility infrastructure caused by terrorist activity has centered on the facilities that are directly associated with the generation, transmission, and distribution of electricity, the loss of other facilities should also be considered. Alternate reporting plans for corporate headquarters, dispatch centers, control rooms, work locations, and service centers are essential components of a comprehensive emergency response and business continuity planning document. Perhaps the most significant results of an attack at one of these locations would be the loss of human capital and impaired ability to coordinate operational and business activities.

The coordination of all essential services should be performed under a unified ICS structure spearheaded by local, state, or federal officials. It is at the governmental level that the overall response and restoration strategies must be developed and communicated. The overall strategy would include prioritizing the needs of all agencies. The utility should consider the following issues when preparing for an incident as well as during the response phase of an incident:

- Providing lodging for employees and outside contractors;
- Providing clean water and nonperishable food, which may include the ability to procure and stage freshwater tankers due to the potential contamination of freshwater supplies;
- Obtaining fuel to operate vehicles, equipment, and generators; and
- Providing means for employees to communicate with their families after an attack and before the employees are deployed or as they are being deployed.

Crisis Communication

Inability to communicate is a common shortfall identified by most companies during response to a large-scale natural disaster. Whether similar problems would arise after a terrorist attack would very much depend on the nature of the attack and whether other facilities were also attacked along with the power system. Of course, if power goes out across a large region, then communication can rapidly become a serious problem. Recent events have demonstrated that communications can become problematic and utilities cannot rely solely on telecommunication companies to solve their communication problems. Partnering with local emergency groups and state emergency management groups should be done to determine what systems they utilize and to what extent their systems could be used by the utilities during an emergency.

Utilities should also investigate programs that may be available to complement their communications systems by working with their local telecommunication companies to determine their involvement with the National Coordinating Center for Telecommunications (NCC). The NCC's mission

is to assist in the initiation of national coordination, restoration, and reconstitution of national security/emergency preparedness telecommunications service or facilities in all conditions, crises, or emergencies. The telecommunications industry and the government staff work together to coordinate support for responding to national security and emergency preparedness issues and to prevent and mitigate impacts on the national telecommunications infrastructure.[6] One example of federal support is the Government Emergency Telecommunications Service (GETS) system. GETS is a White House-directed emergency phone service provided by the National Communications System (NCS) in the Information Analysis and Infrastructure Protection Division of the Department of Homeland Security (DHS). GETS provides emergency access and priority processing in the local and long-distance segments of the public switched telephone network (PSTN). It is intended to be used in an emergency or crisis situation when the PSTN is congested and the probability of completing a call over normal or other alternate telecommunication means has significantly decreased.

Utilities need to look closely at their communication infrastructure and evaluate all alternate communication techniques. During a significant crisis, traditional communication systems, including cellular technology, may be shut down or become overloaded. The trunked 800-MHz radio is the current trend within the country for utility communications. The recommended standard for law enforcement, first responders, and utility emergency communications is the Association of Public Communications Officers (APCO) 25 Standard. Utilities should evaluate their own internal radio communications systems to determine that battery backup systems are in place or that generators can be made available at all communication locations, including repeater sites, to ensure that communication devices remain operative during incidents. Other options, such as satellite communications, need to be evaluated for potential backup communications in case normal communications channels become unavailable. Some utilities have even used temporary fixes such as a hovering helicopter as a relay station for communication using internal radio channels.

It should also be noted that dissimilar communication networks that do not allow emergency responders from different groups to communicate can yield disastrous results. Utilities should take the need for interoperability into account during preparations for emergency response.

Partnering for Mutual Assistance

The support of outside emergency and governmental agencies will be essential following an attack. One of the best investments an organization can make in emergency response planning is the development of relationships with key leaders from local governmental agencies and emergency responders. The constant nurturing of these relationships pays huge dividends for all parties involved as it results in an open environment that fosters both communication and cooperation. To build this relationship, concerted communication efforts on a regular basis are important.

For large-scale incidents, utilities typically rely on assistance from other utilities and qualified contractors to provide the necessary resources to respond to an event. In contrast to many natural events such as hurricanes, where the largest human resource need is for line crews to restore distribution systems, in the aftermath of a terrorist event, human resource needs are more likely to be for substation engineers and technicians, high-voltage-line construction crews, and perhaps also software security and restoration experts.

Typically, when extra human resources are needed, utilities first work with neighboring utilities and regional mutual assistance groups. Acceptance of pre-established rules and guidelines minimizes delays in obtaining help. In addition to local mutual assistance groups, participation in more global resource sharing networks through organizations such as the EEI and the American Gas Association is also valuable. Pre-sharing of specific information between utilities will provide those parties seeking help with a valuable resource during an emergency. Specifically, EEI has established a website to support mutual assistance activities and is developing a model mutual assistance agreement. For the most part, mutual assistance programs are generally limited to the sharing of labor and technical expertise. Recovery from deliberate destruction of utility infrastructure requires not only labor and technical expertise, but also the replacement of damaged critical infrastructure, such as transmission power transformers.

To ease the transition for visiting workers, utilities should develop a comprehensive assimilation program. This involves making sure that all visitors are provided information about the host utility's transmission and distribution system. The host utilities should provide clear-cut direction and guidance on its work rules and expectations in order to ensure that all personnel work safely, are aware of potential hazards, and abide by the host utility's environmental, health, and safety guidelines. The host utilities should have this information prepared in advance to minimize delays.

Host utilities also need to make detailed plans on housing and feeding visiting crews as well as providing them with knowledgeable field guides who are familiar not only with the geography of the area but also with specific work rules, site-specific hazards, and the ability to address all of the visiting crews' concerns.

Additional Special Considerations

Two other factors are likely to complicate the restoration work environment after a terrorist attack. First, law enforcement agencies will likely want to treat some facilities as a

[6]More information about the NCC is available through its website at http://www.ncs.gov/ncc/.

crime scene. While this is necessary and understandable, it is also important that utility personnel be able to gain early access to inspect their equipment and begin the process of planning for restoration, since any extended delay in restoration will cause large costs and further contribute to terrorists' goals of causing social and economic disruption. Thus, prior understandings need to be developed between utilities and law enforcement agencies to ensure that the objectives of adequate investigation and rapid service restoration are adequately balanced. It may be desirable to legally designate some utility personnel as emergency responders.[7]

The need to provide adequate protection and security for repair crews is another issue that may differentiate restoration after a terrorist attack from restoration after outages due to natural causes. Depending on the nature of the attack, responding utility personnel may need additional levels of personal protective equipment (PPE) in order to work in a contaminated environment. Utilities may need to increase security initiatives to ensure the safety of their employees during the assessment and restoration phases. All employees and contractors should have valid IDs, and these should be checked rigorously throughout the process. The utility may require assistance from federal and local law enforcement agencies to help expedite its employees' ability to report to assigned work locations. Such assistance will likely be facilitated if the utility has already trained and worked through scenarios with such agencies.

Utility employees are not experts in terrorist activities and should not underestimate potential dangers. For example, the initial attack might be designed to lure in emergency responders. Once emergency responders arrive at the scene, a second more devastating attack might be launched.

While utility personnel might not be considered emergency responders in the face of biological and chemical attacks, trained emergency responders from responsible governmental agencies may encounter a situation where the expertise of a utility employee might be required in order to respond to a situation where hazardous chemicals are present. To accomplish this objective, a utility might consider training certain employees in the use of U.S. Environmental Protection Agency (EPA) PPE Level A. Level A PPE, which consists of self-contained breathing apparatus and a totally encapsulating chemical-protective suit, provides the highest level of respiratory, eye, mucous membrane, and skin protection. These employees should only be counted on as a last resort during the initial phase of recovery from a biological or chemical attack and only for the purpose of mitigating any uncontrolled energy hazards (electrical, natural gas, steam, and so on). Another option is to work with other energy responders to train already-certified EPA Level A emergency responders to work at utility sites. This approach can be taken for their own protection, as well as for assisting in any utility-specific activities.

Utility employees typically possess a strong sense of commitment and desire to help, especially in the face of extreme duress. However, it is important to remember that injuries and death to employees, co-workers, family, and friends may occur as result of terrorist activity. Utilities may need to develop or enhance employee assistance programs that will help provide services, such as temporary shelter or housing, grief counseling, and dependent care, to ensure that employees' basic needs are met during a crisis. Additionally, business continuity plans that address high absentee levels are an important tool to ensure that critical business activities are sustainable in the event of various possible extreme situations, including health emergencies.

TESTING FOR RESTORATION—DRILLS

The first important step in ensuring readiness for any unplanned event is preparation through the planning process. The ability to identify "what-if" scenarios and then develop appropriate response plans is key to developing a comprehensive emergency response plan. Once plans have been developed, the next step is to test their effectiveness. The best way to accomplish this objective is through the use of drills and exercises. A well-constructed drill will test the ability of personnel to respond to simulated real-life situations as well as test their understanding of the overall plan. The drill will test the ability of personnel to understand their roles and responsibilities as well as test the overall effectiveness of the plan in resolving the emergency situation. The crucial elements for a successful exercise include establishing clear objectives, providing realistic scenarios that simulate real-life conditions, and establishing expected actions or outcomes. Perhaps the most valuable component of a drill is an after-action review that allows modifications to the plan to be discussed and implemented. The drills should include representatives of agencies outside local, state, and federal.

RESTORATION CONSIDERATIONS

Restoration of electric service after either a man-made or a natural disaster is a crucial element in helping the affected community to recover. In the event of a terrorist attack that causes significant damage to utility infrastructure, the utility will need to quickly develop and/or modify plans that will enable restoration of service to customers. In some cases, temporary restoration will precede initiation of a plan to institute more permanent repairs.

When faced with a terrorist attack that damages utility infrastructure, the utility should be prepared to adhere to

[7]In 2006, Congress passed the Safe Port Act, which the President signed into Public Law 109-347. This law, which recognizes electric utilities as "essential service providers" and instructs federal agencies to not impede their access to a damaged site or impede restoration except under exceptional circumstances, is a significant improvement. However, inasmuch as any terrorist event would be an "exceptional circumstance," designation of a few selected utility personnel as "first responders" would be a more certain way to ensure the needed access.

the following steps before actually initiating any restoration activities:

- *Accounting for all personnel*. The first concern for emergency responders will be for life and safety. Having a process in place to account for all personnel is essential in order to minimize the risk to emergency responders.
- *Site security*. Law enforcement officials will want to immediately secure the scene to ensure that the area is safe, conduct an investigation, and gather evidence. Utilities should be prepared to work with emergency responders to ensure their safety and de-energize the facility if necessary.
- *Establishment of ICS and command post*. Utilities should immediately implement an ICS organizational structure and appoint an incident commander to coordinate with outside agencies. During the initial stages of an incident, the incident commander will most likely be operating within a unified command structure along with fire, police, and governmental officials.
- *Site assessment*. Once a damaged site has been released by law enforcement, utility personnel will be able to make initial site assessments of hazards and damage and then develop the necessary strategies and plans to remediate the site, identify PPE requirements for employees, and determine what equipment must be isolated or bypassed, and what equipment can be utilized for restoration purposes.
- *Command and control*. During an event that may result in severe damage and/or islanding of a system, it is imperative to establish command and control locally, such as through the use of a "mini" control center that will serve as the hub during the restoration process. "Mini" control centers not only can help support operational restoration efforts but also can provide local visible presence to emergency responders, government officials, and the public. Major substations normally can meet some of these requirements, but if a substation has been attacked, a mobile command center vehicle might be used instead. Many utilities have such vehicles.

When developing restoration plans, a utility should consider the time of year and resulting demands on its system, including the amount of load served as well as the remaining capacity of in-service equipment. Other considerations should include:

- Minimizing the effects of cascading outages
  - —Sections of a large power system can separate into islands as a result of cascading outages. These independent islands should have automatic and manual load-shedding capabilities in response to decreasing island frequencies.
  - —Islands with excess generation result in increasing frequencies and thus depend on turbine-generator governors to stabilize frequencies.
- Synchronizing isolated islands
  - —Islanded or isolated sections of the power system should be interconnected with larger systems to share generation reserve capacity and inertial stability.
  - —All regions should have synchronizing capability within substations to interconnect systems.
- Control of isolated islands
  - —Management of independent islands requires coordinated control of generation to maintain both frequency and voltage.
  - —The use of isochronous and/or advanced generation control should be reviewed by control areas.
  - —Methods should be developed to manage load, generation, and spinning reserve.
- Complete restoration
  - —In the event of a widespread power failure, restoration procedures should be specific to restoration using both external and internal generation supplies. Depending on the severity of damage to particular aspects of the transmission system and/or specific substations and generating stations, islanding schemes may need to be developed or revised to determine which would be the easiest and most effective to implement based on the specific damage incurred.
  - —Specific hydroelectric and gas-turbine generators should be designated as black-start capable. Procedures should focus on restoring generation and controlling transmission system voltages.

SERVICE RESTORATION

Once the damage from a terrorist attack on the power system have been assessed, the damaged locations made secure for utility personnel to work, and replacement equipment ordered, then service restoration can begin.

It is important that all utilities have restoration plans that can be undertaken after a blackout. Such plans must cover the entire footprint of the area served and must be reviewed periodically and revised as needed to reflect infrastructure additions and retirements within the bulk power system. Even with multiple restoration plans, the utility will still have to evaluate the extent of the blackout and the severity of the damage to equipment to determine which plan(s) will result in an orderly, quick, and safe restoration. The following three major restoration scenarios should be considered:

- System-wide blackout with minimal or no damage to major generation, transmission, and distribution infrastructure (similar to the August 2003 blackout);
- System-wide blackout as a result of widespread damage to infrastructure or control systems that will impact restoration and operation of the system; and
- Local blackout as a result of damage to a local utility infrastructure or to control systems.

Restoration priorities should reflect the criticality of system restoration infrastructure, public health and safety considerations, and the sensitivity and criticality of customer loads. For example, system restoration infrastructure comprising the power company command-and-control centers, communication sites, emergency off-site power to nuclear stations, auxiliary power to key substation and generating station facilities, and key natural gas facilities should be restored first. Major facilities that impact public health and safety, such as key 911 and emergency operation centers, major hospitals, critical water treatment plants, major airports, and urban load centers, are next. All other customer loads can be restored after that. These restoration plans and priorities need to be flexible, given that the normal supplies (substations, transmission lines, and others) for those facilities may have incurred significant damage and the restoration priority thus possibly affected. For those circumstances, alternate means of supply that differ from the normal supply may need to be considered.

Black-Start Equipment

After a system-wide blackout, most, if not all, of the generation will have been shut down, and so the first step in restoration is to identify essential black-start generation equipment within the affected utility's service area. Black-start units are generators capable of starting up independently, without any connection to the bulk power system. These units involve equipment such as black-start diesel-generators which can be started on battery power and run on previously stored fuel to supply the necessary power to operate the auxiliary equipment, including the governor and excitation controls for larger units. Hydro-generators and combustion turbine-generators also can be used for black-start.[8]

This generation equipment is critical, since it will be needed to energize the transmission system from various system locations concurrently. Utilities must identify which generators are capable of providing this service and also if these are strategically located within the system to quickly provide the required restoration capacity. Furthermore, adequate black-start generation resources should be available throughout an RTO/ISO footprint to expeditiously restore the critical loads according to the restoration priority.

As generation becomes available and the transmission system is energized, utility operators should focus on synchronizing as much generation as possible to maintain system stability and voltage control. A small amount of load may be picked up to control voltages; however, the majority of customers should not be restored until the system has sufficient generation real-power reserves to meet the expected peak loads and reactive-power reserves to control transmission system voltages. Synchronizing with neighboring utilities is a priority because it allows reserve sharing and provides increased system stability.

Because of restructuring of the marketplace in certain parts of the nation where deregulation has occurred, the local utility may no longer own the required generation capability. To facilitate restoration efforts, utilities in both regulated and deregulated markets need to recognize the importance of black-start capability in relation to restoration efforts. Considering internal investment or encouraging others to invest in black-start capability is vital. In deregulated markets, appropriate compensation mechanisms should be implemented to ensure incentives for providing black-start capability. To the extent possible, efforts should be made to ensure that any new generation units are constructed with black-start capability.

After a blackout, operators must immediately request that all steam-based black-start units start up even if the transmission system is not yet ready for the generating unit to interconnect. This will prevent boiler pressure from dropping too far such that a longer period of time is required for the unit to be ready to interconnect.

Testing of black-start equipment must be done periodically, and a requirement should be implemented to verify that the designated units could respond within an agreed-upon time. Generation restoration start-up times vary considerably between hydroelectric units, combustion turbines, steam units, and nuclear units. Utilities should evaluate these differences and develop plans that consider these timing issues.

As the generation infrastructure ages, some existing black-start generating units are approaching retirement age. Such retiring black-start generation should be appropriately replaced.

Restoring Damaged Infrastructure

When significant damage to utility infrastructure has occurred, the restoration process may be complicated and lengthy. Utilities should be prepared for a prolonged recovery period and extensive allocation of both human resources and funding toward these efforts. In addition to the traditional means for restoration, such as through the use of generators and mobile transformers, utilities may also need to examine other alternatives that will provide for the quickest possible

[8]Utilities must consider the possibility that natural gas might not be available. Terrorists could take out gas transmission lines at the same time they are attacking the electric system. Alternatively, many gas transmission compressor stations now operate on electricity; if these are in the blacked out region, they will stop, severely limiting the amount of gas that can be delivered.

restoration while establishing the groundwork for permanent restoration in the future.

The utility will need to implement and adapt any plans it already has for bypassing damaged facilities and temporarily restoring customers to service. Many operational and support groups within the company will need to be part of this temporary restoration process. Utility engineers will provide a significant role in the design of a temporary system as well as making necessary changes to the supervisory control and data acquisition (SCADA)/modeling systems to reflect the changes that will be made. Typically, temporary restoration steps will not provide the same "normal" level of contingency design that is built into permanent restoration. Therefore, all systems used to monitor the system, equipment ratings, load flow analysis programs, and alarm points may have to be modified to ensure that operators can effectively monitor and operate the system in its temporary state.

Many industry utility vendors have recognized the threat of significant damage to utility infrastructure and have introduced mechanisms for quick restoration. Utilities need to consider the implementation of emergency restoration systems that will provide them with the necessary tools to implement a quicker recovery from a terrorist attack. For example, the introduction of modular restoration structures will enable utilities to quickly support transmission lines. These structures require no special foundation, can be used at any voltage level, and can be adapted for myriad suspension designs, angles, or tensions. The erection of transmission towers, installation of necessary hardware, and stringing of conductors requires significant logistical support and resources. The use of helicopters and large cranes, as well as the expertise of the employees, is critical to the rebuilding of transmission towers.

Various operational methodologies could enable utilities to restore service in a quick and efficient manner:

- *Bypassing at the transmission/switching station level.* Utilities should examine all potential operating scenarios, including the worst-case scenario of bypassing the entire facility. In order to bypass a particular station, temporary poles or towers could be used. In some cases, this might involve the use of transmission lines at voltages lower than those they are normally rated for in order to match the voltage ratings of equipment at the stations normally supplied by the bypassed station. For example, consider the loss of a substation receiving power at 345 kV, where the voltage is reduced to 138 kV for distribution. If the transmission line supplying power to the damaged substation is still intact, it could still carry power, but only at 138 kV. The power it could carry would be considerably reduced, but in an emergency that would still be very useful.
- *Bypassing at the distribution substation level*. Temporary restoration plans should be developed to address the restoration of service to customers and the associated load supplied by a particular distribution substation. There are several options that utilities will need to consider in the development of their plans. When looking at alternate supply options, utility engineers need to evaluate spare capacity at alternate supply locations to ensure that this equipment is capable of picking up the load(s) from the station that must be bypassed.
- *Customer load normally capable of being supplied from alternate substation.* Some utilities have radial distribution systems capable of being supplied by a minimum of two alternate sources. This can be accomplished through the use of an auto-loop system or an automatic transfer scenario. Ideally, in order to diversify the supply, the normal and alternate supplies should be provided from two different source substations in order to ensure continuity of service in the event of the loss of an entire substation.
- *Customer load normally supplied from the same substation.* In these cases, utility engineers must identify how to segment the load so that it can either be picked up in its entirety by an alternate source or so that it is "cut up" into various portions that can be picked up by different stations. For radial overhead systems, this may be as easy as performing field switching to isolate and segment the load and restore service accordingly. It is more complex for an underground network system. If multiple secondary networks are affected by the loss of an entire distribution substation, a sequence of carefully considered steps must be made in order to switch out feeders from a nearby network and connect them to the distribution feeders whose normal supply has been destroyed.
- *Mobile generation.* Another alternative is mobile generation, which can be used to supply load directly from the source or at the customer's premises. Mobile generators can be important for responding to a significant wide-scale power outage.
- *Distributed generation.* Increased use of distributed generation and renewable power alternatives can also provide viable alternate supply sources.
- *Mobile transformers and switchgear.* If a utility can quickly reestablish a transmission supply and gain access to distribution feeder supply exit cables, the use of mobile transformers and switchgear is a viable alternative. This option will also require additional space, not only to site this equipment but also to ensure it does not interfere with the rebuilding of the permanent station.

COMMUNICATIONS WITH THE PUBLIC

A critical yet often overlooked aspect of power system restoration is public communications. Timely communica-

tion of accurate information is essential to successful resolution of a crisis. During a crisis, however, engineers and operators must focus on the technical aspects of the job at hand and can find it difficult to make others aware of their plans and objectives during the restoration efforts. If communication is lacking, however, even well-developed restoration plans and restoration efforts can be perceived by the public as failures.

In general, the public is more receptive to being told bad news regarding a situation than to being kept uninformed or misinformed. Some members of the public, for example, may have developed their own contingency plans, including plans for self-evacuation or relocation, and must be able to make decisions based on accurate and timely information from government agencies, emergency responders, and utilities that provide critical services. Agencies, too, must be able to adjust their plans based on information supplied by utilities.

It is therefore imperative that all utilities have a well-thought-out crisis communication plan developed and carried out by people within the utility who have responsibility for communicating with government officials, news media, and the public. Crisis communication should:

- Describe the channels to be used to communicate information;
- Summarize clearly and concisely the incident and its impact on the utility infrastructure and its workforce;
- Project with reasonable accuracy what can be expected and when, ensuring that the information communicated is based on input from operations people and not on some notion of what the public wants to hear; and
- Provide regular updates with quantitative results and information on any unexpected changes.

Personnel assigned to the development of crisis communication plans should be well versed in other companies' public communications success and failures. Case studies of specific incidents should be reviewed. Utility company personnel assigned to communications during a crisis should be well trained in crisis management and public speaking. In addition, it is important that communication flow is channeled through a central point to promote the dissemination of accurate information. The ICS structure addresses this issue through the appointment of a communicator who works very closely with the incident commander.

Depending on the extent of the damage to utility infrastructure, restoration of service could take weeks or months. Stakeholders are more likely to be understanding if they are kept informed and up to date. Credibility and trust are difficult to gain and easy to lose. A utility will build trust and credibility by openly communicating with emergency responders, governmental officials and agencies, community leaders, customers, and the general public.

FINDINGS AND RECOMMENDATIONS

Findings

Finding 7.1 The main difference between a terrorist attack and a major natural disaster is that terrorists could selectively target key equipment, *especially large transformers*. Instead of days to weeks, full restoration of electric power could take months to years following a well-planned, well-executed terrorist attack.

Finding 7.2 The risk of terrorism to the nation's electric system as a whole is significant, but the probability of attack faced by any individual utility is low. Therefore it is neither realistic nor equitable to expect utilities or states to undertake all the needed equipment development and stockpiling without federal assistance. This is particularly true for the design, development, and manufacture and stockpiling of a set of high-voltage restoration transformers. While the utility industry, through the Edison Electric Institute, is working to build the Spare Transformer Equipment Program (STEP), *the number of spare transformers that might be available is much smaller than the number that a large terrorist attack could destroy*.

Finding 7.3 Analysis of vulnerabilities and planning for restoration of power after an attack are essential. Plans must cover a variety of attacks, be easily understood, and be specific to the operating utility infrastructure.

Finding 7.4 Strong and streamlined working relationships between utilities, federal and state governments, and law enforcement agencies are essential if utilities are to rapidly evaluate damaged equipment and implement plans for restoration of electric service to customers after a terrorist attack.

Finding 7.5 Greater use of distribution automation and demand-side management, as well as greater deployment of distributed generation and planning for the use of these facilities in the event of contingencies, hold considerable potential to reduce the vulnerability of the existing power system. Most of the needed technology already exists. Progress depends primarily on appropriate state regulatory and legislative initiatives.

Finding 7.6 All major incidents should be followed by a lessons-learned review of the entire incident to ensure that all weaknesses and deficiencies are identified and addressed.

Finding 7.7 Policies to balance risk communication and privacy/nondissemination of information require further investigation and research. Among the basic questions are how much information to communicate, to whom, under what threat levels, when, and how. Issues include approaches for maintaining openness, and the mechanics of disseminat-

ing evolving information to the public in view of potential legal ramifications and the responsibility to limit information available to terrorists. A key consideration is avoiding overreactions by informing the public while providing the highest level of protection to the nation.

Recommendations

Recommendation 7.1 The Department of Energy and the Department of Homeland Security should fund the research, development, manufacture, and deployment of stocks of compact, easily transported, high-voltage restoration transformers for use in temporary recovery following the loss of several to many regular transformers.

Recommendation 7.2 Utilities and federal, state, and local governments, and law enforcement agencies should develop official memoranda of understanding (MOUs). These MOUs should spell out each party's responsibilities before, during, and immediately following a deliberate destruction of utility equipment that leads to a disruption of electric service; provide a clear understanding of who is in charge; and explain how decisions will be reached in dealing with potential tensions between crime scene investigation and timely service restoration as well as unanticipated contingencies. The MOUs should also help to ensure the appropriate allocation of resources, and address concerns about potential government seizure of utility supplies and equipment during catastrophic events,[9] which can seriously hinder prompt utility restoration of electric service.

Recommendation 7.3 State and federal law or regulations should be modified to:

- Recognize utilities as essential service providers so that relevant utility employees can be trained and legally designated as first responders to deal with attacks on the power system.
- Provide utilities, when needed, with temporary exemptions from laws that restrict their use of equipment, access to roads, materials, supplies, and other critical elements for restoration of electric service to essential loads, including those that have an impact on public health and safety.
- Ensure that state regulatory agencies support prudent efforts by utilities to commit and acquire the necessary resources for service restoration and provide reasonable assurance for recovery of these costs.

Recommendation 7.4 The Department of Homeland Security and the Edison Electric Institute should jointly develop programs and offer training for key utility personnel to respond to both conventional security threats and potential chemical/biological attacks on the electric infrastructure. The training should provide increased awareness of the possible threats, through risk assessments, and provide specific training for the use of protection equipment, detection and sensor equipment, and emergency decontamination procedures. Existing drills and restoration procedures must be expanded to address the potential for biological or chemical attacks that would disrupt electric operations and infrastructures.

Recommendation 7.5 The Department of Homeland Security with the Department of Energy and the electric reliability organization should work with utilities that have not yet done so to:

- Establish a team reporting to top management that coordinates physical, cyber, and operations security through comprehensive plans that clearly define what is expected of security personnel before, during, and after a deliberate destructive act; identifies the technologies and strategies to be used to continuously monitor critical company facilities; and establishes an Incident Command System and designates an incident commander to work with outside agencies.
- Examine their internal radio communications systems to determine that battery backup systems and portable generators are in place to ensure that all communication devices will remain operational during a crisis. Because traditional communication systems may become unavailable during a destructive attack on the electric system, options such as satellite communications should be evaluated (and periodically tested) for potential use as backup communication. In addition, the ERO could help ensure that neighboring utilities and operators have compatible communications systems.
- Assess black-start capabilities in their systems under the assumption that major physical disruption of the transmission system can occur, develop appropriate contingency plans, and test both the plans and the equipment on a regular basis.
- Assess the potential for the cascading collapse of long stretches of transmission line, and, where appropriate, include offsetting towers at various intervals or reinforcing or upgrading towers at more frequent intervals along the line.

Recommendation 7.6 State legislatures should change utility law to explicitly allow micro-grids with distributed generation. IEEE should revise its standards to include the appropriate use of islanded distributed generation and microgrid resources for local islanding in emergency recovery operations. Utilities should reexamine and, if necessary, revise their distribution automation plans and capabilities in

[9]For example, during Hurricane Katrina there were efforts by some government entities to commandeer some utility communication systems and fuel supplies.

light of the possible need to selectively serve critical loads during extended restoration efforts. Public utility commissions should consider the potential emergency restoration benefits of distribution automation when they review utility applications involving such investments.

REFERENCES

Alderfer, R., T. Starrs, and M. Eldridge. 2000. *Making Connections: Case Studies of Interconnection Barriers and Their Impact on Distributed Power Projects*. NREL Report NREL/SR-200-28053. Golden, Colo.: National Renewable Energy Laboratories.

EEI (Edison Electric Institute). 2006. Section 203 Application and Petition for Declaratory Order from the Federal Energy Regulatory Commission Docket Nos. EC 06-140-000 and EL 06-86-000. Available at http://www.eei.org/about_EEI/advocacy_activities/Federal_Energy_Regulatory_Commission/060718FamaFercSpareTransformers.pdf, accessed October 2007.

EPRI (Electric Power Research Institute). 2005a. *Counterterrorism Measures and the Protection and Restoration of an Electric Grid. Infrastructure Security Initiative*. Palo Alto, Calif.: EPRI. October 30.

EPRI. 2005b. "Emergency Communications Phase 1 ISI Report. Infrastructure Security Initiative." Palo Alto, Calif.: EPRI. September 30.

EPRI. 2006. "Recovery Transformer—A Prototype Factory Build and Test Project." Available at http://www.epriweb.com/public/000000000001014534.pdf.

IEEE (Institute of Electrical and Electronic Engineers). 2003. *P-1547: IEEE Standard for Interconnecting Distributed Resources with Electric Power Systems*. IEEE Standard 1547-2003. New York: IEEE. Approved June 12.

King, D.E. 2006. "Electric Power Micro-grids: Opportunities and Challenges for an Emerging Distributed Energy Architecture." Ph.D. Thesis, Department of Engineering and Public Policy, Carnegie Mellon University, Pittsburgh, Pa.

Morgan, M.G., and H. Zerriffi. 2002. "The Regulatory Environment for Small Independent Micro-Grid Companies." *Electricity Journal* 15(9): 52–57.

NRC (National Research Council). 2002. *Making the Nation Safer: The Role of Science and Technology in Countering Terrorism*. Washington, D.C.: The National Academies Press.

Stiegemeier C., and R. Girgis. 2006. "Rapidly Deployable Recovery Transformers." *IEEE Power and Energy Magazine* 4(2): 38–45.

Walker, J. 1999. "Auckland Light Out from Failure to Recovery (Power System Disturbance)." *Proceedings of the 21st International Telecommunications Energy Conference*. PI 3-1. Copenhagen, June 6–9. New York: IEEE.

8

Strategies for Securing Crucial Services and Critical Infrastructure in the Event of an Extended Power Outage

As discussed in Chapters 6 and 7, there are many things that can and should be done to make the nation's electric power transmission and distribution systems more robust in the face of natural disruptions, equipment failures, or terrorist attacks. However, given the enormous complexity of the electric power system, and the fact that so much of the system is spread, unprotected, across large geographic areas, there is simply no way it can be made completely impervious to harm from natural disasters, system failures, or terrorist threats.

THE NEED FOR PLANNING FOR OUTAGES

Modern society and the digital economy have become ever more dependent on the continuous availability of electric power. For more and more applications, the need is not just for power, but for stable, highly reliable, high-quality power.[1] Many organizations with especially critical needs for electric power have already made arrangements for alternate sources of generation including power-conditioning equipment and backup power supplies. These organizations range from major hospitals, most of which now have regularly tested backup generators that can power critical systems in operating rooms and critical care facilities,[2] to financial institutions that must protect vital records and financial transaction data, to process industries that must keep production facilities, such as microelectronic fabrication lines or chemical plants, energized. In addition, virtually all critical air navigation systems and most of the backbone of major communication systems are highly dependent on high-quality uninterruptible power. Accordingly, most are now also protected by backup power supplies.

Yet many organizations that provide vital social services such as water, food, fuel, and communications remain vulnerable to both short- and long-term power interruptions. Indeed, some have become even more vulnerable with the widespread use of computer technology. For example, years ago telephones received their power over the same lines that carried the voice signals. In ordinary situations, an interruption of telephone service for a few hours or even a few days is an inconvenience. However, in an extended interruption of telephone and communication services during a major disaster, whether it is a terrorist attack or a natural disaster such as that experienced after Hurricane Katrina, lives may be lost if the public is unable to call 911, or if other emergency communications are disrupted.

There are many other situations in which electricity is required in order for basic services to function. These services include operating traffic signals to ensure the smooth flow of traffic in dense urban cores, pumps in the systems that provide potable water supplies and sanitary sewer systems, and compressors in natural gas supply systems that may be the fuel source for backup power systems or commercial and residential heating and/or air conditioning systems. The importance of functioning heating and cooling systems is forcefully demonstrated by the deaths that occurred from prolonged exposure to cold in the aftermath of the 1998 ice storm in Quebec, and from prolonged exposure to heat in the aftermath of Hurricane Katrina.

Under Homeland Security Presidential Directives HSPD-5 and HSPD-7, the President of the United States charged the Department of Homeland Security (DHS) with developing and implementing plans to create a framework through which the plans and activities of the federal government, state and local governments, the private sector, and nongovernmental entities could be aligned for the purpose of identifying critical infrastructure priorities and developing strategies to protect and restore critical infrastructure and preserve pub-

[1] "Stable" means, among other things, that the value of both voltage and frequency are maintained within tight margins. "High quality" means that the AC voltage and current wave forms are clean sinusoids with no significant harmonics, spikes, or similar short-term disruptions that can create havoc for modern electronics.

[2] Note, however, that during the Northeast blackout of August 2003, some of these hospital backup systems failed to operate, reinforcing the importance of regular testing and maintenance.

lic health and safety. In response to these directives, DHS developed and released the National Incident Management System, National Response Plan, and National Infrastructure Protection Plan. Together these documents create a framework to facilitate government and private sector interaction to establish national priorities, goals, and requirements for homeland security and critical infrastructure protection. In addition, these plans provide a framework for multijurisdictional and cross-sector interaction to address interdependencies of critical infrastructure and key resources to ensure that federal funding and resources are applied in the most effective and efficient manner.

The enormity and complexity of identifying security vulnerabilities, prioritizing actions, and developing executable plans at the local, regional, or national level should not be underestimated; nor should the challenge of aligning private sector business priorities with the national security and public health and safety priorities of governments.[3] These challenges extend well beyond the scope of this study and have yet to be comprehensively addressed. However, having noted the more general problem, the remainder of this chapter focuses specifically on the near- and long-term strategies for securing crucial services and critical infrastructure in the event of an extended power outage and provides recommendations on assessing and implementing these strategies.

STRATEGIES FOR SECURING CRUCIAL SERVICES

Assessing and Mitigating Vulnerabilities

In 2005, at the request of the state of Pennsylvania, investigators at the Carnegie Mellon Electricity Industry Center undertook an assessment of the nature and extent of critical social services in Pennsylvania that would be disrupted by power outages of a few hours to several weeks (PA DEP, 2005). Table 8.1 shows a slightly modified version of the taxonomy developed by that study. The study determined that with technology available today, and with careful foresight, many social vulnerabilities could be eliminated at modest cost. For example, the study found that while conventional traffic lights have electromechanical controllers and lamps that require over 100 watts, modern LED traffic lamps require less than a tenth as much power and can be operated on solid-state controllers. Systems like this, equipped with trickle charge battery backup, are now commercially available. Indeed, several such systems that had been installed in Ohio continued to operate during the August 14, 2003, Northeast blackout. The California Energy Commission has set up a program to help pay the incremental costs of backup for such lights.[4] In a press release announcing that program in 2002, Energy Commissioner Robert Pernell noted:

> When electric power fails and signal lights go out at a busy corner, traffic slows to a crawl. . . . Automobile accidents increase, and pedestrians find that weaving their way through the unregulated maze can be a dangerous, challenging prospect. But now local governments can protect critical intersections from power interruptions that can threaten motorists and pedestrians alike.

Promoting such solutions on a comprehensive basis will require greater coordination and planning. For example, in an extended blackout, it would probably not be necessary that all gas stations or cash machines have backup generators to run their pumps or dispense cash, nor would it likely be cost-effective for them to do so. Yet, private or public arrangements could be made to ensure that at least some facilities are so equipped and the public is informed about where to find them. Similarly, many water and sewer systems, or rapid transit systems, may not find it cost-effective to install dedicated backup systems. However, over time and with careful planning, as local utilities need to add peaking capacity, it might be possible to locate small generating facilities so that if and when the grid goes down, power can continue to be supplied to pumps or allow trains to get to stations (perhaps only a few at a time).

Note, too, that some minimum provision of some of these services is essential to restoring the power system—service trucks have to be able to get through and be fueled, crews need communications, and, in some circumstances, may also need police protection. Utilities have viewed ensuring access to such services as an important part of their contingency plans (see Chapter 7). However, to date most have not been proactive with respect to issues such as siting peaking plants close to critical loads so that, if necessary, they could be run independently of the grid. Nor have most worked with states and local communities to address other power needs in the event of a complete loss of power from conventional sources. In the future, if issues of critical services become more salient, some utilities may choose to voluntarily undertake initiatives to reduce the vulnerability of critical services in the absence of power from the grid. However, it is probably best that they maintain their primary focus on sustaining, or rapidly restoring, conventional service.

Few states and cities have conducted systematic studies to assess their vulnerabilities and develop cooperative public-private plans to reduce them. Clearly, it would be wise for states and cities, especially those that are assessed to be particularly vulnerable (Willis et al., 2005), to undertake such studies and to involve key players from private sector service providers, trade associations, and public agencies. Box 8.1 summarizes an exercise conducted by various departments

[3]For example, when power and telecommunications were operated as regulated utilities, it was relatively easy for government to request a specific change (such as moving a switching center to a less vulnerable location) as the costs could simply be added to the "rate base." Today, with the introduction of competition across much (but not all) of the power system, "socializing" such added costs becomes a great deal more difficult.

[4]See www.energy.ca.gov/releases/2002_releases/2002-05-20_backups.html.

TABLE 8.1 Examples of Critical Social Services That Depend on the Availability of Electric Power

Service Category	Specific Service	Typical Existing Backup	Resulting Vulnerabilities
Emergency Services	911 and related dispatch centers	Most have comprehensive backup power systems. Fuel supply and reliability could be an issue in long outages.	See classified version.
	Police headquarters and station houses	Varies. Some stations do not have backup. AC power is often required for recharging hand-held radios.	See classified version.
	Fire protection services	Same as above.	See classified version.
	Emergency medical services	Same as above.	See classified version.
	Hazardous materials response teams	Same as above.	See classified version.
Medical services	Ambulance and other medical transport services	Limited.	See classified version.
	Life-critical in-hospital care (such as emergency rooms, life support systems, operating rooms)	Full backup in most major facilities, but some failed during the blackout of August 14, 2003. Some systems have inadequate testing procedures. Fuel supply and reliability could be an issue in long outages.	See classified version.
	Less-critical in-hospital services (refrigeration, heating and cooling, sanitation, etc.)	Availability of backup varies. Many smaller facilities lack backup.	See classified version.
	Clinics and pharmacies	Many have no backup.	See classified version.
	Nursing homes	Same as above.	See classified version.
Communications and cyber services	Radio broadcast media	Major stations have backup systems with several days of fuel on hand.	See classified version.
	Television broadcast media	Many stations have backup power systems with several days of fuel.	See classified version.
	Cable television and broadband services	Minimal backup.	
	Conventional telephone	Conventional phone systems have backup power systems that can power switches and conventional phones. However, many modern head-sets and PBX systems require power to operate and do not have backup.	See classified version.
	Wireless (cellular) telephone and data systems	Modest backup. Battery backup typically provides only 2–8 hours of service.	See classified version.
	Wired data service	Many backbone systems have backup. Most local systems do not.	
	Computer services (on and off premise)	Many large data centers typically have good backups with several days of fuel on hand and priority fuel contracts. On-site typically limited to several minutes.	See classified version.
Water and sewer	Water supply	Limited backup. Most systems require pumping in treatment plants. Many systems also require pumping for delivery.	See classified version.
	Sewer systems	Very limited backup. Many systems require pumps for collection. Most require power for treatment.	

TABLE 8.1 Continued

Service Category	Specific Service	Typical Existing Backup	Resulting Vulnerabilities
Food	Retail groceries (cash registers, lighting, refrigeration, security)	Backup varies with location, local power reliability, and firm preferences.	See classified version.
	Wholesale grocery and distribution networks	Same as above.	
	Food production facilities (farms, animal facilities, processing, packaging, etc.)	Same as above.	See classified version.
Financial	Cash machines	Typically no backup.	See classified version.
	Credit card systems	Little or no backup at most retail outlets. Most central credit facilities do have backup. If communications systems also go down, then credit checking is not possible.	See classified version.
	Banks	Little or no backup at smaller banks except for security systems.	See classified version.
Fuel	Bulk fuel delivery	Backup varies. Some natural gas pipe lines are now using electric pumps. Some barge and port operations could be disrupted.	See classified version.
	Local storage infrastructure	Backup varies. Some locations can switch from pump to gravity feed.	See classified version.
	Retail gasoline sales	Most have no backup.	See classified version.
Non-emergency government services	Information service offices	Same as above.	See classified version.
	Operations units	Many have no backup.	See classified version.
	Prisons and other detention facilities	Many have some backup but may not be able to operate for extended periods.	See classified version.
	Schools	Most have no backup.	See classified version.
Transportation systems Transportation and mobility	Traffic lights	With few exception, no backup (although the technology is commercially available).	See classified version.
	Tunnels	In many cases no backup for ventilation. In some cases lighting has limited battery backup.	See classified version.
	Light rail systems and subways	Typically no backup except short-term emergency lighting.	See classified version.
	Conventional rail systems, including railroad crossings	Grade crossings have backup batteries. Backup for system operations is uneven.	See classified version.
	Air traffic control, navigation, landing aids, and airport operations and services.	FAA rules require backup power systems for all flight-critical systems. However, many terminal operations (such as ramp movement) have no backup.	See classified version.
	River lock and dam operations	Probably partial backup but specifics are unclear.	See classified version.
	Buses	Backup depends on system. Many have ability to fuel buses without off-site power.	See classified version.
	Drawbridge operations	Probably partial backup but specifics are unclear.	See classified version.

continued

TABLE 8.1 Continued

Service Category	Specific Service	Typical Existing Backup	Resulting Vulnerabilities
Lighting	Building evacuation and stairwell lighting	Battery-operated emergency lighting (only lasts a few hours) is required by building codes.	See classified version.
	Residential lighting	In most cases only backup is flashlights, candles, lanterns.	See classified version.
	Indoor commercial and industrial lighting	Backup is minimal in most buildings.	See classified version.
	Security lighting	Varies, but if there is backup it is typically short-lived batteries.	See classified version.
	Street lighting	Typically no backup.	See classified version.
Building operations (other than lighting)	Building elevators	Backup varies with local building codes, height and age of building.	See classified version.
	Space heating and cooling	Backup is minimal in most buildings.	See classified version.

NOTE: Some of these services, such as 911, emergency medical services, and en-route air traffic control, already have substantial backup. Many others, such as water and sewer systems, gas pumps, and cash machines, currently have no provisions for backup.

SOURCE: This table is a modified and elaborated presentation that is based on a taxonomy developed by researchers at Carnegie Mellon for the state of Pennsylvania (PA DEP, 2005).

at Carnegie Mellon University to assess options for sustaining the city of Pittsburgh's vital services if grid power is not available.

The importance of the private sector in the event of a terrorist attack cannot be overstated. Most major electricity and communications infrastructure facilities are in private hands, and their workers will necessarily function as first responders. Critical health care, transportation, banking, and fuel supply facilities are also mostly privately owned. Collaborative advance planning with such entities is absolutely necessary to ensure consideration of all contingencies. For example, a hospital administrator may know that he or she can plan for 24 hours of on-site generation, but for longer periods of time, fuel supplies will be needed to keep the hospital functioning. Having plans in advance for prioritizing who gets scarce fuel supplies will reduce chaos and add to the resilience of a given community in responding to a disaster.

Public policy and legal barriers to collaborative planning also need to be addressed. Significantly, the Pennsylvania study found a lack of transparency and trust across various levels of governments. For example, when, at the request of the Pennsylvania Department of Environmental Protection (DEP), the Carnegie Mellon Electricity Industry Center conducted its study for the state of Pennsylvania (PA DEP, 2005), neither investigators at Carnegie Mellon nor senior officials in the DEP were able to obtain critical data from the State Office of Emergency Preparedness or the U.S. Army Corps of Engineers on topics such as whether the locks through which barges carrying diesel fuel into the state did or did not have backup power and would be able to continue to operate in the event of an extended blackout. Political leaders need to analyze the data security and privacy protection laws of their agencies with an eye to minimizing and overcoming obstacles that can impede local and regional planning, as well as determine how interagency communication will function in a national or more localized emergency.

Improving the Reliability of Services

Obviously, planning costs and resources, as well as federal grants to the private sector or to local and state agencies, may be necessary to fund risk assessments and risk mitigation and restoration plans. Whether in the form of grants, incentive regulations, or tax- or fee-based subsidies, action needs to be taken to ensure that the private sector first responders undertake planning and restoration exercises. Again, the Pennsylvania study (PA DEP, 2005) suggested a variety of options that state or local governments might pursue, in appropriate circumstances, to encourage or require private parties to improve the reliability of important social services. The report's suggestions include (PA DEP, 2005, pp. 91-92):

- Provide information and suggestions to private parties to help them see how they might benefit from strategies that would make the services they provide more robust in the face of power outages. For example, once they think about it, a multistory retirement home that installs back-up power for its elevator might find that advertising this fact provides it with a comparative advantage.

BOX 8.1
The Pittsburgh Study

To develop specific data on sustaining services if the electric grid fails, the Carnegie Mellon Electricity Industry Center assigned the students in a 2004 engineering project course run jointly by the Carnegie Mellon University Department of Engineering and Public Policy, the H. John Heinz III School of Public Policy and Management, and the Department of Social and Decision Sciences the task of assessing options for sustaining Pittsburgh's vital services if grid power is not available.

The team of 20 undergraduates, two Ph.D. students, and four faculty members was assisted by a review panel with members from Duquesne Light Company, Allegheny Energy, the Pittsburgh Emergency Management Agency, Pittsburgh Department of City Planning, Pittsburgh Police, Dominion Peoples Gas, Pittsburgh Water and Sewer Authority, Pittsburgh International Airport, and the University of Pittsburgh Medical Center. Additional information was provided by PNC, Citizens Bank, Chevron, Guttman Oil, the Allegheny County Airport Authority, and the Allegheny County Sanitary Authority. Since some of the data when compiled could potentially be misused, the following summary has been approved for public distribution.

Potentially critical services were classified into the following categories: (1) emergency services, (2) private services, (3) utilities, and (4) ground and air transportation. Three reference blackout events were determined for which the robustness of each service was evaluated. The reference events were designed to vary in duration and size of the affected area. The diesel fuel supply available in Pittsburgh and the interactions between the services under different blackout scenarios were assessed. While some important services, such as hospitals and 911 emergency response, have taken measures to ensure that service will continue during a blackout, there are several vital services (e.g., police zone stations and traffic control) that are highly sensitive to electricity outages. Results from the assessment conducted include the following:

1. Three of the five Pittsburgh police zone stations were found not to have backup generation installed on site.
2. Important private services (e.g., grocery stores, gas stations, and cellular phone service) are vulnerable. Although the social benefits from keeping these services running during an outage are large, these benefits are dispersed among individuals, whereas the capital costs are concentrated in the hands of the service provider. There is little incentive for the private service providers to change.
3. Traffic networks are vulnerable, as all traffic lights would fail during a blackout. Tunnel ventilation fans would also become inoperable. Installing LED lights with backup batteries would reduce congestion in the event of a blackout and save money for the city in terms of annual electricity and maintenance costs. Backups for fans in heavily used tunnels were found to have a positive benefit-cost value.
4. Liquid fuel pipelines and storage tanks rely on electricity to pump fuel and generally have no backup. Some fuel can be released from storage tanks via gravity flow, but the switch over from pump to gravity flow can be time consuming.
5. An outage during extreme hot or cold weather could have significant health and economic impacts. If the outage occurs during very cold weather, forced-air heaters and auto-pilot boilers would fail; during hot weather, air conditioners would fail. In either event, some people could be at risk, and it is important to ensure that emergency shelters would be available and that information regarding such emergency services is disseminated through an effective information campaign. In addition to health effects, an extended outage during the winter could cause pipes in homes to freeze, putting even more stress on emergency management personnel. While some plans do exist for handling such emergencies, it is important that such plans be regularly reviewed and updated to ensure that the region is well prepared for an extended power outage.
6. The natural gas system is highly reliable, possibly more so than the diesel supply chain. Although natural gas generators are typically more expensive than diesel, natural-gas-powered backup might be an option worth considering for high-value services, especially if the generators are used to produce electricity and heat during normal operating conditions.
7. While air traffic control is fully backed up and the Pittsburgh International Airport has substantial backup, the latter is not sufficient to operate the ramps at gates. This would introduce significant delays that could then propagate through other parts of the system.

SOURCE: *Sustaining Pittsburgh's Vital Service when the Power Goes Out, Report of a Student Project Course, Department of Engineering and Public Policy*, Carnegie Mellon University, 2004, 108 pp. This is a sensitive document with limited circulation. A summary version is available at www.andrew.cmu.edu/user/phines/pdfs/executive_summary_when_the_power_goes_out.pdf.

- Encourage firms to offer "preferred customer" services that assure continued availability of services to those customers who have paid a fee which allows the companies to make the necessary additional investments. For example, customers of some fuel companies are now offered preferential delivery positions during emergencies in exchange for a fee. The Commonwealth of Pennsylvania may be able to create a supportive environment for preferential service agreements in other industries by increasing the awareness of potential blackouts. Entities such as gas stations have no incentive to install emergency power systems unless they are permitted to recover their cost through surcharges during emergencies. Such surcharges would be in the public interest, and the Commonwealth should consider studying whether barriers exist to fostering back-up power installations funded through peak charges.
- Require organizations to post public information on the presence or absence of back-up or other solutions to keep specific services such as elevators or gasoline pumps running in the event of a power disruption. In much the same way that the publication of EPA's toxic release inventory has induced many companies to cut emissions, such postings might induce companies to take steps to make their critical services more robust.
- Make changes in building codes and other legal requirements for business practice. For example, a decade ago Pittsburgh adopted a building code that requires elevators in newly constructed buildings of more than seven stories to have back-up power. Similarly, a community could require, as a condition of doing business, that firms operating gasoline pumps, ATM machines, or similar devices must work together to arrange that some percentage of them will remain operational in the event of a power outage.
- Provide tax incentives, subsidies, or grant programs to support the development of needed facilities. Given limited resources, this option should be used sparingly, but there might be some circumstances, such as certain upgrades in the emergency rooms of private hospitals, that warrant modest assistance.
- Pass laws or change regulations to facilitate the construction, interconnection, and operation of distributed generation systems, and the operation of competitive micro-grid systems.

The Pennsylvania study also suggested the following options, which might be pursued to encourage or require *public and nonprofit parties* to improve the reliability of important social services (PA DEP, 2005, pp. 92-93):

- Provide information and suggestions to local governments and non-profit organizations, such as hospitals, to help them see how they might benefit from strategies that would make the services they provide more robust in the face of power outages. For example, LED traffic lights require far less power than conventional traffic lights. Cities and towns could be encouraged to covert to LED systems and add trickle charge battery back-up. Such systems have capital expenses of several thousand dollars per intersection over the cost of an LED conversion without back-up, but this may be justified for critical urban corridors.
- Offer selective state subsidy programs, or lobby for the creation of selective Federal subsidy programs, to cover just the *incremental* cost of making systems more robust. To continue with the traffic light example above, such a program might cover only the trickle-charge battery back-up portion of the costs of conversion. Since this would dramatically improve the access of emergency vehicles during power blackouts, it might be a program that the DHS should support. Federal funding already exists for emergency power for air navigation. Restricted funds may be available from the DHS for increased security, the Airport Trust Fund for hub and reliever airports, and the Highway Trust Fund for tunnels. Use of state and local general tax revenue may be justified for survivable missions, such as police precinct back-up power. Water and sewer system back-up should be studied as systems are repaired and upgraded. A formal investigation of funding sources such as these is warranted.

One issue that the Pennsylvania report does not address is the range of actions that individuals can take to reduce their own vulnerabilities. These include such simple precautions as stocking basic supplies such as extra batteries and storing a supply of drinking water (as well as understanding that hot water heaters contain such a supply); owning hand crank radios and cell-phone chargers; stocking fuel for camp stoves and portable generators, and so on. While a few citizens, particularly in rural areas, have long taken such actions, many more would be wise to do so. Local governments could do much to raise citizen awareness of the value of such precautionary preparation.

The United States and its political subdivisions vary greatly in terms of demographics, political culture, geography, and attractiveness as a terrorist target. For that reason, no one strategy can be expected to meet the needs of all regions or all situations. However, the committee believes that the need to do systematic public and private planning applies to every community. The committee also believes that the very fact that communities have prevention and restoration plans for critical services and infrastructure could serve as a deterrent to terrorist attack.

Many studies have looked at the potential reliability benefits of distributed generation resources and micro-grids (Galvin Electricity Initiative, 2006; King, 2006; Lovins and Lovins, 1982; Zerriffi, 2004; Zerriffi et al., 2005). The stochastic simulations conducted by Zerriffi suggest that massive use of distributed resources can achieve reliability improvements over conventional power system architectures of several orders of magnitude. However, the regional reliability benefits that could be achieved with more modest use of distributed resources are less clear. To achieve full benefits from such systems, changes would need to be made in the standards and operating strategies of distribution systems, which, because they lack intelligent real-time control, typi-

cally now require that all distributed resources disconnect from distribution feeders the moment any problems develop. The discussion in Chapter 9 identifies current and near-term technological improvements that should be assessed in these planning exercises. For outages of longer duration, the committee believes that local governments should consider how the alternatives of distributed generation, portable generation, and load prioritization might be employed.

In its deliberations, the committee tried to determine the available surge capacity for portable generation. Caterpillar Inc. has a variety of portable diesel and gas-fired generator sets that can be mobilized rapidly. For example, these systems were installed in Lower Manhattan in the aftermath of the attacks on September 11. However, global demand for such generation sets is large, and manufacturing is currently running at or near capacity. Thus, in the event of an outage of very wide extent and duration, the demand for large portable power sources could easily exceed supply. The committee was unable to determine the status of planning for surge capacity for large backup power sources, for example the use of naval or civilian ships as temporary sources of power for coastal cites if conversion equipment is available. Similarly, diesel electric locomotives[5] might be temporarily pressed into emergency service as sources of electric power.

The Importance of Federal Leadership

Potential initiatives at the federal level to reduce social vulnerability in the face of extended loss of electric power include the following:

- DHS could develop, and then publicly disseminate, a set of strategies and technologies that public and private organizations and individuals might adopt in order to make critical social services of the sort outlined in Table 8.1 less vulnerable in the event of regional power outages of varying durations. Such an advisory document would be especially valuable if it contained specific "best practice" examples and associated cost estimates as well as illustrations of how market forces might be harnessed or incentives might be structured to encourage private initiatives that reduce vulnerability.
- Congress could provide resources and other incentives to encourage states and cities to form public-private task forces to assess the vulnerability of their vital social services to disruptions in electric power of varying duration. In order to do this, legal arrangements would have to be made to protect sensitive information, and legal and administrative arrangements should be developed to facilitate access to such information that is held by government parties.[6]
- Because some investments for better preparedness for extended blackouts are very much in the public interest but may not meet the more limited investment criteria of private firms or local municipalities, federal authorities could consider offering tax breaks or selected subsidies for the incremental costs of some protective systems. For example, although municipalities may choose to convert from conventional traffic lights to LED lights because of the substantial energy and cost savings that can result, they may not be willing to invest in trickle charge battery backup. A federal program, similar to the program developed by the California Energy Commission that covered the incremental cost of trickle charge battery backup for traffic lights along key arteries in dense urban cores, could be useful in this regard, as could a program that would help provide for more extended backup of critically located cell towers.

FINDINGS AND RECOMMENDATIONS

The process of assessing risks, prioritizing crucial services and critical infrastructure, aligning interests, and securing the cooperation of public and private sector stakeholders is an enormous and challenging task. Since an extended power outage could be local, regional, or involve multiple regions, leadership at the federal level is crucial to the development of flexible and effective plans to address a broad range of possible scenarios. Hence, the conclusions and recommendations in this chapter emphasize the need for this leadership and the close coordination of all levels of government with the private sector to develop robust plans for meeting local and national crucial services in the event of an extended power outage or substantial reduction of grid power.

Finding

Finding 8.1 Even if all reasonable steps are taken to ensure the reliability of the electric power transmission and distribution system, and to speed its rapid restoration after outages, there is no way that it can be made completely reliable in the face of major disruption by natural causes or large, well-planned, terrorist attacks. For this reason, and because modern society is increasingly dependent on electric power for the provision of critical social services, steps should be taken to ensure that the most important of these services (see

[5]The committee learned from a discussion with a representative of Burlington Northern Santa Fe that it does have conversion kits that can allow DC diesel electric locomotives to be used as 60 Hz AC power sources. However, as one might expect, the number of such kits is quite limited, at least within Burlington Northern Santa Fe.

[6]For example, the Census Bureau has arrangements under which serious researchers can gain access to detailed census track data, although it is very sensitive, by providing training and then making those researchers sworn census officers who are legally bound to conform to certain rules to protect sensitive data. To the committee's knowledge, neither DHS nor any state homeland security organization has developed equivalent arrangements to facilitate access to data they hold.

Table 8.1) can continue to be sustained if power from the grid is not available.

Recommendations

Recommendation 8.1 The Department of Homeland Security and/or the Department of Energy should initiate and fund several model demonstration assessments each at the level of cities, counties, and states. These assessments should examine systematically the region's vulnerability to extended power outages and develop cost-effective strategies that can be adopted to reduce or, over time, eliminate such vulnerabilities. These model assessments should involve all relevant public and private participants, including public and private parties providing law enforcement, water, gas, sewerage, health care, communications, transportation, fuel supply, banking, and food supply. These assessments should include a consideration of outages of long duration ($\geq$ several weeks) and large geographic extent (over several states) since such outages would require a response different from those needed to deal with shorter-duration events (hours to a few days).

Recommendation 8.2 Building on the results of these model assessments, DHS should develop, test, and disseminate guidelines and tools to assist cities, counties, states, and regions to conduct their own assessments and develop plans to reduce their vulnerabilities to extended power outages. DHS should also develop guidance for individuals to help them understand steps they can take to better prepare for and reduce their vulnerability in the event of extended blackouts.

Recommendation 8.3 State and local regions should use the tools provided by DHS as discussed in Recommendation 8.2 to undertake assessments of regional and local vulnerability to long-term outages, develop plans to collaboratively implement key strategies to reduce vulnerability, and assist private sector parties and individuals to identify steps they can take to reduce their vulnerabilities.

Recommendation 8.4 Congress, DHS, and the states should provide resources and incentives to cover incremental costs associated with private and public sector risk prevention and mitigation efforts to reduce the societal impact of an extended grid outage. Such incentives could include incremental funding for those aspects of systems that provide a public good but little private benefit, R&D support for new and emerging technology that will enhance the resiliency and restoration of the grid, and the development and implementation of building codes or ordinances that require alternate or backup sources of electric power for key facilities.

Recommendation 8.5 Federal and state agencies should identify legal barriers to data access, communications, and collaborative planning that could impede appropriate regional and local assessment and contingency planning for handling long-term outages. Political leaders of the jurisdictions involved should analyze the data security and privacy protection laws of their agencies with an eye to easing obstacles to collective planning and to facilitating smooth communication in a national or more localized emergency.

Recommendation 8.6 DHS should perform, or assist other federal agencies to perform, additional systematic assessment of the vulnerability of national infrastructure such as telecommunications and air traffic control in the face of extended and widespread loss of electric power, and then develop and implement strategies to reduce or eliminate vulnerabilities. Part of this work should include an assessment of the available surge capacity for large mobile generation sources. Such an assessment should include an examination of the feasibility of utilizing alternative sources of temporary power generation to meet emergency generation requirements (as identified by state, territorial, and local governments, the private sector, and nongovernmental organizations) in the event of a large-scale power outage of long duration. Such assessment should also include an examination of equipment availability, sources of power generation (mobile truck-mounted generators, naval and commercial ships, power barges, locomotives, and so on), transportation logistics, and system interconnection. When areas of potential shortages have been identified, plans should be developed and implemented to take corrective action and develop needed resource inventories, stockpiles, and mobilization plans.

On a longer time scale, urban planners could include the potential for blackouts and other security issues in their activities.

REFERENCES

Galvin Electricity Initiative. 2006. Available at http://www.galvinpower.org/resources/listall.php?sct=14.

King, D.E. 2006. "Electric Power Micro-grids: Opportunities and Challenges for an Emerging Distributed Energy Architecture." Ph.D. Thesis. Department of Engineering and Public Policy, Carnegie Mellon University, Pittsburgh, Pa.

Lovins, A.B., and L.H. Lovins. 1982. *Brittle Power: Energy Strategy for National Security.* Andover, Mass.: Brick House Pub. Co.

PA DEP (Pennsylvania Department of Environmental Protection). 2005. *Critical Electric Power Issues in Pennsylvania: Transmission, Distributed Generation and Continuing Services when the Grid Fails*. Report prepared for the PA DEP by the Carnegie Mellon Electricity Industry Center, Carnegie Mellon University, Pittsburgh, Pa., February.

Willis, H.H., A.R. Morral, T.K. Kelly, and J.J. Medby. 2005. *Estimating Terrorism Risk*. Arlington, Va.: RAND Center for Terrorism Risk Management Policy.

Zerriffi, H. 2004. "Electric Power Systems Under Stress: An Evaluation of Centralized Versus Distributed System Architectures." Ph.D. Thesis. Department of Engineering and Public Policy, Carnegie Mellon University, Pittsburgh, Pa.

Zerriffi, H., H. Dowlatabadi, and A. Farrell. 2005. "Incorporating Stress in Electric Power Systems Reliability Models." *Energy Policy* 35(1): 61–75.

9

Research and Development Needs for the Electric Power Delivery System

As discussed in earlier chapters, one of the most important steps in ensuring the electric power delivery system's resilience to terrorism is to ensure that it is as resilient as possible against more routine disturbances, that it can be rapidly restored if and when a disruption occurs, and that while the disruption is in progress, the impact on critical services is as modest as possible. The committee has concluded that, with a few notable exceptions, there is relatively little R&D that can be targeted just at terrorism, but that much that is intended to improve operations also will help against terrorism. Many of the most promising technologies under development for improving the power system may not harden it against terrorist attack, but they often will improve grid resilience and response and recovery. This chapter assesses research needs for reducing the risk from terrorist attacks in the context of overall power delivery system needs. It also notes alternative strategies by which the electric power system could be guided to greater robustness.

As discussed in Chapter 2, recent decades have witnessed chronic underinvestment in sustaining and upgrading the U.S. transmission and distribution system. The same has been true for research investments. Funding for R&D is also addressed in this chapter.

R&D FOR MEETING THREE BROAD GOALS

This chapter addresses R&D needs to meet the three goals discussed in previous chapters:

- Thwarting terrorist attacks (Chapters 3, 4, and 5);
- Reducing vulnerability to terrorist attacks (Chapter 6); and
- Reducing the impact of a terrorist attack and its consequences (Chapters 7 and 8).

Because the electric power system is one of the most complex systems every built, R&D programs to improve it are understandably complex as well. No one or two items will solve the problem of protecting against terrorism, mitigating impacts, and supporting recovery, although certain priorities can be identified.

Thwarting Attacks

Physical attacks on the bulk power system[1] and on critical components of the distribution system can cause widespread, potentially long-term outages. Thwarting such attacks involves developing physical security and sensing technology that enhances the robustness of the system to physical attacks on various components of the power system and provides adequate early warning.

Improved means for countering cyber attacks also are needed and can be furthered by research to ensure secure communications, protect the energy management systems (EMSs) that control the bulk power network, and enhance the development of distribution management systems (DMSs) for controlling the distribution system. A wide range of intelligent electronic devices, relays, and controls at substations (primarily at the distribution system levels) are potentially vulnerable because they can be accessed remotely via several different types of communication networks.

Reducing Vulnerability to Attacks

Reducing vulnerability and enhancing resilience involve modifying the electric power system to better manage the loss of key components. R&D can provide a variety of options for enhanced monitoring, reduced system stress, improved reliability, incorporation of advanced technology, specific components, efficient demand-side management, and the use of distributed energy resources.

[1]It is again noted that the term "bulk power system" generally applies to large central generation stations and those portions of the transmission system operated at voltages of 100 kV or higher.

Any physical or electrical disturbance affects the performance of the electric power system. Therefore, advanced emergency control techniques that would adjust disrupted power flow to an acceptable operating state would make the system more resilient to malicious attacks. Particularly important is the development of improved tools and strategies that allow a more nuanced real-time treatment of which loads are and are not served during restoration.

Reducing the Impact of an Attack

Reducing the impact of an attack (and its consequences) involves developing and using advanced network technologies and control features at both the bulk power system level and the distribution system level. Distributed energy resources could also play a significant role in minimizing power disruptions to customers, powering critical services and facilities, and facilitating restoration. Several concepts in this area involve the expanded use of combined heat and power technology, distributed generation, and micro-grids. Such technologies already are in use but not fully deployed. However, considerable research focused on hardware, control systems, control policy, and the impacts of alternative regulatory arrangements is needed to enable resolution of technical and regulatory impediments to integrate such resources into the overall system.

The extended loss of electric supply due to a malicious attack could have a significant impact on several interdependent civilian infrastructure systems,[2] including water treatment and pumping facilities, sewage treatment plants, transportation, communication systems, gas pipelines, and traffic control systems. Although studies have qualitatively evaluated the impact of the loss of power supply on specific systems, they have not, for the most part, considered all interdependent systems collectively. Moreover, in most regions, efforts have not been made to investigate and model the impacts of a long-term curtailment of the electricity supply. A critical aspect of system interdependencies is that official policies will be needed to coordinate these systems, establish hierarchies in terms of responsibilities and control following an attack, enunciate a clear public message, and continuously update information in a coordinated fashion.

The need for a well-coordinated, automatic or semi-automatic plan for restoring the electric system after a coordinated malicious attack has been a topic of intense discussion in the electric power industry. North American Electric Reliability Council (NERC) guidelines require every region to have such a plan. Automating recovery to reduce the possibility of human error, however, is an enormous task requiring significant investment in research toward developing techniques to coordinate various options and develop decision-making tools.

MAJOR TECHNOLOGY AREAS FOR REDUCING VULNERABILITY TO NATURAL DISASTERS AND TERRORIST ATTACKS

This section discusses a wide range of specific technologies for which R&D is promising. They are grouped into eight technology areas according to how they will benefit the power system.

Technologies That Allow Significant Increases in Power Flow

Increasing the power flow capacity of transmission lines can increase security because it provides greater ability to bypass a damaged line in delivering power from generating stations to load centers.

Reconfiguring Conductors

The transfer capability of some transmission circuits can be increased by raising the operating voltage and reconfiguring conductors into a more compact arrangement on existing rights-of-way.

High-amperage Conductors

New, recently developed conductors having composite cores or using aluminum alloys have higher current-carrying capability than conductors in general use. Under high rates of power flow, they have less mechanical sag at high temperatures because of lower thermal expansion as compared to typical conductors with steel cores. Reducing the sag of a loaded line allows greater loading of lines, although increased thermal capacity, if not used properly, can place more stress on the power system.

High-temperature Superconducting Cables

High-temperature superconducting cables can potentially carry three to five times as much current as conventional cables of the same size, but considerably more research is required before these cables can be made technically successful and ready for widespread use. Although initial assessments indicate that such cables are very complex and expensive special-purpose devices with limited applications, they nonetheless deserve consideration.

Composite Structures

New composite materials that are inherently insulating and corrosion-resistant could potentially replace metals in the support structures for substations and transmission lines and could also allow for reconfiguring existing rights-of-way to increase power flow. Many complex issues still have to

[2]See Chapter 8 for more details.

be addressed regarding their selection and application and to reduce costs.

Equipment That Allows Greater Control of Energy Flows

Greater control of energy flows reduces the risk of cascading failures and may speed restoration of power after a major outage. Medium-voltage (4-13 kV) and high-voltage (>69 kV) high-power electronic-based controllers can provide flexibility and speed in controlling the flow of power over transmission and distribution lines. New energy storage units can help level loads and improve system stability. Some specific examples of these equipment technologies are given below.

Flexible AC Transmission System (FACTS) Devices

High-voltage power electronic-based controllers are currently being demonstrated. FACTS controllers can increase the power transfer capability of transmission and distribution lines and improve overall system reliability by reacting almost instantaneously to disturbances. The unified power flow controller and the convertible static compensator are key examples of FACTS technology. They control both real and reactive power flows among transmission corridors and maintain the stability of transmission voltage. More research, design, and development is needed to reduce the cost and enhance the performance of FACTS technologies. The next steps should include the development of the fourth generation of FACTS controllers using advanced power electronics devices.

Advanced Power Electronic Devices

The next major step in the development of power electronic devices would be to replace the silicon-based thyristors used in current devices with thyristors based on wide-band-gap semiconductor materials, such as silicon carbide, gallium nitride, or very-thin-film diamond materials. These materials have the potential to reduce the cost of power electronic controls.

FACTS Integrated with Storage

Fast-response devices for energy storage could be used with FACTS controllers to provide ride-through capability for transient and brief outages. One promising technology, superconducting magnetic energy storage (SMES), responds to disturbances in less than one AC cycle and provides ride-through capability for multi-second outages. Research is needed to adapt the high-temperature superconducting materials described above for cables for use in the high-field SMES environment, potentially lowering the cost so that these units can be used to support the electric power transmission system.

Voltage-sourced Converters

Voltage-sourced converters can be used to connect independent asynchronous AC transmission systems. Other thyristor-based controllers can supply reactive power (i.e., volt-ampere-reactives) for voltage support and reactive power management in transmission systems. Connection of systems that now cannot be connected might lead to increased power flow.

Intelligent Universal Transformers

The intelligent universal transformer concept involves a state-of-the-art power electronic system and is not a transformer device in the traditional sense. It would be designed to replace conventional transformers with a power electronic system that steps voltage as traditional transformers do, but can also manage and control consumer demand and power flows, and compensate for reactive power.

Advanced Monitoring and Communications Equipment

Substantial improvements in the cost and performance of sensors and communications media and equipment offer the prospect of increasing the capacity of existing power system facilities by monitoring and compensating for the operating conditions of numerous devices simultaneously. Examples include the following.

Integrated Communication Architecture

Overlaying a communication architecture on the existing power delivery system could be a foundation for enhancing the functionality of the power system and, therefore, its resilience. This requires an open standards-based systems architecture for an infrastructure for data communications and distributed computing. Several technical elements of this infrastructure include, but are not limited to, data networking, communications over a wide variety of physical media, and embedded computing technologies. Challenges remain in fully deploying such an architecture while meeting cyber security challenges.

Wide Area Measurement System

The Wide Area Measurement System (WAMS), based on a combination of satellite communications employing time-stamping with fiber or wireless, will provide the real-time information needed for integrated control of large, highly interconnected transmission systems. By constantly monitoring the health of a network across a wide geographical area, WAMS can detect abnormal system conditions as they arise.

Dynamic Thermal Circuit Rating Technology

Dynamic thermal circuit rating (DTCR) technology can be used to increase the thermal loading on individual transmission lines. Present limits are both static and often conservative, based on assumed weather conditions. DTCR uses real-time information about weather, load, temperature, line tension, and/or line sag to estimate actual thermal limits, allowing higher thermal capacity of lines. Certain DTCR devices are commercially available, and others are currently being demonstrated on a few transmission systems.

Video Sag Monitoring

Direct monitoring of line sag can be used to extend the effectiveness of DTCR even further. A video "sag" meter has been prototyped that uses a digital camera mounted on a transmission tower to monitor the vertical position of the line. Sag monitoring is listed separately here and not included under the broader title of remote video monitoring of critical components because it enables dynamic operation.

Topology Estimators

Topology estimators can be used to accurately determine the real-time transmission grid configuration status of an interconnection. Accurate information on topology is necessary for accurate state estimation and the subsequent security-constrained dispatch that is the key computation for solving congestion problems.

Improved Simulation and Modeling

Faster-than-real-time simulation and improved modeling would enable very rapid computation of the power condition's status, and in turn:

- Faster-than-real-time, look-ahead simulations of operating conditions;
- What-if analyses from both the operations and the planning points of view;
- Integration of risk analysis into system models and quantification of effects on system security; and
- Through the use of advanced simulation, pattern recognition, and diagnostic models, determination of the location and nature of suspicious events.

Monitoring of Constraints

Sensor output, communication, and computation can be used in combination to monitor the effect of transmission constraints on wholesale power market activities. Operating in a limited fashion for the Eastern Interconnection, this capability could be enhanced to include probabilities of line outages on which a probabilistic reliability index could be based.

Database Protocols Development

A common information model is needed for transmission and distribution operations and maintenance databases. It would support interoperability by greatly reducing the number of needed software translators in situations involving a range of applications.

Technologies That Enable Increased Asset Utilization

Growth in the demand for electric power in dense urban areas will continue to challenge the capacity of the traditional medium-voltage underground network grids installed in most large cities to provide reliable power. To meet projected increases in demand while still providing safe, reliable, and affordable power, utilities will have to reconfigure networks and minimize secondary (low-voltage) cable. Technology options include the following:

Submersible (Underwater) Fast Switches

Fast switches enable connection of customers to alternate power sources during system reconfiguration, and a capability for reconfiguration at medium voltage minimizes the impact of a catastrophic event at a single power station or circuit. In underground networks where flooding is possible, there is a need for switches that can operate underwater while still energized so as to mitigate outages.

Low-voltage Switches and Smart Fuses for Isolation

Low-voltage devices such as automated breakers (switches) and smart fuses that respond to appropriate rise times allow for reconfiguration and isolation of faulty sections of the low-voltage grid network.

Technologies That Are Particularly Intended to Enhance Security

The technologies discussed in this chapter will contribute to enhanced security of the electric power system even though that is often not their primary goal. Technologies specifically intended to improve security will, in most cases, provide significant benefits in the face of major equipment failures resulting from natural disasters as well as terrorist attacks.

Probabilistic Vulnerability Assessment

A key priority among efforts to improve overall system security is to assess power system vulnerabilities to terrorism and identify the most effective countermeasures. Probabilis-

tic vulnerability assessment is a framework for objectively identifying the most significant threats to the electricity supply chain and assessing the relative cost-effectiveness of various potential solutions. The probabilistic methods developed in this effort will also provide the basis for improved assessment of risks encountered during normal power system operations.

Emergency Control and Restoration

Following a major terrorist attack or natural calamity, a system is needed to focus the initial response on prevention of cascading. Wide-area control and the use of fast-acting autonomous agents may create self-sufficient "islands" that can maintain power within a large blacked-out area.

Complex Interactive Networks

Continuation of R&D on complex interactive networks would enable analysis of information about the status of the power delivery system and the secure communications system after an attack, as well as coordination of their use for adaptive islanding. Once a stable configuration of power delivery system islands is established, algorithms for self-healing would gradually return the power delivery system to its normal state as more resources became available.

Most sensing and control agents in a power system today simply respond to changing local conditions according to preprogrammed instructions. Enhanced intelligent network agents (INAs) would have decision-making capability, based on internal analysis of network-wide conditions. Once implemented, INA technology would facilitate adaptive islanding and the smart power delivery system, which is among the technologies described below.

Smart Power Delivery System

The smart power delivery system would contain transmission-class fault anticipators tied to a network of distributed data processors communicating with regional operations centers, allowing simulations to be run to determine optimal corrective responses to any disruption. When attacks occur, a network of sensors would instantly detect a voltage fluctuation and communicate this information to intelligent relays and other equipment located at substations. These relays would automatically execute corrective actions, isolating the failed lines and re-routing power via power electronic-based controllers to other parts of the power delivery system. Many consumers would be unaware that a disruption had occurred. Additionally, advanced system analysis will allow utilities to determine reliability metrics based on probabilistic techniques, which would lead to improved asset utilization.

Integrated Asset Management

More sophisticated maintenance procedures will be vital to hardening the power system and ensuring the reliability of increasingly complex transmission networks. Software is needed that would interpret the raw data coming from real-time monitors into the critical information needed by system operators.

Integration of Distributed Energy Resources

There is a need to develop interconnection standards and requirements related to integrating distributed energy resources with power delivery systems. The effect of distributed resources on system performance, especially at high penetration rates, also needs to be determined.

Real-time Analysis

Real-time analysis of system stability and security will be needed to properly detect a multi-pronged terrorist attack or a sequence of other natural or man-made disasters. Online analytical tools are needed that will take this information, such as the data available from WAMS, and determine automatically what actions should be taken to prevent incipient disturbances from spreading. Meeting real-time system control requirements will require completing such analysis in a fraction of a second. Power system visualization would improve operator situational awareness, allowing a faster response to rapidly deteriorating situations.

Solid-state and Superconducting Fault Current Limiters

Unless carefully planned, the location of generation on a given power system can pose a risk of short-circuit currents that are dangerous to utility field personnel and may cause considerable damage to the power system. Fault current limiters would use either power electronics or superconductivity to limit short-circuit currents. These solid-state devices not only would act as a circuit breaker, but also would act in milliseconds to limit fault current levels.

Solid-state Power Electronic Circuit Breakers

Solid-state breakers will allow the system of the future to respond more quickly to disruptions and terrorist attacks.

Recovery Transformers

As noted in Chapters 3 and 8, the large power transformers in generating station switchyards and major substations are vulnerable to terrorist attack and could take months or years to replace. Options for bypassing damaged substations to bring power from remote generating stations to load centers are very limited because the grid is already stressed

during peak demand. The result of a coordinated attack on key substations could be rolling blackouts over a wide area until the substations are repaired.

Under such conditions, the availability of compact, easily transported recovery transformers would be invaluable. Recovery transformers would be usable for a variety of applications to replace the large power transformers optimized for a particular substation. They would be smaller for easier transport and relatively inexpensive. They would also be less efficient and therefore more costly to operate, and so would be used only until a regular replacement is available.

Recovery transformers need further development and testing. Then a reasonable supply of them would have to be manufactured and stored in strategic U.S. locations for use to recover as quickly as possible from any widespread disaster affecting a large part of the electric transmission infrastructure (see Chapter 8). The increased standardization of substation transformers being embraced by utilities will facilitate use of these recovery transformers.

Physical Security

Chapter 3 detailed a set of very-near-term developments that relate to physical security, including advanced design and engineering steps to harden substation sites and to make key components less vulnerable, improved sophisticated electronic surveillance technology that integrates sensor and monitoring, and security systems for high-voltage submarine cables.

Consumer Products

An array of R&D opportunities exist related to consumer products for enhancing the public's resilience to terrorism, particularly in residential and urban settings, but these are not considered within the scope of this report and so are not addressed here.

Technologies That Enable Greater Connectivity and Control

Making the nation's power system truly secure from disasters will require true consumer connectivity that includes the optimization of end-use devices. Means for achieving this include those outlined below.

Demand-side Management

Demand-side management (DSM), which is defined as the further deployment and utilization of energy-efficient electric end-use devices and greater use of consumer load control, will also be critical to complement the supply options inherent in a secure power system. DSM includes the ability to dispatch both loads and distributed energy resources. A variety of new communications and customer-interface technologies will be needed to enable load control to complement the options available for response to security concerns.

Advanced Distribution Automation

Advanced distribution automation (ADA) is defined as distribution monitoring and control, distribution system management, and consumer interaction (e.g., load management, "smart" metering, and real-time pricing). ADA will enable real-time optimization, such as operating distributed energy resources when other facilities have been compromised. Two developments are needed to make ADA a reality: (1) an open communication architecture and (2) a redeveloped power system from an electrical architecture standpoint. ADA will use various advanced technologies, including communications systems, distributed computing, embedded system computing, sensor and monitoring technologies, and power-electronics-based components.

Self-healing Control Methodology for Distribution Systems

For the distribution system to be secure, it is essential to enable distribution system monitoring through a web of sensors integrated with an overall control methodology to respond to terrorist attacks and reduce the duration and impact of failures through a self-healing methodology.

Low-cost Sensors

A series of web-enabled, inexpensive sensors that can be linked to global positioning satellites would allow higher levels of control of control.

Pre-failure Indicators

High-speed, online sensors are needed for detecting distortions in the 60-cycle power line carrier. Waveform distortions need to be correlated with early indicators of system component failure. Pattern recognition software is needed that will analyze the power line waveform and detect pre-failure indicators in real time.

Technologies to Reduce Demand on the Power System

Although the technologies described below are not directly related to addressing threats from terrorism, they would collectively reduce the stress on the electric system infrastructure and thereby contribute to its resilience in the face of attack.

Efficient Lighting

Much of the artificial illumination in place today is considerably less efficient than theoretically, or even practically, possible. Increased use of high-efficiency lighting systems

that combine efficacious light sources with luminaries that effectively direct light where it is desired, coupled with controls to adjust light levels as needed, will collectively improve overall lighting efficiency.

Efficient Space Conditioning (Building Heating and Cooling)

Considerable progress has been made in the last few decades toward improving the efficiency of space conditioning equipment. Much of the progress is due to state building codes and federal standards that dictate the minimum efficiency of new air conditioning systems. More opportunities exist to further enhance the efficiency of heating and cooling systems and thus reduce demand for electric power.

Efficient Domestic Water Heating

Electric water heaters lose heat through tank walls and piping. Research is needed on newer systems that produce hot water on demand, thereby eliminating the storage tank and its associated losses of heat. In addition, R&D is needed on (1) heat pump water heaters that can utilize heat from the surrounding air to heat water while providing cooling and dehumidification of the surrounding room air space, and (2) systems that recover waste heat from air conditioning systems.

Distributed Energy Resource Technologies

Distributed Generation

Distributed generation (DG), micro-grids, and other distributed energy resources technologies can augment the large central power generators of the present-day electric power delivery system. Energy conversion efficiencies for DG technologies are still substantially below those for conventional generation technologies. However, it is often possible to use the waste heat in industrial processes, an approach known as combined heat and power (CHP), boosting overall efficiency to high levels (e.g., 75 percent). Key DG technologies requiring R&D are intelligent control systems, high-efficiency internal combustion engines, microturbines, fuel cells, and Stirling engines. Also needed is R&D on CHP for residential applications, photovoltaic devices and low-cost "balance of system" electronics, solar-thermal systems, and building-integrated and concentration solar systems.

Electric Energy Storage

Electric energy storage refers specifically to a capability for storing already-generated electrical energy and controlling its release for use at another time. Most electrical energy storage systems have demonstrated efficiencies of between 60 and 70 percent, a level that must be improved significantly to make applications such as load leveling feasible. Key energy storage technologies requiring R&D are lead acid batteries, nickel-cadmium batteries, nickel-metal hydride batteries, lithium-ion batteries, vanadium redox flow batteries, sodium-sulfur batteries, flywheel energy storage, ultracapacitors, miniature compressed air energy storage, and superconducting magnetic energy storage.

R&D Priorities

The technologies discussed above are correlated in Table 9.1, with the goals to which they may contribute: thwarting attacks, reducing vulnerability, and reducing the impact of prolonged outages. Although relatively few technologies are listed directly for thwarting attacks, reducing vulnerability to and the impacts of attacks also reduces terrorists' incentives for attacking the power system. Therefore to some extent, all the technologies listed in Table 9.1 will contribute to thwarting attacks.

The committee was assisted in the selection of these technologies by the advice of many experts in industry, academia, and research institutions whose views were solicited in a widely circulated questionnaire. This exercise and the results are described in Box 9.1. The full list of promising R&D projects considered in the questionnaire is shown in Appendix H.

The committee believes that the following should have the highest priority in the mid- to long-term time frame:

1. Development, demonstration, and deployment of high-voltage recovery transformers;
2. Development and demonstration of the advanced computational system intended to support more rapid estimation of system state and broader system analysis;
3. Development of a visualization system for transmission control centers to support informed operator decision making and reduce vulnerability to human errors;
4. Development of dynamic systems technology and demand response demonstrations to allow interactive control of consumers and consumer loads;
5. Development of multilayer control strategies that include capabilities to island and self-heal the power system; and
6. Development of improved energy storage that can be deployed as dispersed systems.

HOW MUCH RESEARCH?

The market is very good at commercializing well-developed basic technology ideas. However, many of the ideas discussed in this chapter are not yet at the stage that they can be readily turned into operating hardware or systems. The earlier the stage of development, and the longer the interval from idea to commercial application, the lower the prob-

TABLE 9.1 Promising Research Technologies for Reducing Vulnerability

Research Areas	Technologies	Objectives		
		Thwart Attack	Reduce Vulnerability	Reduce Impact
Technologies that allow significant increases in power flow	• Reconfiguring conductors		X	X
	• High-amperage conductors		X	X
	• High-temperature superconducting cables		X	
	• Composite structures		X	
Equipment that allows greater control of energy flows	• Flexible AC transmission system (FACTS) devices		X	
	• Advanced power electronic devices		X	
	• FACTS integrated with storage		X	
	• Voltage-sourced converters		X	X
	• Intelligent universal transformers		X	X
Advanced monitoring and communications equipment	• Integrated communication architecture		X	X
	• Wide-area measurement system		X	
	• Dynamic thermal circuit rating technology		X	
	• Video sag monitoring	X	X	X
	• Topology estimators		X	
	• Improved simulation and modeling		X	
	• Monitoring of constraints			
	• Database protocols development			
Technologies that enable increased asset utilization	• Submersible (underwater) fast switches	X	X	
	• Low-voltage switches and smart fuses for isolation		X	
Technologies that are particularly intended to enhance security	• Probabilistic vulnerability assessment	X	X	X
	• Emergency control and restoration		X	X
	• Complex interactive network		X	X
	• Smart power delivery system	X	X	X
	• Integrated asset management	X	X	
	• Integration of distributed energy resources		X	X
	• Real-time analysis	X	X	
	• Solid-state and superconducting fault current limiters		X	
	• Solid-state power electronic circuit breakers		X	
	• Recovery transformers			X
	• Physical security technologies	X		
Technologies that enable greater connectivity and control	• Demand-side management		X	
	• Advanced distribution automation		X	X
	• Self-healing control methodology for distribution systems		X	X
	• Low-cost sensors		X	
	• Pre-failure indicators	X	X	
Technologies to reduce demand on the power system	• Efficient lighting		X	X
	• Efficient space conditioning (building heating/cooling		X	X
	• Efficient domestic water heating		X	X
Distributed energy technologies	• Distributed generation		X	X
	• Electric energy storage		X	X

ability that conventional market forces will result in research and development being done. Society funds longer-term fundamental research as a way to provide options for the future. However, the question of how much society should invest in research to develop basic ideas to protect the electric power system from terrorist threats is difficult to answer for three reasons:

1. Because the probability of terrorist attacks on the power system, the magnitude of such attacks, and the likelihood of success are all unknowable, it is impossible to calculate accurately what the benefits of R&D might be.
2. It cannot be known beforehand what new technologies and options research will make available.
3. As indicated above in this chapter, most investments in power delivery system research would serve broad needs, not just the need to protect the system from terrorist attacks. Even those investments that are most antiterrorism-specific have other beneficial aspects (e.g., recovery transformers could be moved quickly to a stricken area after a large earthquake or hurricane).

In view of these considerations, the best that can be done is to develop some order-of-magnitude arguments concerning research investments. The committee was unable to find any rigorous estimates of the national impact of prolonged blackouts resulting from terrorist attacks. In Chapter 1, the committee concluded that a sophisticated terrorist attack could cost hundreds of billions of dollars, mostly from the loss of economic activity while power is unavailable.

Over the next decade, a well-designed research program could result in knowledge and technology that could significantly reduce the cost of a large, long-term blackout caused by terrorist attack. This is particularly true if that research also included some of the strategies discussed in Chapter 8 that would make critical social services less vulnerable in the face of disruption of electrical supply. The committee has not been able to develop meaningful quantitative estimates of the probability of attack. However, a simple parametric assessment can help to bound the potential value of R&D undertaken to reduce the power delivery system's vulnerability to terrorist acts, as shown in Figure 9.1. For example, suppose that over the coming decade, there is a 1 in 100 chance that a large coordinated terrorist attack on the electric power delivery system could impose societal costs of the order of $100 billion. A 1 in 100 chance of a loss of $100 billion can then be represented as an expected loss of $1 billion (gray horizontal line) in Figure 9.1. If a research investment over that same decade could reduce losses from such an attack to $10-billion and the cost of deployment of the new technology and systems could be supported as meeting the conventional needs of the system, then the value of the research in this case could be roughly $100 million (see gray curved line at vertical axis).

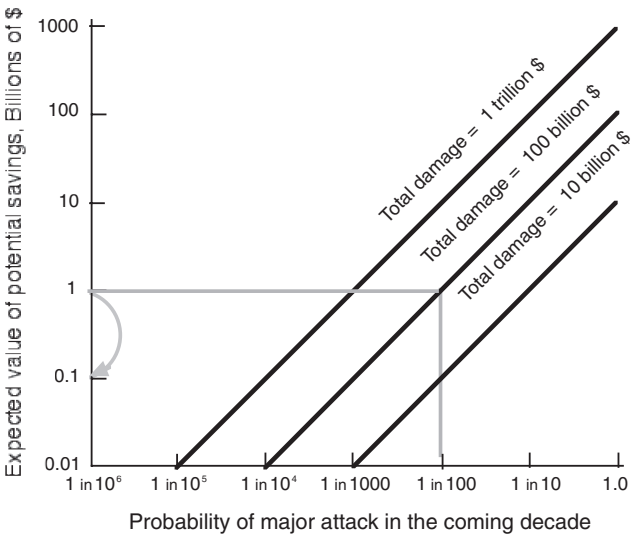


FIGURE 9.1 Diagrammatic means for estimating potential terrorist attack cost mitigation resulting from investment in R&D.

Of course, new technical knowledge alone is not sufficient. Knowledge must also be put to work in the form of deployed systems. Those investments are typically much larger than the investments required to do the research. However, given the conclusion reached above in this chapter—that to a first order, much of the research needed to better prepare to deal with terrorism is very similar to the research needed to make general improvements and upgrades to the power delivery system—much of the cost of implementation might well be justified by other societal needs.

In 2004, the Electric Power Research Institute (EPRI) did an extensive analysis of the costs of making all of the improvements needed to deploy the advanced technologies detailed in this chapter. (EPRI, 2004). EPRI estimated that the power sector was spending about $18 billion per year (in 2004 $) on capital investments in the transmission and distribution system and that an additional expenditure of $165 billion over 20 years, or $ 8.3 billion per year, would be needed to fully deploy the technologies relevant to enhancing the resilience and functionality of the power delivery system. To develop these technologies so that they are available for deployment, the committee believes that an additional R&D investment of approximately 10 percent of those additional expenditures, or $800 million per year, over current funding levels would be needed. This amount is in addition to investments in R&D targeted at power generation or environmental sciences.

BOX 9.1
Questionnaire Respondents' Views on General R&D Needs for the Power Delivery System Needed Specifically to Address Terrorism

In gathering input for Chapter 9, the Committee on Enhancing the Robustness and Resilience of Electrical Transmission and Distribution in the United States to Terrorist Attack prepared and circulated a questionnaire to industry and academic experts in transmission and distribution R&D needs, including several members of the committee. The questionnaire first asked respondents to allocate a *research budget*[1] across the research areas shown in Table 9.1 and then across the technologies listed for each area, "considering all the needs and objectives of the U.S. electric power transmission and distribution system." Respondents were asked to think about "(1) the importance of the area to the future operation of the U.S. electric power system, and (2) how easy it would be to make progress in each area (i.e., the marginal returns per R&D dollar invested)." After completing the first part of the questionnaire, respondents were asked to go through the same tasks again, this time considering "*only* the need to improve the security and reliability of the U.S. electric power transmission and distribution system." Respondents were asked to rate the technologies listed in Table 9.1 as to their potential importance in enhancing the resilience of the nation's power delivery infrastructure.

Based on responses to the questionnaire, the following technologies were viewed as high-priority R&D goals by most experts:

- High-voltage recovery transformers;
- Systems to improve operator awareness and system visualization;
- Advanced demand response based on dynamic systems;
- Multi-layer control strategies;
- Distributed control and recovery;
- Distributed generation and micro-grids;
- Low-cost undergrounding techniques;
- Physically robust/resilient poles, conductors, etc.;
- Solid-state transformers;
- Smart meters;
- Distribution power electronic devices;
- Advanced relaying and protection;
- Advanced failure detection and location; and
- Improved distributed storage.

Most of the R&D priorities identified by questionnaire respondents showed little differentiation between those needed for improving today's system *without* a specific focus on the risk of terrorism and those identified with such a focus. However, when the focus was countermeasures to the risk of terrorism, the following emerged as clearly more important:

- High-voltage recovery transformers,
- Systems to improve operator awareness and system visualization,
- Advanced demand response based on dynamic systems,

FUNDING RESEARCH AND DEVELOPMENT

Current Situation and Challenges

Judicious investments in research and development of pertinent technologies can help to enhance the quality of human life and better serve society's needs, as well as reducing the costs of increasing the capacity of the transmission and distribution systems to handle increasing loads. A balanced, cost-effective approach to investment in R&D and to the subsequent use of technology can make a sizable difference in mitigating risks.

R&D on electricity transmission and distribution in the United States is conducted by a variety of organizations. The U.S. DOE has a significant effort aimed at a select group of technologies, primarily concerning electric power transmission technologies, and especially focusing on superconductivity for cables and short-circuit current limiters. EPRI has a substantial effort, funded both by U.S. utilities and by institutions from as many as 30 other countries. Other national efforts, supported by DOE, EPRI, utilities, and several equipment suppliers, are carried out through organizations like the Power System Engineering Research Center (PSERC) and the Consortium for Electric Reliability

- Multilayer control strategies (including capabilities to island and to self-heal), and
- Improved distributed storage.

In general, while respondents acknowledged that improving end-use energy efficiency would reduce stress on the electric power infrastructure, they nearly uniformly felt that R&D related to reliability, demand response, control, hardening the system, and recovery had priority over reducing the stress on the system by decreasing demand through enhancing efficiency.

In addition to the needs described above for development of technologies, systems, and software, respondents identified several other "nonhardware" research topics.

Public Perception of Risk

Although there is considerable literature about the general public's perception of risk, very little research has been done on reactions to blackouts, whether caused by natural disasters, equipment failure, or terrorism. A team of researchers could be prepared to be deployed within hours following such an event. One goal of the work would be to develop protocols for responding effectively to major disruptions of the power supply, so that the public would be kept informed and made aware of constructive steps to take.

Lessons Learned from Blackouts

A research team organized by the Department of Homeland Security (DHS) and deployed following blackouts could learn about efforts made by utilities, government officials, business leaders, and others to respond in resilient ways.

Public Response

The organizational structure employed and the effort made to communicate with the public following a significant terrorist attack on the power system need to be addressed. In particular, managing the public response to distress could contribute substantially to mitigating the loss of life and the discomfort experienced by the public following a terrorist attack on the power system. DHS could develop guidelines for communications under these conditions.

Market Disruptions

DHS could consider research into the unique problems that could result from terrorist attacks on the power system in areas where centralized markets exists. Disruption of markets can be as difficult to deal with as problems with the physical electric system and could lead to chaos if the potential consequences and countermeasures are not thought out in advance. Such work should develop guidelines for market operators to use in the event of market disruption.

As the respondents reallocated priorities for R&D related to security, they tended to decrease funding for all other items.

[1]No precise budget was specified, but respondents were told "if your allocation would depend on how much money you have available and for how long, assume you have $400 million per year for at least the next decade."

Technology Solutions (CERTS). The manufacturers of the electrical apparatus and equipment used in power systems also conduct research related to development of new equipment. Most of these efforts are modest and are conducted outside the United States. Smaller firms increasingly are developing technologies that are digitally based and intended for potential deployment on power systems.

In addition, individual utilities sponsor some R&D projects, but these internal R&D budgets and R&D staffs are only a fraction of what they were in the mid-1990s. Two states have substantial R&D programs. The California Energy Commission (CEC) has a major transmission research effort underway. The New York State Energy Research and Development Authority (NYSERDA) has complementary work underway as well.

Nationally, a temporary R&D tax credit enacted as part of the Economic Recovery Tax Act of 1981 has been extended several times, although the R&D tax credit that expired on December 31, 2005, was not renewed until December 2006, resulting in a 1-year gap. In recent years, support for R&D investment has been constricted by a number of factors, including reduced federal funding and the cost pressures on private industry. As a result, it has become increasingly important that there be renewed support for research funding.

It is also essential that support for necessary improvements to the U.S. electric power delivery system be continuous in this critical time. The tax credit provision strengthens the innovation, productivity, and competitiveness of the U.S. economy and is vital to U.S. leadership in technological innovation and global competitiveness in the 21st century.

Many of the technologies described above are not yet sufficiently developed to be attractive private sector research investments toward deployable products and systems, even with tax credits. Others are still too expensive or do not have the level of functionality required for wide adoption, even though they may provide substantial benefits to society as a whole.

The current level of R&D funding in both the public and private sectors of the electric industry is at an all-time low. Neither the utility industry nor the electrical apparatus industry is spending as much as could be justified by the expected benefits of improved technology, particularly for longer-term research. The committee believes that a much larger annual R&D investment is required in order for today's transmission and distribution technologies to evolve and for the necessary new technologies to become realities.

In trying to be responsive to their stakeholders, utilities typically tend to limit R&D to areas of immediate application and payback. Aside from these short-term developments, utilities have little incentive to invest in R&D for the longer term. Furthermore, for regulated investor-owned utilities, there is the additional pressure caused by Wall Street to sustain and increase dividends. In addition, during the restructuring of the last decade a substantial number of utilities agreed to rate caps, which, in the face of ongoing cost increases, put pressure on what were perceived as discretionary budget items such as R&D. Government is likely to be the only source of funding for basic and long-term R&D. Therefore, this research is unlikely to be undertaken unless the government significantly increases funding for electric transmission and distribution R&D.

There have been various attempts in regulatory proceedings to encourage or establish increased levels of R&D investments. The results from such efforts have been mixed. In some cases, funds have been used for economic development activities or local demonstrations of already commercially available technology, activities that contribute little to stimulating the innovations in science and technology that are needed. Usually, developments by any one state are not sufficient to influence the market for technology. Collaborative programs have had more success in this regard; however, states have difficulty in funding any research outside their state.

In addition, the enthusiasm among state regulators to encourage higher levels of R&D for the utilities they regulate is tempered by the difficulty of providing strong business cases for R&D—the results of which are inherently unpredictable. Moreover, investments in R&D often require patience before longer-term paybacks are realized. Yet another difficulty in encouraging R&D concerns the phenomenon of "free-rider" utilities, so-called because they take advantage of R&D done by others—often while participating in collaborative arrangements. Such free-riders inhibit some entities from joining collaborative efforts.

In addition to problems with state mandates and underinvestment in the industry, research priorities differ by utility and by region. The extent to which utilities have staff capable of managing research activities also varies, as does the strength of their connections with local universities, national and commercial laboratories, and national research organizations.

Low levels of support for R&D have led to dramatic shrinkage in university programs in power systems. For a while the field was seen by many electrical engineering (EE) departments as uninteresting. Today, with all the new developments underway, that is no longer true. However, when having to choose between hiring an assistant professor in power engineering who might manage to secure research support of a few hundred thousand dollars per year, and an assistant professor in a field such as micro-electronics who might succeed in securing research support in excess of a million dollars per year, EE department heads have been understandably reluctant to replace retiring power engineers or add new junior faculty in this area. The result has been a growing shortage of people with strong technical capabilities in this field.

Societal benefits from adequate R&D investment in the electric power delivery system could extend far beyond the benefits from enhancing the resilience of the power system. These include the economic benefits from enhancing the depth of research in the United States overall and the enhancements in overall productivity. A modern power delivery system is critical to supporting the nation's future and will not evolve without increased R&D.

A Possible Path Forward

To achieve the level of R&D expenditure discussed above, R&D budgets would have to be increased substantially both in industry and by the federal government. To date, no agreement has been reached by the diverse players in the power industry, political decision makers, or society as a whole on a strategy to secure funding at a level to adequately address research needs in the electricity industry. This committee likewise found total agreement hard to attain, with all but a few members of the committee agreeing that federal legislation and regulations should be pursued that can achieve the following goals for the electric power sector:[3]

[3]The committee did not achieve consensus on the need for substantial additional federal funding because of the following issues: a) as a mature industry, electric power companies and suppliers should be able to fund their own research; b) rapidly expanding grids in other countries should provide ample incentives for new developments; and (c) much of the underlying R&D is done by other industries (e.g,, communications and information

- A coherent national plan for increasing both public and private sector R&D funding to address electricity needs;
- An increase in the current level of U.S. R&D (public and private) to $10 billion per year. While somewhat speculative, this amount is approximately three times the current level of R&D, but only about 3 percent of total U.S. R&D, only about 0.1 percent of U.S. annual GDP, and less than 5 percent of annual utility revenue;
- An approximate doubling of federal electricity R&D budgets, increases that should not be burdened with further earmarks;
- A federally legislated requirement that the electricity industry's share of this increase for R&D should come from consumers;
- Specification by such a mandate that 3 percent of the amount charged on a consumer's electricity bill be directed to R&D. Existing programs and R&D budgets that meet the criteria outlined below should be awarded the funds raised by the 3 percent levy. The program should be designed to require each and every industry or market participant[4] to invest 3 percent of the value-added portion of their revenues annually in R&D as defined below. Value-added should be defined as follows:
  - —For the generation portion, it should be the total cost of generation.
  - —For the transmission ownership portion, it should be the transmission wires charge.
  - —For the transmission operations portion, it should be the cost of operations.
  - —For the distribution portion, it should be the distribution wires charge.
  - —For the retail service provider, it should be the marginal cost of services provided to the consumer.
- Structuring of the program to ensure that the amount invested in R&D is fully recoverable from consumers according to a method that involves every U.S. provider and consumer in as fair and equitable a manner as possible. Consumers generally are the intended beneficiaries of the outcomes of the needed R&D and ultimately must pay the bill;
- Management of the investments in R&D by the industry participant (1) to conduct R&D directly itself or to contract such work to a for-profit research provider or (2) to fund R&D performed by nonprofit research institutions, national public-private collaborations, or state and federal government entities, such as national laboratories;
- Regular open review of each individual industry participant's R&D portfolio by a consortium of its stakeholders to obtain input on research direction and priorities;
- Exclusion of activities from the proposed R&D program according to the definition by the Internal Revenue Service, which is as follows: "Scientific research does not include activities of a type ordinarily carried on as an incident to commercial or industrial operations, as, for example, the ordinary testing or inspection of materials or products or the designing or construction of equipment, buildings, etc." (Treasury, 1986);
- Oversight of the program by an appropriate combination of accountability authorities—such as state energy regulatory commissions, the Federal Energy Regulatory Commission, or the Internal Revenue Service—charged with ensuring that research dollars are being applied to their intended targets. To facilitate tracking, appropriate accounting systems will have to be implemented;
- A 10-year sunset and review embedded into the program design.

The committee recognizes the potential for a variety of pitfalls in a program with the general objectives outlined above. If they are not carefully crafted, such programs also can be subject to abuse. Accordingly, the committee recommends that an executive branch agency be charged with developing a proposal that addresses the issues in implementing such a program.

ALTERNATIVE VIEWS OF HOW POWER SYSTEMS COULD EVOLVE

In large measure, today's electric power system can be viewed as comprising more than 130 cohesive electrical zones. These zones have evolved based on utilities' efforts to meet the growth in electrical load by locating generating facilities reasonably close to customer load centers and arranging a network of electric transmission and distribution systems (wires, breakers, transformers, and so on) to meet customer needs. These zones were tied together over time (interconnected) to enhance reliability and to enable the most cost-effective and efficient use of generation. Many zones are considered "control areas" and are controlled in an independent way that includes coordination with other control areas in a region. Today's control areas could be described as being partially independent while being integrated with neighboring control areas.

The configuration of today's power system is based largely on central station power plants located in control areas. The power delivery system that integrates these power

technology) which the electric industry should be able to adapt and apply without more federal spending. Most committee members conclude that the needed R&D will not take place on a useful schedule without more federal involvement.

[4]This includes vertically integrated utilities, power generators, transmission owners, transmission operators, distribution utilities, and retail providers (where they are active).

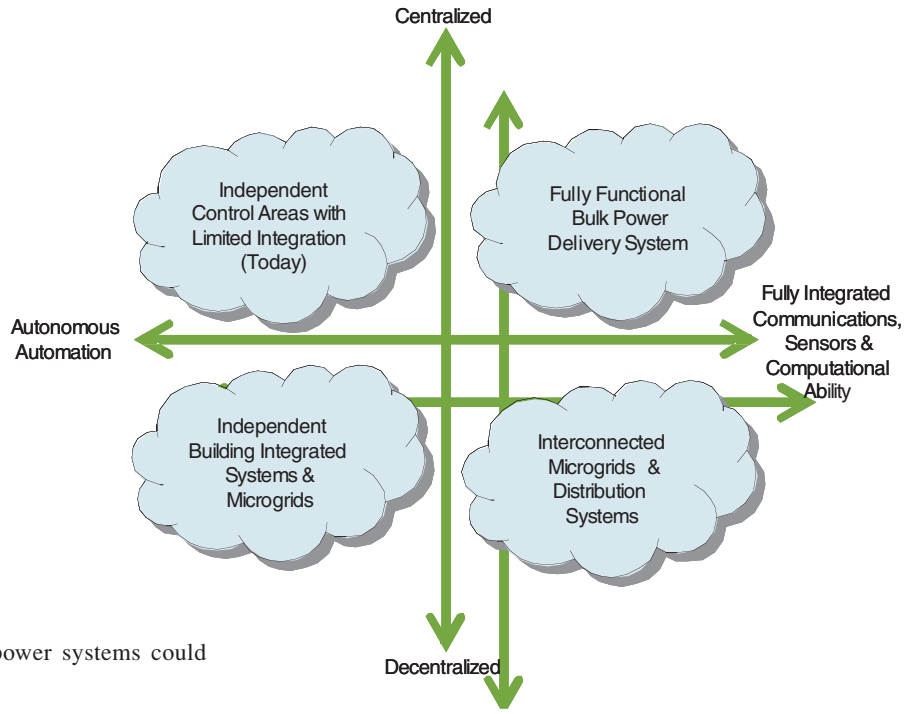


FIGURE 9.2 Alternative ways in which power systems could evolve.

production facilities with consumers is constrained, as evidenced by the growing number of failed wholesale transactions. In addition, the power delivery system is mechanically controlled with only limited integration of communications, automation, or computational ability. Figure 9.2 depicts the potential evolution of today's power system along two dominant dimensions—one the degree of centralization, the other the degree of system integration—fully integrated communications, sensors, and computational ability vs. greater autonomy depending on how automation occurs.

In this paradigm, the issue of whether tomorrow's power system will become more decentralized or more centralized is the greatest driver. The path taken will affect decisions about which technologies to pursue most vigorously, but the committee does not recommend one approach over the other.

The Decentralized Approach

The basic philosophy in the decentralized approach is to first increase the independence, flexibility, and intelligence of local systems for optimization of energy use and energy management at the local level, and then to integrate local systems as necessary or justified for delivering power supply and services that consumers desire. Four configurations are associated with a decentralized approach:

- Device-level power systems
- Building-integrated power systems
- Distributed power systems
- Fully integrated power systems

The decentralized approach starts with the notion that consumers increasingly expect energy-consuming devices and appliances to operate optimally. Optimal operation not only potentially enables a highly mobile digital society, but also, once the optimal performance of devices is defined, provides elements of performance which enable, in turn, a building-integrated system. Building-integrated systems can also accommodate increasing consumer demands for independence, convenience, appearance, environmentally friendly service, and cost control.

Building-integrated systems can, in turn, be integrated into distributed systems, which can then be interconnected and integrated with technologies that ultimately enable a fully integrated national-scale "perfect" power system (Figure 9.3). Note that such systems could be restricted in terms of their rating size and might not have the advantage of economies of scale that current interconnected centralized systems have. Each configuration in this approach reflects a distributed level of both instrumentation and control and would require a complementary set of milestones on the path to comprehensive national power system perfection.

The four different configurations reflect development of the system in two important dimensions:

- *Level of intelligence and energy capacity in distributed devices and systems.* Increased investment in local intelligence and infrastructure also accelerates progress through entrepreneurial leadership opportunities not initially available at higher levels of system integration.

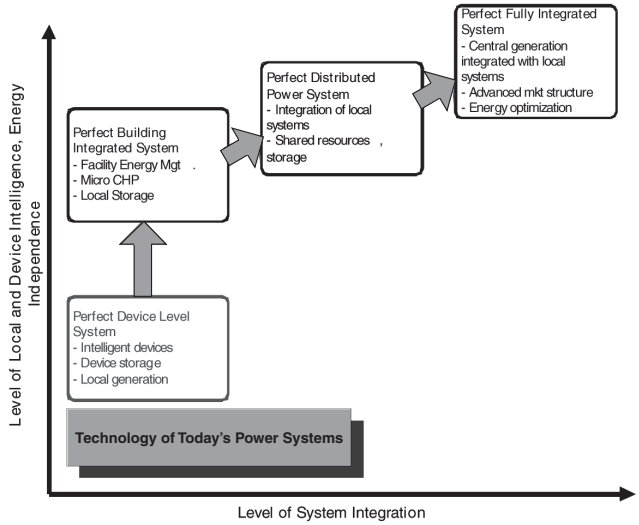


FIGURE 9.3 Development path for the perfect power system. SOURCE: Galvin Electricity Initiative (2006).

- *Level of integration of the entire power delivery infrastructure.* Higher levels of integration require ever more significant transformation of the infrastructure for communications and control, as well as of the overall power delivery infrastructure.

Each of these configurations can essentially be considered a possible structure for a future power system in its own right, but each stage logically evolves to the next stage based on the efficiencies, and the quality or service value improvements, to be attained. In effect, these potential system configuration stages build on each other starting from a device-level power system connected to other device-level power systems that then can evolve into a building-integrated power system, a distributed power system, and eventually a fully integrated power system as diagrammed in Figure 9.4. Figure 9.4 also highlights technologies that would have to be further developed for this concept to evolve.

The optimum configuration may vary for different environments. For instance, the availability of inexpensive and clean central generation (e.g., advanced coal, advanced nuclear, advanced hydro, and large wind systems) may accelerate the migration to the fully integrated stage, whereas other service systems developing from new portable, localized, or distributed infrastructures may achieve their final optimum in the distributed structure.

In a stochastic simulation of a completely decentralized system, Zerriffi (2004) showed that such systems could achieve dramatic improvements in power delivery reliability in the face of system disruptions (see also Farrell et al., 2004). Although no civilian system has approached this level of decentralization, some military systems have begun to evolve toward it.

Distributed systems have also become attractive to those concerned with energy efficiency and reducing CO_2 emissions, because it is typically possible to operate them as high-efficiency combined heat and power systems. The net energy use efficiency of such systems can be twice that of central stations in which "waste" heat must be disposed of via cooling towers. Recent analysis by King (2006) suggests that even with current technology and rate structures, micro-grids could be cost attractive in some applications. However, there are significant regulatory barriers that must be addressed if such systems are to become widespread (King, 2006; Morgan and Zerriffi, 2002).

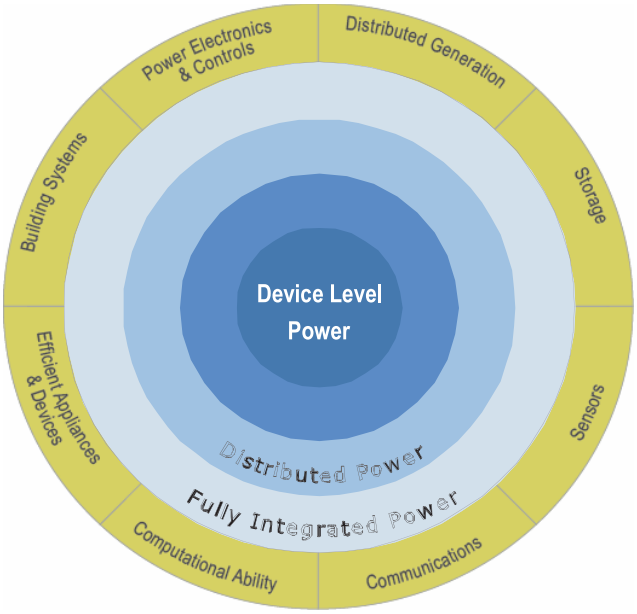


FIGURE 9.4 Evolution of possible configurations (from center outward) and relevant nodes of innovation (in outer ring) enabling the power system. SOURCE: Galvin Electricity Initiative (2006).

The Centralized Approach

The centralized approach assumes that the creation of an intelligent electricity power delivery infrastructure will evolve from the existing power system through bottom-up transformation created by individual companies adding advanced capabilities piece by piece onto the existing grid.

The basis of this transformation is that over the last few decades, advances in diverse technologies—solid-state electronics, microprocessors, sensors, communications, and information technology (IT)—have transformed society and commerce, permanently increasing society's capabilities and expectations. These advances also present new opportunities for operating and using the electric power network, opportunities not envisioned when the power delivery system was first formed. For the power system itself, there is the possibility of creating a nimbler, more flexible network that marries electric power with cutting-edge communication and computing capabilities—an intelligent system that can

predict power problems before they get out of hand and heal itself when damage is unavoidable.

Another aspect of an intelligent system is the ability to fully utilize existing assets through greater system control and flexibility, along with new concepts of designing for high reliability. Opportunities for improving the overall efficiency of the power system equipment use and operation, while still maintaining reliability, are possible in areas such as a dense urban environment, where existing assets are located in close proximity but are often not fully employed.

For electricity customers, a smart power system means not only enhanced power reliability and security but also new services that can add value by giving customers options for control of use, and thus the cost of electricity. For example, customers may be able to monitor their building or industrial-process energy use in real time, choose from a menu of service packages to best fit their energy needs and use patterns, and even sell excess electricity from distributed generation back to their power provider. The promise of a smart power delivery system clearly carries advantages for utilities and consumers.

The change to an intelligent digital system will come from the gradual confluence of innovative projects undertaken by individual companies, rather than through a sudden transformation. Although the new smart devices and technologies developed for these projects will be of value individually, the greater benefit to the power network will be realized only when they all work together. Ensuring that the individual sensing, communications, and computing equipment installed over the coming years can be integrated with other systems and, eventually, come together to form a single system requires an overall power network architecture—that is, common methods and tools for planning and designing the smart systems, and a complete suite of standards. For this purpose, current information technology has some shortcomings. Architecture and standards for power systems have to include consideration of how the legacy systems can be preserved and integrated.

At present, more than 150 different communications protocols are used in the U.S. electric utility industry. Interoperability in today's environment is thus impossible. The industry and the federal government have begun to recognize this deficiency and have initiated several efforts to formulate an architecture that could underpin a smart power system.

These various approaches all rely, in one way or another, on one or more innovative technologies. Many of these technologies have not been fully researched, developed, or demonstrated.

FINDINGS AND RECOMMENDATIONS

Findings

Currently available technology can and should be used more extensively to protect the power delivery system against terrorists, disgruntled employees, or severe natural disasters. There are, however, serious limits (both economic and technical) to how much protection current technology can provide. Advanced technology can raise these limits significantly. The committee's assessment of the status of research and development for the electric power delivery system led it to draw the following general findings.

Finding 9.1 Even in the absence of terrorist attacks, current and projected future inadequacies in the electric power delivery system are likely to result in deteriorating reliability, excessive instances of degraded power quality, and the inability to provide enhanced services to consumers.[5] Inadequate investments in this infrastructure and growing demand for electric power have led to an increasingly stressed system.

Finding 9.2 Underinvestment in R&D for the electric power delivery system has been even more pronounced than underinvestment in the infrastructure. New technologies and techniques are not being developed that could overcome stresses and reduce the cost of delivering electric power to meet the new and growing needs to which the system must respond.

Finding 9.3 There is considerable overlap between the R&D needed to reduce vulnerability to terrorist attack and the R&D that can address the challenges already faced by the power delivery system. An R&D strategy for the power delivery system focused exclusively on terrorism is likely to be less cost-effective and less successful than an integrated strategy to address all the needs and challenges confronting the system, including those posed by terrorism.

Finding 9.4 EPRI, DOE, and a number of utilities and corporations have all engaged in R&D road mapping exercises for the electric power delivery system. The most critical needs are already well identified, and a much larger and more comprehensive R&D program could be created rapidly. The elements of this program are listed in Table 9.1. A more extensive list is shown in Appendix H. DOE would have primary responsibility for most of this program.

Recommendations for R&D to Reduce Vulnerability to Terrorism

DHS should cooperate with DOE to support the following parts of an enhanced R&D program for electric power transmission and distribution to harden the system against terrorism, mitigate the impacts of terrorist acts, and enhance recovery.

Recommendation 9.1 Complete the development and demonstration of high-voltage recovery transformers, and

[5]See also Chapters 2, 6, and 7.

develop plans for the manufacture, storage, and installation of these recovery transformers.

Recommendation 9.2 Continue the development and demonstration of the advanced computational system currently funded by the Department of Homeland Security and underway at the Electric Power Research Institute. This system is intended to assist in supporting more rapid estimation of the state of the system and broader system analysis.

Recommendation 9.3 Develop a visualization system for transmission control centers which will support informed operator decision making and reduce vulnerability to human errors. R&D to this end is underway at the Electric Power Research Institute, Department of Energy, Consortium for Electric Reliability Technology Solutions, and Power System Engineering Research Center, but improved integration of these efforts is required.

Recommendation 9.4 Develop dynamic systems technology in conjunction with response demonstrations now being outlined as part of an energy efficiency initiative being formed by EPRI, the Edison Electric Institute, and DOE. These systems would allow interactive control of consumer loads.

Recommendation 9.5 Develop multilayer control strategies that include capabilities to island and self-heal the power delivery system. This program should involve close cooperation with the electric power industry, building on work in the Wide Area Management System, the Wide Area Control System, and the Eastern Interconnection Phasor Project.

Recommendation 9.6 Develop improved energy storage that can be deployed as dispersed systems. The committee thinks that improved lithium-ion batteries have the greatest potential. The development of such batteries, which might become commercially viable through use in plug-in hybrid electric vehicles, should be accelerated.

The committee believes that electric power R&D budgets should be increased substantially, although there was no consensus as to the appropriate source of the funding. Resolution might come as a result of considering research policy options: What are the impacts if the funding comes from the government, or from private industry, or from some combination thereof? One possibility is a federally mandated program constructed such that each industry participant invests some fraction (say 3 percent) of the value-added portion of its revenues annually in R&D, that the expense is fully recoverable, and that the cost is allocated to every U.S. provider and consumer as fairly and equitably as possible. DHS should work with DOE and the Office of Management and Budget to substantially increase the level of federal basic technology research investment in power delivery.

REFERENCES

EPRI (Electric Power Research Institute). 2004. "Power Delivery System of the Future: A Preliminary Study of Costs and Benefits." Palo Alto, Calif.: EPRI.

Farrell, A.E., H. Zerriffi, and H. Dowlatabad. 2004. "Energy Infrastructure and Security." *Annual Review of Environment and Resources* 29: 421–469.

Galvin Electricity. 2006. *Phase 1 Summary, The Galvin Electricity Initiative*. Available at www.galvinelectricity.org.

King, D.E. 2006. "Electric Power Micro-grids: Opportunities and Challenges for an Emerging Distributed Energy Architecture." Ph.D. Thesis, Department of Engineering and Public Policy, Carnegie Mellon University, Pittsburgh, Pa.

Morgan, M.G., and H. Zerriffi. 2002. "The Regulatory Environment for Small Independent Micro-Grid Companies." *Electricity Journal* 15(9): 52–57.

Treasury (U.S. Department of the Treasury). 1986. Scientific Research Under IRC 501(c)(3). Treasury Regulation 1.501(c)(3)-1(d)(5)(ii). Available at http://www.irs.gov/pub/irs-tege/eotopico86.pdf. Accessed November 2007.

Zerriffi, H. 2004. "Electric Power Systems Under Stress: An Evaluation of Centralized Versus Distributed System Architectures." Ph.D. Thesis, Department of Engineering and Public Policy, Carnegie Mellon University, Pittsburgh, Pa.

10

Recommendations

Disruption of the U.S. power system can impose great economic costs, and in some circumstance can endanger lives. However, power outages have in general not given rise to "terror," even on the part of those affected.

Chapter 1 identifies five different types of individuals and subnational groups that might wish to attack the transmission or distribution system. Of these, the one of greatest concern for this report is terrorist groups with significant capabilities and resources whose intent is to kill large numbers of people or cause widespread societal damage or harm.

Although there are many examples of terrorist and military attacks on power systems elsewhere in the world, to date international terrorists have shown limited interest in attacking the U.S. power grid. However, that should not be a basis for complacency. An attack that disrupted power across a wide geographic region and for an extended period could impose costs of *hundreds of billions of dollars*. If such attacks were repeated several times, or undertaken in conjunction with more conventional terrorist attacks designed to kill people, their impact could be considerably magnified.

Because electric power transmission and distribution systems are spread all across the country, often in very remote locations, they are vulnerable to attack. As explained in Chapter 2, this vulnerability is exacerbated by the fact that, after years of underinvestment, these systems are already under stress and are now facing new demands for wheeling power in a competitive market that the system was not designed to support. As the discussions in Chapters 3, 4, and 5 make clear, knowledgeable terrorists could inflict considerable damage.

Chapters 6 and 7 explain that many of the modifications needed to reduce vulnerability are improvements that should be made to upgrade the system even without any threat of terrorism. Utilities, federal and state regulators, and others are gradually figuring out how to provide the needed incentives and cover the costs of such improvements in the new restructured industry.

There are also a variety of upgrades and redesigns that could be undertaken primarily to make the system more robust in the face of terrorism and to facilitate rapid recovery should an attack occur. But prioritizing and paying for such changes poses significant methodological and institutional challenges. First, expensive upgrades undertaken primarily in response to the threat of terrorism should be made only after a careful quantitative probabilistic assessment of costs and benefits. Second, the risk from terrorism faced by most individual utilities is smaller than the collective risk faced by U.S. society as a whole. Thus, the level of protective investment that may be optimal from the perspective of the national interest may be significantly higher than the level that makes sense for individual firms. This problem is not unique to the power industry, and it is a problem that has not yet been adequately addressed for any of this country's vulnerable infrastructures that are owned and operated by private firms.

In the case of electric power delivery, there are several areas where federal funding is clearly justified and where adequate preparation for possible terrorist attacks is not likely to occur without federal involvement. The most obvious of these is investment in the development, construction, and stockpiling of compact, easily transported high-voltage restoration transformers and other key equipment of long delivery time. Conventional high-voltage transformers are the single most vulnerable component of the transmission and distribution system. They are difficult to move, not stockpiled in great numbers, and for the most part no longer made in this country. Acquiring new ones could take months or even longer if a substantial number were needed. Through the Electric Power Research Institute (EPRI), the industry has done initial design work on a compact, easily transported replacement transformer. However, the development, construction, and stockpiling of a significant number of these devices will almost certainly not occur without substantial federal support and funding.

Clearly, U.S. utilities and state and federal governments should take all reasonable steps to ensure that the nation's

transmission and distribution systems are robust in the face of possible attack and can be rapidly restored if such an attack does ever occur. But that alone is not sufficient. Our society continues to become ever more dependent on electric power. Even without the threat of terrorism, there is a risk of occasional power outages, some of which will be widespread and may last for some time. Terrorism increases the probability of both the extent and the duration of such outages and could cause them to occur at particularly inconvenient or damaging moments. Thus, in addition to strengthening the grid, society should also focus on identifying critical services and developing strategies to keep them operating in the event of power outages—be they accidental or the result of terrorist attack. These issues are discussed in Chapter 8, and recommendations are offered there to reduce future vulnerability.

There are many technologies and strategies that could be employed to make the power system more robust in the face of terrorist attack, speed service restoration after an attack, and continue the provision of critical services while the power is out. They all cost money, often much more money than society can afford. The best way to make existing approaches cheaper, and to develop new, even more effective and affordable approaches, is through research. Chapter 9 discusses the current state of research for electric power and presents a set of recommendations for research needs and strategies. Two key points became apparent as the committee explored these issues. First, with only a few exceptions, the research that is needed to address the broad problems faced by the transmission and distribution system, and the research that would be conducted specifically to address the threat of terrorism, are largely the same, and the latter cannot be adequately undertaken without a balanced and comprehensive approach to the former. Second, measured in a number of ways, the current level of power system research investment is *much* smaller than it should be. This deficiency has long been recognized by those who work in and with the industry. However, agreeing on institutional arrangements that can significantly increase the levels of research investment in this field has been a persistent problem. Chapter 9 notes one possible strategy, but the committee did not have a unanimous view on how best to proceed.

Details on specific research needs can be found in the discussion in Chapter 9.

In the sections below, the recommendations from Chapters 6 through 9 are sorted according to the agency or institution that should take primary responsibility for handling the issue.

SPECIFIC RECOMMENDATIONS FOR THE DEPARTMENT OF HOMELAND SECURITY

The Department of Homeland Security (DHS) should develop a strategy to assess how secure inherently vulnerable infrastructure (such as the electric power delivery system) should be made from the perspective of the collective national interest.

Because the level of security that is economically rational for most infrastructure operators will be less than the level that is optimal from the perspective of the collective national interest, the DHS should develop a coherent plan to address the incremental cost of upgrading and protecting critical infrastructure to that higher level.

In the specific context of electric power delivery, the DHS should:

- **Recommendation 1** Take the lead and work with the DOE and with relevant private parties to develop and stockpile a family of easily transported high-voltage recovery transformers and other key equipment. Although the expected benefits to the nation of such a program are difficult to quantify, they would certainly be many times its cost if the transformers are needed (see Chapters 3, 6, and 9).
- **Recommendation 2** Work to promote the adoption of many other technologies and organizational changes, identified in this report, that could reduce the vulnerability of the power delivery system and facilitate its more rapid restoration should an attack occur (see Chapters 6 and 7).
- **Recommendation 3** Work with the power industry to better clarify the role of power system operators after terrorist events through the development of memoranda of understanding and planned and rehearsed response programs that include designating appropriate power-system personnel as first responders (see Chapters 7 and 8).
- **Recommendation 4** Offer assistance to the Federal Energy Regulatory Commission, to state public service commissions, and to other public and private parties in finding ways to ensure that utilities and transmission operators have appropriate incentives to accelerate the process of upgrading power delivery and eliminating its most obvious vulnerabilities (see Chapter 6).
- **Recommendation 5** Work with the Department of Energy and the Office of Management and Budget to substantially increase the level of federal basic technology research investment in power delivery. The committee notes that (1) much of what is needed has the nature of a "public good" that the private sector will not develop on its own; (2) current levels of research investment are woefully inadequate; and (3) most of the system's vulnerabilities to terrorism are integrally linked to other more general problems and vulnerabilities of the system and cannot be resolved in isolation (see Chapter 9).
- **Recommendation 6** Take the lead in initiating planning at the state and local level to reduce the vulnerability of critical services in the event of disruption

of conventional power supplies, and offer pilot and incremental funding to implement these activities where appropriate (see Chapter 8).

- **Recommendation 7** Develop a national inventory of portable generation equipment that can be used to power critical loads during an extended outage. Explore public and private strategies for building and maintaining an adequate inventory of such equipment (see Chapter 8).

ADDITIONAL RECOMMENDATIONS

While the seven recommendations listed above are the committee's primary recommendations to DHS, other specific recommendations are made in Chapters 6 through 9, both to DHS and to other key players. These are reproduced below sorted by responsible actor and ordered approximately in terms of how long the completion of each action will likely require.

There is one other subject on which the committee does not make a recommendation but considers that a comment is in order. Chapter 5 notes that the power industry faces a more serious aging-workforce problem than that confronting many U.S. industries. There are growing shortages among both the craft and engineering workforce. This issue is also discussed briefly in the context of graduate education and research in Chapter 9. Although the committee makes no specific recommendations on these issues, it is clear that, without significant attention, the problem of inadequate human resources will become increasingly serious and over time could make it more difficult to achieve the various objectives outlined in this report. The industry itself will have to take the lead in addressing the shortage of craft workers, taking steps to persuade new entrants to the job market that a career in power systems is interesting and attractive. DOE, the National Science Foundation, and Congress could all help to address the shortages in the engineering workforce through expanded programs of graduate fellowship and research support. In addition, DHS would be well advised to examine potential restrictions in visa programs that might dissuade students from entering the United States to study power engineering, or staying to work in the U.S. power industry or research universities once they have graduated. Given the imminent shortages of skilled engineers, there are security concerns associated with restrictions that are too tight as well as those that are too loose.

Additional Recommendations Primarily for Active Participation by DHS

The list below focuses on actions DHS could take, usually in conjunction with DOE. Actions for other agencies and parties follow.

Recommendation 7.4 The Department of Homeland Security and the Edison Electric Institute should jointly develop programs and offer training for key utility personnel to respond to both conventional security threats and potential chemical or biological attacks on the electric infrastructure. The training should use risk assessments to develop increased awareness of the possible threats and should provide specific training for the use of protection equipment, detection and sensor equipment, and emergency decontamination procedures. It is essential that existing drills and restoration procedures be expanded to address potential biological or chemical agents which may be part of an attack launched to disrupt electric operations and infrastructures. *Time Scale for Action: 1–3 Years*

Recommendation 6.4 Local load-serving entities should work with local private and public sector groups to identify critical customers and plan a series of technical and organizational arrangements that can facilitate restricted service to critical customers during times of system stress. DHS could accelerate this process by initiating and partially funding a few local and regional demonstrations that could provide examples of best practice for other regions across the country. *Time Scale for Action: 2 years*

Recommendation 8.1 DHS and/or DOE should initiate and fund several model demonstration assessments each at the level of cities, counties, and states. These assessments should examine systematically the region's vulnerability to extended power outages and develop cost-effective strategies that can be adopted to reduce or, over time, eliminate such vulnerabilities. These model assessments should involve all relevant public and private sector parties providing law enforcement, water, gas, sewerage, health care, communications, transportation, fuel supply, banking, and food supply. These assessments should include a consideration of outages of long duration ($\geq$ several weeks) and large geographic extent (over several states) because the response required to deal with such outages would differ greatly from those needed to deal with shorter-duration events (hours to a few days). *Time Scale for Action: 3–5 years.*

Recommendation 8.2 Building on the results of these model assessments, DHS should develop, test, and disseminate guidelines and tools to assist cities, counties, states, and regions to conduct their own assessments, and develop plans to reduce their vulnerabilities to extended power outages. DHS should also develop guidance for individuals to help them understand steps they can take to better prepare for and reduce their vulnerability in the event of extended blackouts. *Time Scale for Action: 3–5 years.*

Recommendation 8.6 DHS should perform, or assist other federal agencies to perform, additional systematic assessment of the vulnerability of national infrastructure such as

telecommunications and air traffic control in the face of extended and widespread loss of electric power, and then develop and implement strategies to reduce or eliminate vulnerabilities. Part of this work should include an assessment of the available surge capacity for large mobile generation sources. Such an assessment should include an examination of the feasibility of utilizing alternative sources of temporary power generation to meet emergency generation requirements (as identified by state, territorial, and local governments, the private sector, and nongovernmental organizations) in the event of a large-scale power outage of long duration. Such assessment should also include an examination of equipment availability, sources of power generation (mobile truck-mounted generators, naval and commercial ships, power barges, locomotives, and so on), transportation logistics, and system interconnection. When areas of potential shortages have been identified, plans should be developed and implemented to take corrective action and develop needed resource inventories, stockpiles, and mobilization plans. *Time Scale for Action: 2 Years (Assessments), 2–5 Years (Response Plans).*

Recommendations Primarily for Utilities, System Operators, and Law Enforcement

Recommendation 7.2 Utilities, governments at the federal, state, and local level, and law enforcement agencies should develop official memoranda of understanding (MOUs) that spell out each party's responsibilities before, during, and immediately following deliberate destruction of utility equipment that leads to a disruption of electric service. These MOUs should provide a clear understanding of who is in charge and explain how decisions will be reached in dealing with potential tensions between crime scene investigation and timely restoration of service, as well as with unanticipated contingencies. The MOUs should also help to ensure the appropriate allocation of resources and should address concerns about potential government seizure of utility supplies and equipment during catastrophic events, which can seriously hinder a utility's prompt restoration of electric service. *Time Scale for Action: 6 Months.*

Recommendation 7.5 DHS with DOE and the Electric Reliability Organization should work with utilities that have not yet done so to:

- Establish a team reporting to top management that coordinates physical, cyber, and operations security through comprehensive plans that clearly define what is expected of security personnel before, during, and after a deliberate destructive act; identifies the technologies and strategies to be used to continuously monitor critical company facilities; and establishes an Incident Command System and designates an incident commander to work with outside agencies. *Time Scale for Action: 6 Months.*
- Examine their internal radio communications systems to determine that battery backup systems and portable generators are in place to ensure that all communication devices will remain operational during a crisis. Because traditional communication systems may become unavailable during a destructive attack on the electric system, options such as satellite communications should be evaluated (and periodically tested) for potential use as backup communication. *Time Scale for Action: 6 Months.*
- Assess black-start capabilities in their systems under the assumption that major physical disruption of the transmission system can occur, develop appropriate contingency plans, and test both the plans and the equipment on a regular basis. *Time Scale for Action: 6 Months.*
- Assess the potential for the cascading collapse of long stretches of transmission line, and, where appropriate, include offsetting towers at various intervals, or reinforce or upgrade towers at more frequent intervals along the line. *Time Scale for Action: 6 Months.*

Recommendations Primarily for Congress and/or State Legislatures

Recommendation 7.3 State and federal law or regulations should be modified to:

- Recognize utilities as essential service providers so that relevant utility employees will be trained and legally designated as first responders to deal with attacks on the power system. *Time Scale for Action: 1 Year.*
- Provide utilities, when needed, with temporary exemptions from laws that restrict their use of equipment and their access to roads, materials, supplies, and other critical elements for restoration of electric service to essential loads, including those that have an impact on public health and safety. *Time Scale for Action: 1 Year.*
- Ensure that state regulatory agencies support prudent efforts by utilities to commit and acquire the necessary resources for service restoration and that they provide reasonable assurance for recovery of these costs. *Time Scale for Action: 1 Year.*

Recommendation 7.6 State legislatures should change utility law to explicitly allow micro-grids with distributed generation. IEEE should revise its standards to include the appropriate use of islanded distributed generation and micro-grid resources for local islanding in emergency recovery operations. Utilities should reexamine and, if necessary, revise their distribution automation plans and capabilities in light of the possible need to selectively serve critical loads during extended restoration efforts. Public utility commis-

sions should consider the potential emergency restoration benefits of distribution automation when they review utility applications involving such investments. *Time Scale for Action: 2 Years.*

Recommendation 8.4 Congress, DHS, and the states should provide resources and incentives to cover incremental costs associated with private and public sector risk prevention and mitigation efforts to reduce the societal impact of an extended grid outage. Such incentives could include incremental funding for those aspects of systems that provide a public good but little private benefit, R&D support for new and emerging technology that will enhance the resiliency and restoration of the grid, and the development and implementation of building codes or ordinances that require alternate or backup sources of electric power for key facilities. *Time Scale for Action: 2–5 Years.*

Recommendations Primarily for Standards-setting Groups

Recommendation 6.1 The ERO should require power companies to reexamine their critical substations to identify serious vulnerabilities to terrorist attack. Where such vulnerabilities are discovered, physical and cyber protection should be applied. In addition, the design of these substations should be modified with the goal of making them more flexible to allow for efficient reconfiguration in the event of a malicious attack on the power system. The bus configurations in these substations could have a significant impact on the capacity for maintaining reliability in the event of a malicious attack on the power system. Bus layout or configuration could be a significant factor if a transformer, circuit breaker, instrument transformer, or bus work is blown up, possibly damaging nearby equipment. *Time Scale for Action: 1 Year (Assessment), 3–10 Years (Upgrades).*

Recommendation 6.2 The ERO and FERC should direct greater attention to vulnerability to multiple outages (e.g., *N*–2) planned by an intelligent adversary. In cases where major, long-term outages are possible, reinforcements should be considered as long as costs are commensurate with the reduction of vulnerability and other possible benefits. The ERO and FERC should direct greater attention at vulnerability due to multiple outages (e.g., *N*–2) planned by an intelligent adversary. Since necessary reinforcements will entail significant costs, just how far systems should move in this direction will depend on a careful quantitative probabilistic assessment of costs and benefits. *Time Scale for Action: 1–3 Years.*

Recommendation 6.3 The ERO and FERC should develop best practices and standards for improving system-wide instrumentation and the ability of near-real-time state estimation and security assessments, since otherwise operators are at a disadvantage in trying to understand and manage system disruptions as they unfold. *Time Scale for Action: 1–3 Years.*

Recommendations Primarily for State Government, Regions, and Communities

Recommendation 8.3 State and local regions should undertake regional and local vulnerability assessments, building on the models provided by DHS, develop plans to collaboratively implement key strategies to reduce vulnerability, and assist private sector parties and individuals to identify steps they can take to reduce their vulnerabilities. *Time Scale for Action: 1–3 Years.*

Recommendation 8.5 Federal and state agencies should identify legal barriers to data access, communications, and collaborative planning that could impede appropriate regional and local assessment and contingency planning for handling long-term outages. Political leaders of the jurisdictions involved should analyze the data security and privacy protection laws of their agencies with an eye to easing obstacles to collective planning and to facilitating smooth communication in a national or more localized emergency. *Time Scale for Action: 1–3 Years.*

Recommendations Primarily for DOE, EPRI, and Other Research Organizations

Recommendation 9.1 Complete the development and demonstration of high-voltage recovery transformers, and develop plans for the manufacture, storage, and installation of these recovery transformers (also see Recommendation 1 above).

Recommendation 9.2 Continue the development and demonstration of the advanced computational system currently funded by the Department of Homeland Security and underway at the Electric Power Research Institute. This system is intended to assist in supporting more rapid estimation of the state of the system and broader system analysis.

Recommendation 9.3 Develop for transmission control centers a visualization system that will support informed operator decision making and reduce vulnerability to human errors. R&D to this end is underway at the Electric Power Research Institute, Department of Energy, Consortium for Electric Reliability Technology Solutions, and Power System Engineering Research Center, but improved integration of these efforts is required.

Recommendation 9.4 Develop dynamic systems technology in conjunction with response demonstrations now being outlined as part of an energy efficiency initiative being developed by EPRI, the Edison Electric Institute, and DOE.

These dynamic systems would allow interactive control of consumer loads.

Recommendation 9.5 Develop multilayer control strategies that include capabilities to island and self-heal the power delivery system. This program should involve close cooperation with the electric power industry, building on work in the Wide Area Management System (WAMS), the Wide Area Control System (WACS), and the Eastern Interconnection Phasor Project (EIPP).

Recommendation 9.6 Develop improved energy storage that can be deployed as dispersed systems. The committee thinks that improved lithium-ion batteries have the greatest potential. The development of such batteries, which might become commercially viable through use in plug-in hybrid electric vehicles, should be accelerated.

Appendixes

The appendixes provide information on this project and additional details and background information for the material in the report.

- *Appendix A:* Statement of Task
- *Appendix B:* Committee Biographical Information
- *Appendix C:* List of Presentations and Committee Meetings
- *Appendix D*: Acronyms
- *Appendix E:* Summary of NERC Cyber Security Standards
- *Appendix F:* Substation Configurations
- *Appendix G:* Controlling Power Systems
- *Appendix H:* R&D Needs for the Power Delivery System

A

Statement of Task

The National Academies' National Research Council (NRC) will establish a committee of about 18 individuals. The committee will consider approaches to reducing the vulnerability, enhancing the robustness, and improving the resilience and ability to recover of future electrical transmission and distribution (T&D) in the United States to potential terrorist attacks. The committee will use as a starting point the three recent reports addressing electric T&D in the nation, namely, the National Academies' report *Making the Nation Safer: The Role of Science and Technology in Countering Terrorism*; the DOE report *Grid 2030, A National Vision for Electricity Second 100 Years*; and the EPRI report *Electricity Sector Framework for the Future*. The study will address technical, policy, and institutional factors that may affect the evolution of electrical T&D in the United States in the midterm (e.g., 3 to 10 years) and the long term (10 to 25 years). The committee will identify priority technology opportunities, R&D directions, policy and institutional actions, and strategies that will lead to more secure electrical T&D in the face of an uncertain future. The committee will write a report documenting its findings and recommendations. In particular, the committee will likely include the following in its activities:

(1) Examination of the current status of electricity T&D in the United States with the aim of identifying significant technological opportunities that can reduce vulnerability or enhance robustness to potential terrorist attack. The committee can draw on various recent studies (noted above) by DOE, EPRI, and the National Academies on electricity T&D in the United States, and also on other perspectives that may arrive at different conclusions than these studies.

(2) As part of its data-gathering activities, and in order to elicit a wide array of perspectives on how electric T&D and supply in the United States may evolve and the different approaches to reducing the impact of potential terrorist attacks, the committee will invite presentations from electric power industry groups, federal and state representatives, nonprofit groups, consumer groups, small companies, and others. The committee will review the various perspectives vis-à-vis the vision that has been laid out in the DOE and EPRI studies (noted above) as at least one point of reference. The committee will likely organize itself into working subgroups to entertain these presentations and promote discussion on selected issues, such as technology, policies, and institutional issues. The committee may also include a workshop(s) as part of its early data-gathering activities to help the committee focus on the priority issues and questions that need to be answered for its study.

(3) Given that the future evolution of electric T&D in the United States is uncertain, the committee may develop a range of scenarios, considering factors affecting future requirements for the nation's T&D infrastructure, including the need for new capacity, replacement needs, siting issues, vulnerability to terrorism, and the effects of interconnectedness among regional networks.

(4) The committee will analyze the likely implications for the vulnerability, robustness, and recovery and resilience of electrical T&D to potential terrorist attacks in the midterm (3 to 10 years) as well as the long term (10 to 25 years) with an eye on science and technology investment.

(5) Analyze how existing and emerging technological options could improve the reliability, security, robustness, and the ability to recover from disruptions to the electrical T&D system, or systems, and prioritize technical opportunities and R&D needs.

(6) Recommend strategies for implementing the transition from the current situation to a future system that is less vulnerable to disruption from terrorist attack, considering primarily technical barriers.

(7) Write a final report documenting its findings and recommendations.

The National Research Council will issue a final report approximately 15 to 18 months from the time funds are received to initiate the study.

B

Committee Biographical Information

M. Granger Morgan (NAS), *Chair*, is the Lord Chair Professor in Engineering; a professor and the department head, Engineering and Public Policy; a professor in electrical and computer engineering; and a professor in the H. John Heinz III School of Public Policy and Management, Carnegie Mellon University (CMU). Dr. Morgan's research interests are focused on policy problems in which technical and scientific issues play a central role. Methodological interests include problems in the integrated analysis of large complex systems; problems in the characterization and treatment of uncertainty; problems in the improvement of regulation; and selected issues in risk analysis and risk communication. Application areas of current interest include global climate change; the future of the energy system, especially electric power; risk analysis, including risk ranking; health and environmental impacts of energy systems; security aspects of engineered civil systems; national R&D policy; radio interference on commercial airliners; issues of privacy and anonymity; and a number of general policy, management, and manpower problems involving science and technology. Most of Dr. Morgan's professional career has been spent at CMU with short stints at Brookhaven National Laboratory, the National Science Foundation, and University of California, San Diego. His professional activities include a large number of publications, memberships on numerous panels, including the EPA Science Advisory Board and the EPRI Advisory Board, both of which he chairs, and NRC committee work. Dr. Morgan is a member of the National Academy of Sciences. He has a B.A. in physics from Harvard University, an M.S. in astronomy and space science from Cornell University, and a Ph.D. in applied physics and information science from the University of California at San Diego.

Massoud Amin is a professor of electrical and computer engineering, holds the H.W. Sweatt Chair in Technological Leadership, and is the director of the Center for the Development of Technological Leadership at the University of Minnesota in the Twin Cities. His research focuses on global transition dynamics to enhance the resilience and security of national critical infrastructures. Prior to joining the University of Minnesota in March 2003, for 5 years Dr. Amin held positions of increasing responsibility, including area manager of infrastructure security, grid operations/planning, and energy markets at the Electric Power Research Institute (EPRI) in Palo Alto, California. In the aftermath of the tragic events of 9/11, he directed all security-related research and development at EPRI, including the Infrastructure Security Initiative (ISI) and Enterprise Information Security (EIS). Prior to October 2001, he served as manager of mathematics and information science at EPRI, where he led strategic research in modeling, simulation, optimization, and adaptive control of national infrastructures for energy, telecommunication, transportation, and finance. Dr. Amin is the author or co-author of more than 120 research papers, is the editor of seven collections of manuscripts, and serves on the editorial boards of four academic journals. Dr. Amin holds B.S. (cum laude) and M.S. degrees in electrical and computer engineering from the University of Massachusetts-Amherst, and M.S. and D.Sc. degrees in systems science and mathematics from Washington University in St. Louis, Missouri.

Edward V. Badolato was president and CEO of Integrated Infrastructure Analytics Inc. Previously, he was executive vice president for homeland security of the Shaw Group. Prior to that, Mr. Badolato was president of Contingency Management Services Inc., a security, energy, and environmental emergency-consulting firm. He has spent much time in these positions assessing the vulnerability of a variety of energy infrastructure facilities and assets. He served for 4 years at the U.S. Department of Energy (DOE) as Deputy Assistant Secretary for Energy Emergencies and International Affairs, where he was principal director of international energy affairs, energy contingency planning, crisis management, and security matters. During that period, he was the principal architect of the federal government's nuclear weapons security programs as well as its conven-

tional energy emergency preparedness activities. At DOE, he was also in charge of the Strategic Petroleum Reserve and led the federal fact-finding team to Alaska to gather information on the Exxon Valdez oil spill for the President. While serving in the U.S. Marine Corps, he was a military attaché to a number of Middle Eastern countries. He has also led a number of response teams to deal with oil/gas production and pipeline accidents. He has published numerous articles on energy and security and is a member of the Board of Advisors for the Association of Counterterrorism and Security Professionals and the Institute of Gas Technology. He is a member of the Institute of International Energy Economists and the American Society of Industrial Security. He is an adjunct faculty member at Georgetown University's Graduate Business School.

William O. Ball is senior vice president, transmission planning and operations, Southern Company Services. In this role, Mr. Ball is responsible for the planning and operations of the Southern electric systems network transmission grid, transmission policy, and industry interfaces. He is a board member of the Southeastern Electric Reliability Council (SERC), a member of the North American Electric Reliability Council (NERC) Stakeholders Committee, and a member of the Advisory Board of the Consortium for Electric Reliability. Prior to his current appointment, Mr. Ball was vice president of transmission planning, policy, and support services with responsibility for transmission planning, policy, and industry interfaces, and business unit finance and accounting. From January 2001 to March 2002, Mr. Ball was vice president of technical support at Mirant (formerly Southern Energy). In this role, his responsibilities included technical due diligence on business development projects, providing transmission support and O&M support to the various business units, and establishing and implementing safety and health policy at Mirant. From 1999 to 2001, Mr. Ball held the position of director of technical support at Southern Energy, where he was responsible for ensuring that proper technical due diligence was performed on business development projects. From 1995 to 1999, he held the position of manager, system planning, with both generation and transmission planning responsibilities at Mississippi Power Company (MPC). Mr. Ball played a key role in the development and certification of the MPC 1,100 MW combined cycle facility at Plant Daniel. He also served as MPC's technical witness in numerous regulatory hearings concerning retail access. Mr. Ball's earlier roles included a position in the transmission planning department developing transmission pricing methods, developing Southern's first open-access transmission tariffs, and providing transmission policy recommendations and negotiated transmission service contracts with third parties. He also worked on the development of Southern's Clean Air Act compliance strategy and has worked in the areas of distribution engineering, system planning, and bulk power contracts. Mr. Ball is a summa cum laude graduate of Mississippi State University with a bachelor's degree in electrical engineering. He also holds a master's of business administration from the University of Southern Mississippi. Mr. Ball is a registered professional engineer.

Anjan Bose (**NAE**) holds the endowed Distinguished Professor of Electric Power Engineering in the College of Engineering and Architecture at Washington State University (WSU) and is the director of the NSF-sponsored Power Systems Engineering Research Center. From 1998 until 2006, he was dean of the College of Engineering and Architecture, and from 1993 until 1998, he was director of the School of Electrical Engineering and Computer Science. Dr. Bose's research interests are in power grid control through computer technology. Prior to joining WSU, he was on the faculty of Arizona State University and, before that, the Control Data Corporation. He is a member of the National Academy of Engineering, has received several awards from IEEE over the years, and is a member of several professional societies. He was appointed by the Governor of Washington to the board of directors of the Washington Technology Center (and is now serving as vice-chair of the board), and by the U.S. Secretary of Energy to the committee to study the 1999 power blackouts. He has consulted for many electric power companies and related government agencies throughout the world and has extensive experience in the Western Interconnection of the United States. He has a Ph.D. in electrical engineering from Iowa State University.

Clark W. Gellings is vice president of innovation at the Electric Power Research Institute. He has been at EPRI since 1982; prior to that he was with Public Service Electric and Gas Company in New Jersey. Mr. Gellings is both an electrical and a mechanical engineer with a strong background in the development of new products and services for the energy industry, especially applied to the power industry. He has many accomplishments in developing systems for demand side management, optimal and cost-effective utility management, and applying digital technology in the power sector in order to gain efficiencies in generation, dispatching, and end use. He is a member of numerous professional associations and has received many prizes for his work over the years. He has authored or co-authored more than 400 articles or papers and 10 books. He has an M.S. in mechanical engineering from the New Jersey Institute of Technology, an M.S. in management science from Stevens Institute of Technology, and a B.S. in electrical engineering from the Newark College of Engineering.

Michehl R. Gent serves on several policy committees and boards, including the United States Energy Association board and the IEEE-USA Energy Policy Committee. Formerly, Mr. Gent was president and CEO of the North American Electric Reliability Council (NERC). He joined NERC

in 1980 as executive vice president and was elected president in 1982. Prior to joining NERC, he was general manager of the Florida Electric Power Coordinating Group—a voluntary power pool for Florida's electric utilities. Before that, he held several positions in both operations and planning at the Los Angeles Department of Water & Power. He earned a BSEE at Texas A&M and an MSEE at the University of Southern California (USC). He has taught in the graduate schools of USC and Loyola and is a registered professional engineer.

Diane Munns is executive director, Retail Energy Services, Edison Electric Institute. Until January 2007, she served on the three-member Iowa Utilities Board following her appointment in June 1999 after 15 years of service as a regulatory attorney. She was chair of the board from October 2001 until March 10, 2005; her current term as a member ends April 30, 2009. Ms. Munns assumed the presidency of the National Association of Regulatory Utility Commissioners (NARUC) in mid-term 2005 for a term running through 2006. She is a member of the Committee on Electricity and of the Executive Committee and serves on the board of directors. She is a past chair of the NARUC Committee on Finance and Technology. She serves on the Advisory Council to the board of directors of the Electric Power Research Institute, is a member of the Advisory Council of the New Mexico State University Center for Public Utilities, and serves on the Energy Board of the Keystone Center of Science and Public Policy. Ms. Munns is also co-chair of the Leadership Group for the Energy Efficiency Action Plan for the EPA. She has served on the Executive Committee for the Organization of MISO States Inc. Ms. Munns received her bachelor's degree from the University of Iowa and her law degree from Drake University.

Sharon L. Nelson retired as chief of the Consumer Protection Division of the Washington State Attorney General's Office in 2006. She also served as director of the Shidler Center for Law, Commerce, and Technology at the University of Washington School of Law from 2000 to 2003, as chair of the Washington State Utilities and Transportation Commission from 1985 to 1997 and as president of the National Association of Regulatory Utility Commissioners from 1989 to 1990. She serves on the boards of Consumers Union, Itron, and the North American Reliablity Corporation. She is a commissioner on the bipartisan National Commission on Energy Policy. She received her B.A. from Carleton College, M.A.T. from the University of Chicago, and J.D. from the University of Washington.

David K. Owens is executive vice president, Business Operations, Edison Electric Institute (EEI). Previously, Mr. Owens served as EEI senior vice president of finance, regulation, and power supply policy, focusing on enhancement of industry representation on such issues as the Public Utility Regulatory Policies Act (PURPA), Public Utility Holding Company Act (PUHCA), the Federal Power Act, cogeneration and independent power production, transmission access, and bulk power and transmission pricing. He also has responsibility for representing the industry in the areas of finance, rate making, regulation, accounting, and taxes. Mr. Owens also served as vice president of power supply policy, overseeing work on a broad range of issues related to power supply policy and the regulatory structure of the electric utility industry. He joined EEI in 1980 as director of rates and regulation. His responsibilities included coordinating industry positions on rate-related matters before federal, executive, and congressional committees. Prior to joining EEI, Mr. Owens served as chief engineer of the Division of Corporate Regulation of the Securities and Exchange Commission, a division responsible for regulating public utility holding companies. Mr. Owens also was an engineer in the Division of Rates and Corporate Regulation at the former Federal Power Commission and worked as a design and a test engineer for General Electric and Philadelphia Electric Companies, respectively. He is a member of the National Research Council's Board on Energy and Environmental Systems. Mr. Owens holds B.S. and M.S. degrees in engineering from Howard University and an M.S. in engineering administration from George Washington University.

Louis L. Rana is president and chief operating officer of Consolidated Edison Company of New York, a position to which he was elected effective September 1, 2005. Mr. Rana joined Con Edison in 1969 and has held positions of increasing responsibility in electric operations, system operations, and engineering. From February 2003 until his election as president, Mr. Rana was senior vice president of Electric Operations, with overall responsibility for the operation and maintenance of the company's electric system in New York City and Westchester County. He was appointed chief engineer of Distribution Engineering in 1993. He served as general manager of Manhattan Electric Operations in 1997 and was general manager of System Operations during 1997 and 1998. Mr. Rana was named vice president of System and Transmission Planning in 1998 and vice president of Manhattan Electric Operations in 2000. Mr. Rana is a member of the Institute of Electrical and Electronics Engineers (IEEE) and the Research Advisory Committee for the Electric Power Research Institute. He received a B.S. in engineering from Stevens Institute of Technology, an M.S. in electrical engineering from the New Jersey Institute of Technology, and an M.B.A. from Columbia University. Mr. Rana is a licensed professional engineer.

B. Don Russell Jr. (NAE) is Regents Professor in the Department of Electrical and Computer Engineering at Texas A&M University. His research interests are in electric power engineering, power systems protection, control, and computer automation. His policy interests are in energy systems and economics. He is also the director of the Texas

A&M Power Systems Automation Laboratory. Prior to his current appointment, he held several key positions in the Texas A&M system, including associate vice chancellor for engineering research, executive associate dean of the College of Engineering, and deputy director of the Texas Engineering Experiment Station. His industrial interests include the presidency of Power Solutions, an engineering design firm. Dr. Russell has received a number of IEEE awards, including the Herman Halperin Transmission and Distribution Award, and he is a fellow of five professional societies. He is past president of the IEEE Power Engineering Society. Dr. Russell is also a member of the National Academy of Engineering. He has B.S. and M.E. degrees in electrical engineering from Texas A&M University and a Ph.D. in electrical engineering from the University of Oklahoma.

Richard E. Schuler is a P.E. in electrical engineering and has been a professor of economics and of civil and environmental engineering at Cornell University since 1972, where he has also been an adjunct professor in the Johnson Graduate School of Management since 1991. His research focuses on the role of infrastructure in supporting modern societies, including its organization, management, regulation, and pricing and its regional economic and environmental impact. Using both analytic and experimental techniques, he has worked extensively on developing efficient markets for reliable, deregulated electricity supplies that incorporate proper customer participation while encouraging needed investment. Together with colleagues from the Santa Fe Institute, he is also using numerical methods to explore the optimal structure of organizations in the information age. From 1995 to 2001, he directed the Institute for Public Affairs and Cornell's MPA program, and he helped form and directed the Cornell Waste Management Institute from 1987 to 1993, during which time he was also associate director of Cornell's Center for the Environment. Previously, Dr. Schuler served as a Public Service Commissioner in New York State (1981–1983), as an energy consultant with Battelle Memorial Institute (1967–1968), and as an engineer and manager with the Pennsylvania Power and Light Co. (1959–1967). He has served as a faculty-elected trustee of Cornell University from 1994 to 1998, during which time the board appointed him to its executive committee, and, since its formation in 1998, he has been a member of the board of directors of the New York Independent System Operator (responsible for operating the state's electricity system reliably and conducting an efficient wholesale market), where he chairs the Market Performance Committee. Dr. Schuler's degrees are a B.E. in electrical engineering from Yale University in 1959, an M.B.A. in business from Lehigh University in 1969, and a Ph.D. in economics from Brown University in 1972.

Philip R. Sharp is president of Resources for the Future. A member of the U.S. House of Representatives from 1975 to 1995, Sharp took key leadership roles in the development of landmark energy legislation. He helped to develop a critical part of the 1990 Clean Air Act Amendments and was a driving force behind the Energy Policy Act of 1992. Following his decision not to seek an 11th consecutive term in the House, Sharp joined Harvard's Kennedy School of Government, where he was a Lecturer in Public Policy from 1995 to 2001. He served as Director of Harvard's Institute of Politics from 1995 to 1998 and again from 2004 until August 2005 and was a Senior Research Fellow in the Environmental and Natural Resources Program from 2001 to 2003. Sharp served on the Board of Directors of the Cinergy Corporation from 1995 to 2006 and on the Board of the Electric Power Research Institute from 2002 to 2006. He also chaired advisory committees for the Massachusetts Institute of Technology (MIT) studies on the future of nuclear power and the future of coal. Sharp is co-chair of the Energy Board of the Keystone Center and serves on the Board of Directors of the Duke Energy Corporation and the Energy Foundation. He is also a member of the Cummins Science and Technology Advisory Council and serves on the Advisory Board of the Institute of Nuclear Power Operations (INPO) and on the External Advisory Board of the MIT Energy Initiative. Sharp received his Ph.D. in government from Georgetown University.

Carson W. Taylor (NAE) is a retired principal engineer for the Bonneville Power Administration, where he had worked since 1969. His background and experience are in R&D of advanced control and operating strategies to increase transmission transfer capability and power systems reliability, and in training in modeling and simulation techniques. He has also been active in investigating power outages, system stability, security issues, and other system anomalies. He is active in IEEE, has received several awards, and publishes books and articles on a variety of power systems subjects. He is also active in training and education, passing on what he has learned through seminars and short courses. He is a member of the National Academy of Engineering. He has a B.S in electrical engineering from the University of Wisconsin-Madison and an M.S. in electric power engineering from the Rensselaer Polytechnic Institute.

Susan F. Tierney is a managing principal at Analysis Group and is an expert on energy policy and economics, especially in the electric and gas industries. Her areas of expertise include electric industry restructuring, market analyses, wholesale and retail market design, market monitoring, contract disputes, resource planning and analysis, asset valuations, regional transmission organizations, the siting of generation and transmission and natural gas pipeline projects, natural gas markets, electric system reliability, and environmental policy and regulation. Prior to joining Analysis Group, she was senior vice president at Lexecon. She has also served as the assistant secretary for policy at the U.S. Department of Energy, appointed by President

Bill Clinton and confirmed by the U.S. Senate. She was also secretary for environmental affairs in Massachusetts under Governor William Weld, and a commissioner at the Massachusetts Department of Public Utilities, to which she was appointed by Governor Michael Dukakis. She was executive director of the Massachusetts Energy Facilities Siting Council. Dr. Tierney has authored numerous articles and speaks frequently at industry conferences. She serves on a number of boards of directors and advisory committees, including the National Commission on Energy Policy. She is chair of the boards of the Energy Foundation and of Clean Air–Cool Planet and is a director of Catalytica Energy Systems Inc., the Northeast States Clean Air Foundation, the Electric Power Research Institute, and the Climate Policy Center. Dr. Tierney is a member of the Harvard Electric Policy Group, the Massachusetts Renewable Energy Trust Advisory Council, the Environmental Advisory Council of the New York Independent System Operator, and the China Sustainable Energy Program's Policy Advisory Council. She was previously chair of the Electricity Innovations Institute and a member of the Advisory Council of the Independent System Operator–New England. She has taught at the University of California at Irvine. Dr. Tierney earned her Ph.D. and M.A. degrees in regional planning at Cornell University and her B.A. at Scripps College.

Vijay Vittal (NAE) is the Ira A. Fulton Professor in the Department of Electrical Engineering at Arizona State University. His research interests are in the area of power system dynamics, dynamic security assessment of power systems, power system operation and control, and application of robust control techniques to power systems. He is the author and co-author of several papers in his field. In 1992, he co-authored the textbook entitled *Power System Transient Stability Assessment Using the Transient Energy Function Method* with A.A. Fouad, and, in 1999, he co-authored the textbook entitled *Power System Analysis* with A.R. Bergen. During 1993–1994 he was the program director of the Power Systems Program at the National Science Foundation. He has been the recipient of several awards, including several from the IEEE, and is a member of the National Academy of Engineering. He received a B.E. in electrical engineering from the B.M.S. College of Engineering, Bangalore, India, in 1977; an M.Tech. degree in electrical engineering from the Indian Institute of Technology, Kanpur, India, in 1979; and a Ph.D. in electrical engineering from Iowa State University, Ames, in 1982.

Paul C. Whitstock is a managing director with Marsh USA Inc., a risk and insurance services firm. He has been active in the energy industry and is well connected with insurance markets specializing in utility and power-generation risks. He is the client executive for several global energy companies and is actively involved in managing and placing insurance programs for large generating asset and transmission system portfolios. As the power and utility practice leader for Marsh's Mid-Atlantic Zone, Mr. Whitstock acts in both a consulting and a brokerage capacity, lending his expertise in such areas as deal facilitation, risk transfer strategies, and traditional and advance risk financing strategies (including weather hedges and energy trading risks). Mr. Whitstock also has extensive experience with construction and commissioning risks associated with large power-generation projects. Mr. Whitstock has a B.S. in business administration from Ithaca College in Ithaca, N.Y. He has also completed a wide array of risk management and insurance courses at the College of Insurance in New York. In 1992, he received his Chartered Property and Casualty Underwriter designation.

C

List of Presentations and Committee Meetings

**1. Committee Meeting, The National Academies, Washington, D.C.
August 15–16, 2005**

Overview of DHS T&D Security Activities and Study Expectations
William Rees Jr., U.S. Department of Homeland Security

Department of Energy Perspective
David Meyer, U.S. Department of Energy

EPRI's T&D Security Work
Robert Schainker, Electric Power Research Institute

Progress on Security Issues at NERC
Michehl R. Gent, North American Electric Reliability Council

An ISO Perspective
Tom Bowe, PJM Interconnection

**2. Committee Meeting, The National Academies, Washington, D.C.
November 29–30, 2005**

Recent NYC Emergency Operations
Lou Rana, Consolidated Edison Company of New York

Recent Emergency Experiences from the Mid-South
William Ball, Southern Company Services

TVA's Program in Reliability
David Hall, Tennessee Valley Authority

U.S.-Canadian Blackout—The Full Story
Dave Nevius, North American Electric Reliability Council

INL's Security Work
Julio Rodriguez, Idaho National Laboratory

Department of Energy Perspective
William Parks, U.S. Department of Energy

**3. Committee Meeting, The National Academies, Washington, D.C.
February 2–3, 2006**

Protecting Electric Power Systems Against Terrorist Attack
Edward V. Badolato, Integrated Infrastructure Analytics Inc.

Distributed Generation: A Local Solution to a National Challenge
Bruce A. Hedman, Energy and Environmental Analysis Inc.

Securing Communications to SCADA Systems
Scott Mix, KEMA Inc.

Grid Vulnerability in Remote Configuration of Generation Controllers: The Threat of Hacking with Megawatts
Christopher L. DeMarco, University of Wisconsin-Madison

The NEMA Perspective
John Caskey, National Electrical Manufacturers Association

Transformer Security Issues
James Fama, Edison Electric Institute

Informal Presentation: The Transfer Issue
David K. Owens, Edison Electric Institute

Cyber Security of Industrial Control Systems and Potential Impacts on the Electric Grid
Joseph Weiss, KEMA Inc. (via telephone)

4. Committee Meeting, Arnold and Mabel Beckman Center, Irvine, California
April 20–21, 2006

Computer/Network Security and Group Communication
Gene Tsudik, University of California, Irvine

Distributed and Emergency Generation: The Caterpillar Perspective
Joseph Fiorito, Caterpillar Inc.

Galvin Architecture
Clark Gellings, Electric Power Research Institute

The California ISO Perspective
David Hawkins, California ISO

5. Closed Committee Meeting, J. Erik Jonnson Woods Hole Center, Woods Hole, Massachusetts
July 24–25, 2006

6. Closed Committee Meeting, The National Academies, Washington, D.C.
October 1–2, 2006

D

Acronyms

AC	alternating current
ADA	advanced distribution automation
ADC	analog-to-digital converter
AEIC	Association of Edison Illuminating Companies
AGA	American Gas Association
AGC	Advanced Generation Control (balances CA generation with CA load)
AMR	automatic meter reading
ANSI	American National Standards Institute
APCO	Association of Public Communications Officers
ASME	American Society of Mechanical Engineers
BA	balancing area
BNSF	Burlington Northern Santa Fe
BPA	Bonneville Power Administration
CA	control area (entity responsible for an electric region)
CCTV	closed circuit television
CIPC	Critical Infrastructure Protection Committee
CERTS	Consortium for Electric Reliability Technologies
CSC	convertible static compensator
CSSWG	Control Systems Security Working Group
DA	distribution automation
DAC	digital-to-analog converter
DAWG	Disturbance Analysis Working Group
DC	direct current
DCS	distributed control system
DER	distributed energy resources
DG	distributed generation
DHS	U.S. Department of Homeland Security
DOD	U.S. Department of Defense
DOE	U.S. Department of Energy
DOJ	U.S. Department of Justice
DOT	U.S. Department of Transportation
DSM	demand-side management
DTCR	dynamic thermal circuit rating
EEI	Edison Electric Institute
EHV	extra-high voltage
EIA	Energy Information Administration
EIPP	Eastern Interconnection Phasor Project
EMP	electromagnetic pulse
EMS	Energy Management System (monitors system frequency and AGC)
EPA	U.S. Environmental Protection Agency
EPAct	Energy Policy Act (most recent was passed by Congress in 2005)
EPRI	Electric Power Research Institute
EPSA	Electric Power Supply Association
ERCOT	Electric Reliability Council of Texas Inc. (RRO)
ERO	Electric Reliability Organization (enforces reliability standards)
ERP	enterprise resource planning
ETAG	Electronic Tagging (Etag) (system used to coordinate the scheduling of energy)
FACTS	flexible AC transmission system
FARC	Fuerzas Armadas Revolucionarias de Colombia
FBI	Federal Bureau of Investigation
FEMA	Federal Emergency Management Agency
FERC	Federal Energy Regulatory Commission (bulk power markets regulator)
FRCC	Florida Reliability Coordinating Council (RRO)
GDP	gross domestic product
GIS	gas-insulated substation

HS-ARPA	U.S. Department of Homeland Security Advanced Research Projects Agency
HSPD	Homeland Security Presidential Directive
I3P	Institute for Information Infrastructure Protection
ICCP	Inter-Control Center Communications Protocol
ICS	Incident Command System
IEC	Israel Electric Corporation
IEC	International Electrotechnical Commission
IED	intelligent electronic device
IEEE	Institute of Electrical and Electronics Engineers
IEIA	International Electricity Infrastructure Assurance Forum
IGBT	insulated gate bipolar transistor
IGCT	insulated gate commuted thyristor
INA	intelligent network agents
INL	Idaho National Laboratory
I/O	input/output
ISO	independent system operator
IT	information technology
MISO	Midwest Independent Transmission System Operator
MMW	Maintenance Management Workstation
MRO	Midwest Reliability Organization RRO
MVA	megavolt ampere
MW	megawatt
NERC	North American Electric Reliability Council
NIMS	National Incident Management System
NIPP	National Infrastructure Protection Plan
NIST	National Institute of Standards and Technology
NOPR	Notice of Proposed Rulemaking (FERC)
NPCC	Northwest Power Coordinating Council (RRO)
NRC	National Research Council
NRECA	National Rural Electric Cooperative Association
NSC	National Security Council
NSTB	National SCADA Test Bed
O&M	operations and maintenance
OASIS	Open Access Same-time Information System (system to reserve transmission capacity)
OTA	Office of Technology Assessment
PA DEP	Pennsylvania Department of Environmental Protection
PCSF	Process Control Systems Forum
PCSRF	Process Control Security Requirements Forum
PID	proportional, integral derivative algorithm
PIM	Pooled Inventory Management (program)
PLC	programmable logic controller
PNL	Pacific Northwest National Laboratory
PPE	personal protective equipment
PRO	Planning and Resource Optimizer
PSERC	Power System Engineering Research Center
PUC	public utility commission
PUHCA	Public Utility Holding Company Act (1934)
PURPA	Public Utility Regulation Policy Act (1978)
R&D	research and development
RC	reliability coordinator
RCWG	Reliability Coordinator Working Group
RFC	Reliability*First* Corporation (RRO)
RFID	radio frequency identification
RRO	regional reliability organization (regional member of NERC)
RTO	regional transmission operator
RTU	remote terminal unit
SAIDI	System Average Interruption Duration Index
SAIFI	System Average Interruption Frequency Index
SCADA	supervisory control and data acquisition
SERC	Southeastern Electric Reliability Council, Inc. (RRO)
SMES	superconducting magnetic energy storage
SNL	Sandia National Laboratory
SOX	Sarbanes-Oxley Act (2002)
SPP	Southwest Power Pool Inc. (RRO)
SPS	special protection systems
STEP	Spare Transformer Equipment Program
T&D	transmission and distribution
TSWG	Technical Support Working Group
TVA	Tennessee Valley Authority (Government-owned utility)
UPFC	unified power flow controller
VAR	volt-ampere reactive
VR	virtual reality
VSC	voltage-sourced converters
WACS	wide-area stability and voltage control system
WAMS	Wide Area Measurement System
WECC	Western Electricity Coordinating Council (RRO)
WHO	World Health Organization

E

Summary of NERC Cyber Security Standards

The stated purpose of mandatory NERC Standards CIP-002 through CIP-009 is to provide a cyber security framework for the identification and protection of critical cyber assets to support reliable operation of the bulk electric system. These standards recognize the differing roles of each entity in the operation of the bulk electric system, the criticality and vulnerability of the assets needed to manage bulk electric system reliability, and the risks to which they are exposed. Responsible entities should interpret and apply Standards CIP-002 through CIP-009 using reasonable business judgment.

Business and operational demands for managing and maintaining a reliable bulk electric system increasingly rely on cyber assets supporting critical reliability functions and processes to communicate with each other, across functions and organizations, for services and data, resulting in increased risks to these cyber assets.

Standard CIP-002 requires the identification and documentation of the critical cyber assets associated with the critical assets that support the reliable operation of the bulk electric system. These critical assets are to be identified through the application of an annual risk-based assessment that identifies and documents the risk-based assessment methodology used to identify critical assets. The responsible entity is required to maintain documentation describing its risk-based assessment methodology that includes procedures and evaluation criteria.

The risk-based assessment shall consider the following assets: control centers and backup control centers; transmission substations that support the reliable operation of the bulk electric system; generation resources that support the reliable operation of the bulk electric system; systems and facilities critical to system restoration, including black-start generators and substations in the electrical path of transmission lines used for initial system restoration; systems and facilities critical to automatic load shedding under a common control system capable of shedding 300 MW or more; special protection systems that support the reliable operation of the bulk electric system; and any additional assets that support the reliable operation of the bulk electric system that the responsible entity deems appropriate to include in its assessment.

Using this list of critical assets, the responsible entity must develop a list of associated critical cyber assets essential to the operation of the critical asset. Examples at control centers and backup control centers include systems and facilities at master and remote sites that provide monitoring and control, automatic generation control, real-time power system modeling, and real-time inter-utility data exchange. Critical cyber assets are further qualified if they have at least one of the following characteristics: the cyber asset uses a routable protocol to communicate outside the electronic security perimeter, or the cyber asset uses a routable protocol within a control center, or the cyber asset is dial-up accessible.

To ensure compliance, a senior manager or delegate(s) must approve annually the list of critical assets and the list of critical cyber assets and keep a signed and dated record of the approval.

SECURITY MANAGEMENT CONTROLS: THREATS AND RISKS

Responsible entities must have minimum security management controls in place to protect critical cyber assets. The first step in complying with this charge is the development and implementation of a cyber security policy that represents management's commitment and ability to secure its critical cyber assets. The responsible entity shall, at a minimum,

NOTE: This appendix provides a modified summary recitation of the NERC cyber security standards, available at http://www.nerc.com/~filez/standards/Reliability_Standards.html#Critical_Infrastructure_Protection (accessed November 2007). These standards have been reformatted and to some degree paraphrased in order to enhance their readability among diverse audiences.

ensure the following: This cyber security policy must be readily available to all personnel who have access to, or are responsible for, critical cyber assets.

The responsible entity must assign a senior manager with overall responsibility for leading and managing the entity's implementation of, and adherence to, the policy. This senior manager shall be identified by name, title, business phone, business address, and date of designation. Changes to the senior manager must be documented within 30 calendar days of the effective date. The senior manager or delegate(s) shall authorize and document any exception from the requirements of the cyber security policy.

Information Protection

The responsible entity shall implement and document a program to identify, classify, and protect information associated with critical cyber assets. The critical cyber asset information to be protected shall include, at a minimum and regardless of media type, operational procedures, lists of critical assets, network topology or similar diagrams, floor plans of computing centers that contain critical cyber assets, equipment layouts of critical cyber assets, disaster recovery plans, incident response plans, and security configuration information.

The responsible entity shall, at least annually, assess adherence to its critical cyber asset information protection program, document the assessment results, and implement an action plan to remediate deficiencies identified during the assessment.

Access Control

The responsible entity must document and implement a program for managing access to protected critical cyber asset information. The responsible entity shall maintain a list of designated personnel who are responsible for authorizing logical or physical access to protected information. Personnel are identified by name, title, business phone, and the information for which they are responsible for authorizing access. At least annually, the responsible entity must review the access privileges to protected information to confirm that access privileges are correct and that they correspond with the responsible entity's needs and appropriate personnel roles and responsibilities.

Change Control and Configuration Management

The responsible entity must establish and document a process of change control and configuration management for adding, modifying, replacing, or removing critical cyber asset hardware or software, and must implement supporting configuration management activities to identify, control, and document all entity- or vendor-related changes to hardware and software components of critical cyber assets pursuant to the change control process.

ELECTRONIC SECURITY PERIMETER(S)

The identification and protection of the electronic security perimeter(s) inside which all critical cyber assets reside, as well as all access points on the perimeter, are required.

Electronic Security Perimeter

The responsible entity must ensure that every critical cyber asset resides within an electronic security perimeter. The responsible entity must identify and document the electronic security perimeter(s) and all access points to the perimeter(s).

1. Access points to the electronic security perimeter(s) must include any externally connected communication end point (for example, dial-up modems) terminating at any device within the electronic security perimeter(s).
2. For a dial-up-accessible critical cyber asset that uses a non-routable protocol, the responsible entity must define an electronic security perimeter for that single access point at the dial-up device.
3. Communication links connecting discrete electronic security perimeters must not be considered part of the electronic security perimeter. However, end points of these communication links within the electronic security perimeter(s) must be considered access points to the electronic security perimeter(s).
4. Any non-critical cyber asset within a defined electronic security perimeter must be identified and protected.
5. Cyber assets used in the access control and monitoring of the electronic security perimeter(s) must be afforded certain protective measures.
6. The responsible entity must maintain documentation on the electronic security perimeter(s), all interconnected critical and non-critical cyber assets within the electronic security perimeter(s), all electronic access points to the electronic security perimeter(s), and the cyber assets deployed for the access control and monitoring of these access points.

Electronic Access Controls

The responsible entity must implement and document the organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the electronic security perimeter(s).

1. These processes and mechanisms must use an access control model that denies access by default, such that explicit access permissions must be specified.
2. At all access points to the electronic security perimeter(s), the responsible entity must enable only ports and services required for operations and for monitoring cyber assets within the electronic security perimeter, and must document, individually or by specified grouping, the configuration of those ports and services.
3. The responsible entity must maintain a procedure for securing dial-up access to the electronic security perimeter(s).
4. Where external interactive access into the electronic security perimeter has been enabled, the responsible entity must implement strong procedural or technical controls at the access points to ensure authenticity of the accessing party, where technically feasible.
5. The required documentation must, at least, identify and describe:
   - The processes for access request and authorization,
   - The authentication methods,
   - The review process for authorization rights, and
   - The controls used to secure dial-up accessible connections.
6. Where technically feasible, electronic access control devices must display an appropriate-use banner on the user screen upon all interactive access attempts. The responsible entity must maintain a document identifying the content of the banner.

Monitoring Electronic Access

The responsible entity must implement and document an electronic or manual process(es) for monitoring and logging access at access points to the electronic security perimeter(s) 24 hours a day, 7 days a week.

1. For dial-up-accessible critical cyber assets that use non-routable protocols, the responsible entity must implement and document monitoring process(es) at each access point to the dial-up device, where technically feasible.
2. Where technically feasible, the security monitoring process(es) must detect and alert for attempts at or actual unauthorized accesses. These alerts must provide for appropriate notification to designated response personnel. Where alerting is not technically feasible, the responsible entity must review or otherwise assess access logs for attempts at or actual unauthorized accesses at least every 90 calendar days.

Cyber Vulnerability Assessment

The responsible entity must perform a cyber vulnerability assessment of the electronic access points to the electronic security perimeter(s) at least annually. The vulnerability assessment must include, at a minimum, the following:

1. A document identifying the vulnerability assessment process;
2. A review to verify that only ports and services required for operations at these access points are enabled;
3. The discovery of all access points to the electronic security perimeter;
4. A review of controls for default accounts, passwords, and network management community strings; and
5. Documentation of the results of the assessment, the action plan to remediate or mitigate vulnerabilities identified in the assessment, and the execution status of that action plan.

Documentation Review and Maintenance

The responsible entity must review, update, and maintain all documentation to support compliance with the requirements, including the following:

1. The responsible entity must ensure that all documentation required reflects current configurations and processes and must review the documents and procedures at least annually.
2. The responsible entity must update the documentation to reflect the modification of the network or controls within 90 calendar days of the change.
3. The responsible entity must retain electronic access logs for at least 90 calendar days. Logs related to reportable incidents must be kept in accordance with the requirements.

INCIDENT REPORTING AND RESPONSE PLANNING

Cyber Security Incident Response Plan

The responsible entity must develop and maintain a cyber security incident response plan. The cyber security incident response plan must address, at a minimum, the following:

1. Procedures to characterize and classify events as reportable cyber security incidents.
2. Response actions, including roles and responsibilities of incident response teams, incident handling procedures, and communication plans.
3. Process for reporting cyber security incidents to the Electricity Sector Information Sharing and Analysis Center (ES ISAC). The responsible entity must

ensure that all reportable cyber security incidents are reported to the ES ISAC either directly or through an intermediary.
4. Process for updating the cyber security incident response plan within 90 calendar days of any changes.
5. Process for ensuring that the cyber security incident response plan is reviewed at least annually.
6. Process for ensuring that the cyber security incident response plan is tested at least annually. A test of the incident response plan can range from a paper drill, to a full operational exercise, to the response to an actual incident.

Cyber Security Incident Documentation

The responsible entity must keep relevant documentation.

PHYSICAL SECURITY OF CRITICAL CYBER ASSETS

The implementation of a physical security program is intended to ensure the protection of critical cyber assets.

Physical Security Plan

The responsible entity must create and maintain a physical security plan, approved by a senior manager or delegate(s), that must address, at a minimum, the following:

1. Processes to ensure and document that all cyber assets within an electronic security perimeter also reside within an identified physical security perimeter. Where a completely enclosed ("six-wall") border cannot be established, the responsible entity must deploy and document alternative measures to control physical access to the critical cyber assets.
2. Processes to identify all access points through each physical security perimeter and measures to control entry at those access points.
3. Processes, tools, and procedures to monitor physical access to the perimeter(s).
4. Procedures for the appropriate use of physical access controls, including visitor pass management, response to loss, and prohibition of inappropriate use of physical access controls.
5. Procedures for reviewing access authorization requests and revocation of access authorization.
6. Procedures for escorted access within the physical security perimeter of personnel not authorized for unescorted access.
7. Process for updating the physical security plan within 90 calendar days of any physical security system redesign or reconfiguration, including, but not limited to, addition or removal of access points through the physical security perimeter, physical access controls, monitoring controls, or logging controls.
8. Means for ensuring that cyber assets used in the access control and monitoring of the physical security perimeter(s) are afforded the same protective measures as other cyber assets.
9. Process for ensuring that the physical security plan is reviewed at least annually.

Physical Access Controls

The responsible entity must document and implement the operational and procedural controls to manage physical access at all access points to the physical security perimeter(s) 24 hours a day, 7 days a week. The responsible entity must implement one or more of the following physical access methods:

1. *Card key*. A means of electronic access whereby the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another.
2. *Special locks*. These include, but are not limited to, locks with "restricted key" systems, magnetic locks that can be operated remotely, and "man-trap" systems.
3. *Security personnel*. Personnel who are responsible for controlling physical access and who might reside on-site or at a monitoring station.
4. *Other authentication devices*. Biometric, keypad, token, or other equivalent devices that control physical access to critical cyber assets.

Monitoring Physical Access

The responsible entity must document and implement the technical and procedural controls for monitoring physical access at all access points to the physical security perimeter(s) 24 hours a day, 7 days a week. Unauthorized access attempts must be reviewed immediately and handled in accordance with established procedures. One or more of the following monitoring methods must be used:

1. *Alarm systems*. Systems that alarm to indicate that a door, gate, or window has been opened without authorization. These alarms must provide for immediate notification to personnel responsible for response.
2. *Human observation of access points*. Monitoring of physical access points by authorized personnel.

Logging Physical Access

Logging must record sufficient information to uniquely identify individuals and the time of access 24 hours a day, 7 days a week. The responsible entity must implement and document the technical and procedural mechanisms for log-

ging physical entry at all access points to the physical security perimeter(s) using one or more of the following logging methods or their equivalent:

1. *Computerized logging*. Electronic logs produced by the responsible entity's selected access control and monitoring method.
2. *Video recording*. Electronic capture of video images of sufficient quality to determine identity.
3. *Manual logging*. A log book, sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access.

Access Log Retention

The responsible entity must retain physical access logs for at least 90 calendar days. Logs related to reportable incidents must be kept in accordance with the requirements of Standard CIP-008.

Maintenance and Testing

The responsible entity must implement a maintenance and testing program to ensure that all physical security systems function properly. The program must include, at a minimum, the following:

1. Testing and maintenance of all physical security mechanisms on a cycle no longer than 3 years.
2. Retention of testing and maintenance records for the proper cycle documented by the responsible entity.
3. Retention of outage records regarding access controls, logging, and monitoring for a minimum of 1 calendar year.

PERSONNEL AND TRAINING

Personnel having authorized cyber or authorized unescorted physical access to critical cyber assets, including contractors and service vendors, are required to have an appropriate level of personnel risk assessment, training, and security awareness.

Awareness

The responsible entity must establish, maintain, and document a security awareness program to ensure that personnel having authorized cyber or authorized unescorted physical access receive ongoing reinforcement in sound security practices. The program must include security awareness reinforcement on at least a quarterly basis using mechanisms such as:

- Direct communications (e.g., e-mails, memos, computer based training, etc.);
- Indirect communications (e.g., posters, intranet, brochures, etc.);
- Management support and reinforcement (e.g., presentations, meetings, etc.).

Training

The responsible entity must establish, maintain, and document an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to critical cyber assets, and review the program annually and update as necessary.

This program will ensure that all personnel having such access to critical cyber assets, including contractors and service vendors, are trained within 90 calendar days of such authorization.

Training must cover the policies, access controls, and procedures as developed for the critical cyber assets and include, at a minimum, the following required items appropriate to personnel roles and responsibilities:

- The proper use of critical cyber assets;
- Physical and electronic access controls to critical cyber assets;
- The proper handling of critical cyber asset information; and
- Action plans and procedures to recover or re-establish critical cyber assets and access thereto following a cyber security incident.

The responsible entity must maintain documentation that training is conducted at least annually, including the date the training was completed and attendance records.

Personnel Risk Assessment

The responsible entity must have a documented personnel risk assessment program, in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements, for personnel having authorized cyber or authorized unescorted physical access. A personnel risk assessment must be conducted pursuant to that program within 30 days of such personnel being granted such access. Such program must at a minimum include the following:

1. The responsible entity must ensure that each assessment conducted includes, at least, identity verification (e.g., Social Security number verification in the United States) and a 7-year criminal check. The responsible entity may conduct more detailed reviews, as permitted by law and subject to existing collective bargaining unit agreements, depending on the criticality of the position.

2. The responsible entity must update each personnel risk assessment at least every 7 years after the initial personnel risk assessment or for cause.
3. The responsible entity must document the results of personnel risk assessments of its personnel having authorized cyber or authorized unescorted physical access to critical cyber assets, and must document that personnel risk assessments of contractor and service vendor personnel with such access are conducted pursuant to Standard CIP-004.

Access

The responsible entity must maintain list(s) of personnel with authorized cyber or authorized unescorted physical access to critical cyber assets, including their specific electronic and physical access rights to critical cyber assets.

- The responsible entity must review quarterly the list(s) of its personnel who have such access to critical cyber assets, and update the list(s) within 7 calendar days of any change of personnel with such access to critical cyber assets, or any change in the access rights of such personnel. The responsible entity must ensure that access list(s) for contractors and service vendors are properly maintained.
- The responsible entity must revoke such access to critical cyber assets within 24 hours for personnel terminated for cause and within 7 calendar days for personnel who no longer require such access to critical cyber assets.

RECOVERY PLANS FOR CRITICAL CYBER ASSETS

Recovery plan(s) must be in place for critical cyber assets, and these plans must follow established business continuity and disaster recovery techniques and practices. The responsible entity must comply with the following requirements.

Recovery Plans

The responsible entity must create and annually review recovery plan(s) for critical cyber assets. The recovery plan(s) must address at a minimum the following:

1. Specify the required actions in response to events or conditions of varying duration and severity that would activate the recovery plan(s).
2. Define the roles and responsibilities of responders.

Exercises

The recovery plan(s) must be exercised at least annually. An exercise of the recovery plan(s) can range from a paper drill, to a full operational exercise, to recovery from an actual incident.

Change Control

Recovery plan(s) must be updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident. Updates must be communicated to personnel responsible for the activation and implementation of the recovery plan(s) within 90 calendar days of the change.

Backup and Restore

The recovery plan(s) must include processes and procedures for the backup and storage of information required to successfully restore critical cyber assets. For example, backups may include spare electronic components or equipment, written documentation of configuration settings, tape backup, etc.

Testing Backup Media

Information essential to recovery that is stored on backup media must be tested at least annually to ensure that the information is available. Testing can be completed off-site.

F

Substation Configurations

In each of the four figures in this appendix, the bus work or node is depicted as a solid line. The squares represent circuit breakers that open the electrical circuit under load or short-circuit conditions. The switches, which have limited ability to interrupt current, serve to isolate components and bus sections.

MAIN AND TRANSFER BUS CONFIGURATION

A main and transfer bus configuration consists of two independent buses, one of which, the main bus, is normally energized. Under normal operating conditions, all incoming and outgoing circuits are fed from the main bus through their associated circuit breakers and switches. If it becomes necessary to remove a circuit breaker from service for maintenance or repairs, circuit operation can be maintained through use of the isolating switches and bus transfer equipment. The circuit breaker to be maintained and its switches are opened, the bus transfer switches are closed, the switch from the transfer bus to the circuit is closed, and then the bus transfer breaker is closed to re-energize the circuit. The circuit is then protected by the bus transfer breaker. Figure F.1 shows the typical configuration of a main and transfer bus scheme.

The main advantages of this scheme include:

- Accommodation of circuit breaker maintenance while maintaining service and line protection;
- Low cost—essentially one breaker per line or transformer;
- Fairly small land area; and
- Easily expandable.

The primary disadvantages of this scheme include the following:

- Failure of a circuit breaker or a bus fault causes loss of the entire bus with outage of all circuits.
- An additional circuit breaker is required for bus tie.
- Since the bus tie breaker has to be able to be substituted for any line breaker, its associated relaying may be complicated.
- Complicated switching is required to remove a circuit breaker from service for maintenance.

The main and transfer bus scheme, which has the potential for a major outage of all circuits, is mainly used in older stations, most often at voltages of 230 kV and below. For large stations, the bus may be broken into two or three sections, with bus-sectionalizing circuit breakers. A bus fault or breaker failure then affects only one section of bus, with the opening of the sectionalizing breakers preventing outages on other bus sections. It is important to distribute circuits onto bus sections in a balanced way, so that sufficient transmission network conductivity remains with a bus section outage.

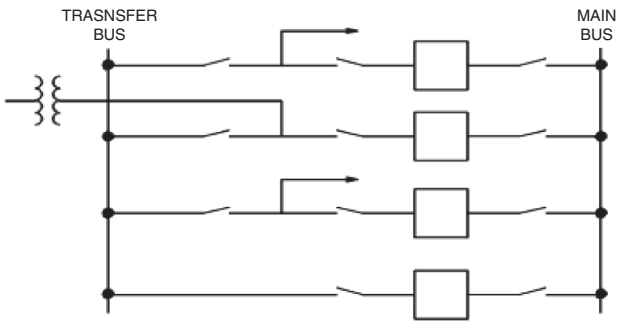


FIGURE F.1 One-line diagram of main and transfer bus scheme. In normal operation, the main bus is energized and the transfer bus is de-energized. In the bottom bay, the breaker and switches are open. In the top three bays, the switches on the left are open with the breakers and other switches closed.

BREAKER-AND-A-HALF CONFIGURATION

The breaker-and-a-half configuration, typically used at extra–high-voltage (EHV) stations, consists of two buses, each normally energized. Electrically connected between the buses are three circuit breakers and, between each two breakers, a circuit, as shown in Figure F.2. In this arrangement, three circuit breakers are used in a bay for two independent circuits; hence, each circuit shares the common center circuit breaker, so there are 1.5 circuit breakers per circuit. The breaker-and-a-half configuration provides for circuit breaker maintenance, since any breaker can be removed from service and isolated without interrupting any circuit. Additionally, faults on either of the main buses cause no circuit interruptions. Failure of a circuit breaker results in the loss of two circuits if a common breaker fails and only one circuit if an outside breaker fails. It is important to balance circuits in the bays, for example, source lines coming into the right-hand side of bays and load lines leaving the left-hand side of bays.

The main advantages of this scheme include the following:

- A bus fault does not interrupt service on any circuit, and circuit breaker failure causes loss of only one or two circuits;
- Flexible operation;
- High reliability; and
- Double feed to each circuit.

The primary disadvantages of this scheme include the following:

- One-and-a-half breakers are required per circuit;
- Relaying is complex, since the center breaker has to respond to faults of either of its associated circuits, and since currents from two sources must be measured for all circuits; and
- Each circuit must have its own potential source for relaying.

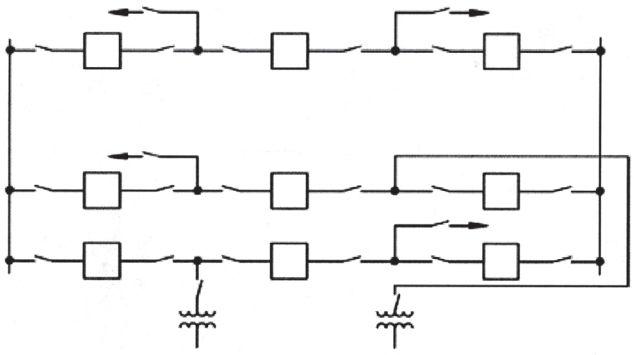


FIGURE F.2 One-line diagram of breaker-and-a-half bus configuration.

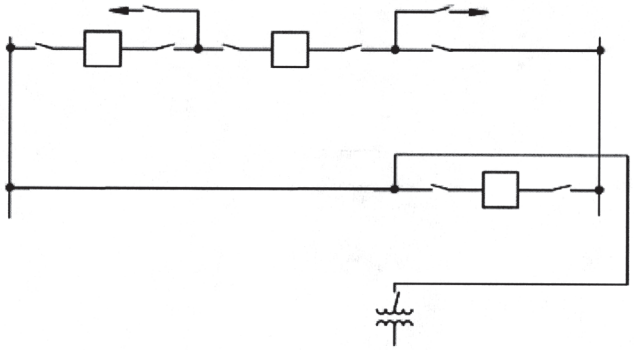


FIGURE F.3 One-line diagram for ring bus configuration.

RING BUS CONFIGURATION

For stations having three to five circuits, a ring bus is often used. As more circuits are added, the configuration may evolve to a breaker-and-a-half arrangement. Figure F.3 shows a three-circuit ring bus that is based on Figure F.2 but with the bottom bay and three breakers and one bay-two circuit removed. A maintenance outage of a circuit breaker or circuit causes an "open ring." For open-ring operation, a subsequent circuit outage may cause outage of additional circuits.

The advantages of this scheme include:

- Low cost—only one circuit breaker per circuit; and
- Flexibility to evolve to a breaker-and-a-half arrangements as more circuits are added.

The disadvantages of this scheme include:

- Reduced reliability in open-ring operation; and
- Temptation to add circuits without evolution to a breaker-and-a-half arrangement.

DOUBLE BREAKER-DOUBLE BUS CONFIGURATION

The double breaker-double bus configuration consists of two main buses, each normally energized. Electrically connected between the buses are two circuit breakers and, between the breakers, one circuit, as shown in Figure F.4. Two circuit breakers are required for each circuit.

In the double breaker-double bus configuration, any circuit breaker can be removed from service without interruption of any circuits. Faults on either of the main buses cause no circuit interruptions. Circuit breaker failure results in the loss of only one circuit.

Because of high cost, the double breaker–double bus configuration is usually limited to large generating stations. The additional reliability afforded by this arrangement over the breaker-and-a-half scheme usually cannot be justified for conventional transmission or distribution substations. Occasionally, at a generating station, one bay of a breaker-and-a-half arrangement is used as a double breaker-double

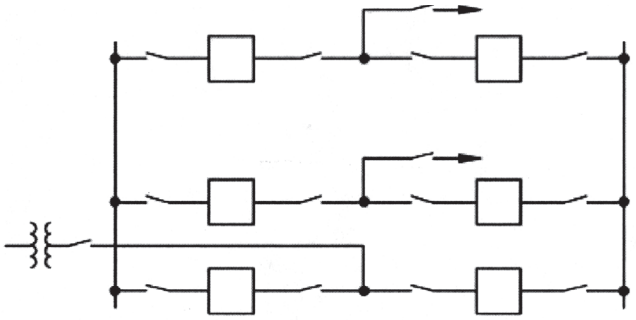


FIGURE F.4 One-line diagram of double breaker–double bus configuration.

bus arrangement for a generator terminal to provide equal access to either main bus.

The main advantages of this scheme include:

- Flexible operation,
- Very high reliability,
- Isolation of either main bus for maintenance without disrupting service,
- Isolation of any circuit breaker for maintenance without disrupting service,
- Double feed to each circuit,
- No interruption of service to any circuits from bus fault,
- Loss of only one circuit for breaker failure, and
- All switching with circuit breakers.

The primary disadvantage of this scheme is high cost because two circuit breakers are required for each circuit.

G

Controlling Power Systems

CONTROL EQUIPMENT AND PRACTICE

Terrorist attacks and other disturbances can evolve into instability in a few seconds or tens of seconds—too fast for control room operator actions. Operators may act within a few minutes during relatively familiar events with alarms, but in new situations, 15 to 30 minutes may be required to make assessments and act, especially if load shedding is required. Thus, various types of automatic controls are required. Improving the control of voltage and reactive power may also require relatively low-cost high-voltage equipment additions such as shunt capacitor banks.

Automatic controls constitute one or more layers of the *defense in depth* or *multiple layers of defense* principle for preventing or mitigating blackouts. In comparison to the addition of new transmission lines, control improvements can be rapidly implemented.

This appendix provides details on automatic controls for electric power systems, including new technology and best practices. Such best practices help power systems to survive major disturbance events, both at power plants and in the transmission network. Besides the more conventional controls, emergency controls often termed "special protection systems" are applied to mitigate extreme disturbance events. Information technologies hold promise to advance control capabilities in the near future.

In short, power system robustness, resilience, and survivability in the face of major disturbances, including terrorist attacks, can be increased significantly, economically, and rapidly by the use/addition of automatic controls. However, there are several necessary requirements, namely, (1) implementation of industry best practices, (2) prioritized upgrading of old analog controls (and actuators such as generator field circuit exciters), and (3) development and implementation of wide-area controls. North American Electric Reliability Council (Electric Reliability Organization) reliability standards for automatic controls, including performance monitoring, should evolve to better reflect best practices. Kundur et al. (2007) describes best practices in detail, listing over 50 best practices.

Automatic Controls

Additional information is provided below on the following means of automatic controls that are listed but not described in Chapter 6.

Techniques for Shedding Load and Generation to Enhance Power System Dynamic Response Capabilities

Power system dynamic response following disturbances can, to some degree, be separated between real (active) power phenomena and reactive power/voltage phenomena. Real power (measured in MW) is always held in balance when the system is operating normally. A disturbance upsets this balance and initiates dynamic response from the rotating synchronous generators in the system. An important aspect of the real power balance deals with the availability of spinning reserve (unloaded generation synchronized and ready to serve additional demand) and the activation of such reserves following islanding. This would also include measures such as load and generator shedding. Activation of reserves at power plants by prime mover/energy supply system control is limited. The tendency to carry reserves on fewer units, with many units base-loaded, reduces performance. The response of units is difficult to predict because power plant operators can select from several control modes such as traditional governor control of speed and system frequency, MW control override of speed control, or coordinated boiler/turbine control with limited speed/frequency control. System frequency regulation by secondary control (automatic generation control) or operator actions often takes tens of minutes for large upsets. Operator-directed or automatic demand-side actions are potential aids during emergencies.

With automatic underfrequency load shedding and with proper coordination between power plant control and

protection as described below, power system survivability following real-power imbalances is quite probable. System frequency excursions are typically limited to 1 to 2 percent of 60 Hz. One continuing concern, however, is unnecessary tripping of generation during frequency excursions because of boiler upsets and other problems. Prioritized control and protection improvements and modernization would reduce tripping and improve system survivability following events with load-generation imbalance.

There are, however, relatively simple and low-cost practices that greatly improve reliability. However, these practices are not always followed—the August 14, 2003, cascading failure providing a prime example (Nedwick et al., 1995; U.S.–Canada Power System Outage Task Force, 2004). Best practices for voltage reactive power require modern excitation equipment at generators. Replacement of very old equipment with modern thyristor exciters and digital voltage regulators will improve generator reliability. Generator voltage regulator controls including limiter circuits should be coordinated with protective relaying. A lack of coordination has contributed to the severity of blackouts. Automatic voltage regulator line drop compensation or automatic transmission-side voltage control should be considered for better regulation of the transmission network voltage profile.

Techniques for Maintaining Proper Transmission Network Voltage Profiles

Voltage should be near the maximum of the allowed voltage range and should be fairly uniform at all locations. This high, flat voltage profile reduces losses that cause heating and sagging into trees. Extensive use of relatively low cost shunt capacitor banks in both transmission and distribution systems allow a high and flat voltage profile, with substantial reactive power reserves at generators for emergencies. Voltage and reactive power are more complicated with separate ownership of generation and transmission systems. Rigorous standards with performance monitoring are required. Overly complex payments for reactive power or reactive power markets should be avoided. The section titled "Examples of Voltage/Reactive Power Practice" below in this appendix describes how poor voltage/reactive power practice played a critical role in the August 14, 2003, blackout (U.S.–Canada Power System Outage Task Force, 2004).

Primary Automatic Controls to Prevent Cascading Instability

Primary automatic controls, which are located mainly at power plants, include automatic voltage regulators and prime mover controls such as speed governors. Automatic voltage regulators include functions such as power system stabilizers, excitation limiters, and possibly connection of line-drop compensation. Prime mover controls include speed and power regulation. Modern controls are digital, allowing a wide variety of sophisticated features, such as deadbands and control mode shifting.

Transmission-level Power Electronic Devices and Mechanical Devices

Transmission-level power electronic devices such as static volt-ampere reactive (var) compensators are employed to provide continuous voltage control, similar to a generator voltage regulator, and/or other functions. Mechanically controlled shunt capacitor/reactor banks are switched by local voltage relays, by SCADA operators, and sometimes by emergency controls. With digital technology, there is room for more sophisticated control similar to that possible with power electronic devices.

Local Load-shedding Practices and Techniques

Local underfrequency load shedding is commonly employed at bulk power delivery substations. Underfrequency load shedding generally requires islanding of a portion of the interconnection with large generation-load imbalance. In a growing number of power companies, local undervoltage load shedding is also employed (Taylor, 2007). Also, to avoid possible blackouts during lightning storms or other transient events, automatic reclosing or single-pole switching is employed. Since most terrorist actions are likely to cause permanent outages, however, automatic reclosing will likely be unsuccessful.

Special Protection Systems or Remedial Action Schemes

Another widely used class of controls is termed special protection systems (SPSs) or remedial action schemes (Taylor, 2007). These are emergency controls that initiate powerful discontinuous actions, such as controlled separation/islanding, load tripping, or generator tripping at the sending end of an inter-tie. Other possible actions are steam-turbine fast valving, capacitor/reactor bank switching, HVDC fast power changes, and dynamic braking. At present, most of these controls directly detect single or multiple outages and then make logic decisions about whether to initiate feedforward action. The *event-based* controls are often implemented to prevent cascading for multiple outages, but are sometimes implemented even for *N*–1 outages. Many SPSs are wide area with outage detection at several sites, binary transfer trip signals to logic computers perhaps at control center(s), and then transfer trip signals to power plants and substations for control action. Reliability for the mission-critical actions must be at least as high as primary protective relaying, requiring as a minimum redundancy so that no single component failure will cause overall control system failure. A large-scale SPS implementation is described below in this appendix.

Wide-area Feedback/Response-based Controls

A promising alternative or complement to local controls or to SPS is wide-area feedback/response-based controls. Two types of these controls are continuous feedback control, and discontinuous control, which take actions similar to those taken by SPSs. Compared to local controls, wide-area controls provide greater observability and controllability. Positive sequence, synchronized phasor measurements are the preferred sensors for control inputs. High-speed digital/optical communications are required.

Continuous Wide-area Control

Continuous wide-area control is being studied by many utilities, vendors, and universities. Perhaps the most serious work is that by Hydro Quebec for power system stabilization (oscillation damping improvement) through generator excitation control, and through the use of static var compensators and other power electronic devices.

Wide-area Discontinuous Feedback Control

Wide-area discontinuous feedback control is based on power system response to disturbances rather than on direct detection of only certain outages, as in most SPSs. Control action occurs for outages *anywhere* in the interconnection that causes a threatening response. Notable is the Wide-Area Stability and Voltage Control System (WACS) in development at BPA (Taylor et al., 2005).

Figure G.1 shows a block diagram of power system stability controls. The SPS path is feedforward. The continuous feedback controls are normally local and mainly at generators, but could be wide area. The feedback (response-based) discontinuous controls are often wide area, but could be local (e.g., underfrequency or undervoltage load shedding).

Sophisticated Control Algorithms

Sophisticated control algorithms use various techniques such as adaptive or "intelligent" control as part of digital control and communication capabilities. Integration with the energy management system (EMS) functions, such as dynamic security assessment, is possible to adapt control to present operating conditions. The description of wide-area controls above focuses on actions to prevent instability and controlled or uncontrolled separations and islanding. If these actions fail, controlled separations could be initiated. This is relatively easy for well-defined inter-ties between areas, but more difficult in a highly meshed system. Adaptive islanding is a research area. Some aspects of this concept have been demonstrated recently in simulation on a large, realistic test system (Yang et al., 2006).

Example of Impact of Voltage/Reactive Power Practice

An example of the impact of voltage/reactive power practices on system performance from the August 14, 2003, blackout is presented (U.S.–Canada Power System Outage Task Force, 2004). The initial outage of the Eastlake 5 generator on August 14 was related to excitation equipment problems during production of high reactive power. (The outage likely would have been avoided with modern equipment.) As an example of poor voltage/reactive power practice, Figures G.2 and G.3 show conditions on August 14, 2003. Figure G.2 shows the 345 kV voltage profile that many engineers would regard as terrible, especially considering that the load was less than 80 percent of peak summer load and that the

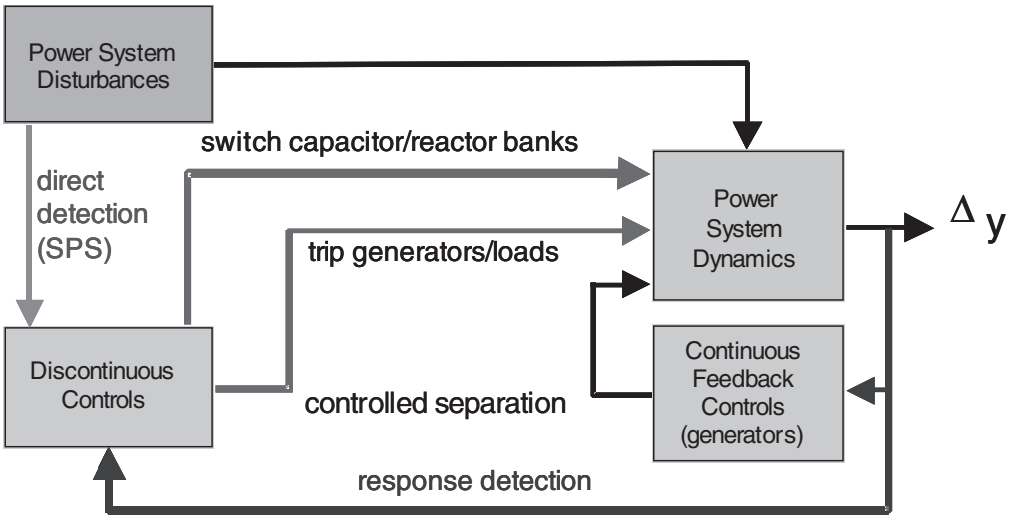


FIGURE G.1 Power system stability controls.

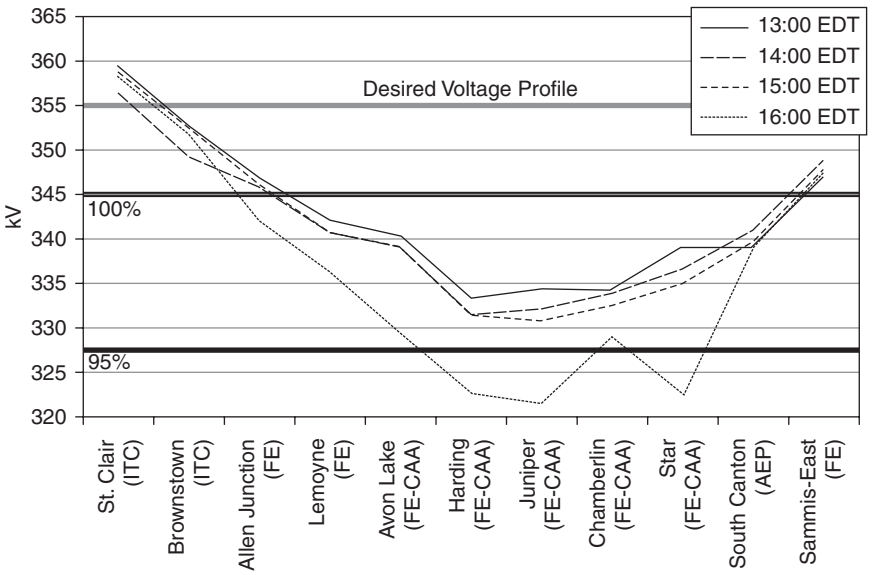


FIGURE G.2 August 14, 2003, voltage profile from west to east across northern Ohio. SOURCE: U.S.–Canada Power System Outage Task Force (2004).

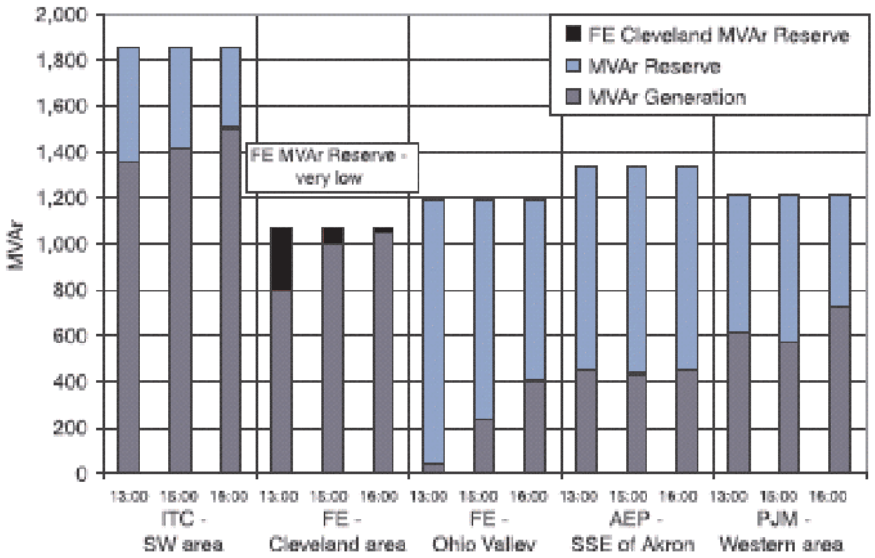


FIGURE G.3 August 14, 2003, reactive power production and reserves. SOURCE: U.S.–Canada Power System Outage Task Force (2004).

13:00 voltage profile was before any outages. Figure G.2 also shows a more desired voltage profile of 103 percent (which could be even higher: standard voltage range is 345 kV ± 5 percent). Voltage at the west (left) end near Detroit is very good. Voltage at a large Ohio River power plant on the east end is relatively low. Despite substantial reactive power reserves in the American Electric Power area (Figure G.2) and a 765 kV infeed, voltage at the South Canton bus is poor.

Figure G.3 shows the very low reactive power reserves at power plants in the Cleveland area. Again, the corresponding high reactive power output combined with old excitation equipment caused the initial Eastlake 5 outage. The poor voltage profile contributed to lines sagging into trees (with heating and sagging inversely proportional to voltage squared). Although inadequately discussed in the reports on the August 14, 2003, blackout, the disaster would likely have been avoided with many more capacitors banks in the Cleveland/Akron area. The power system would have been much more robust and resilient.

Example of Special Protection System Implementation

Bonneville Power Administration (BPA) may have the world's largest implementation of SPSs. The most important SPSs involve the Pacific AC and DC inter-ties, where the main action is tripping of up to 2,700 MW of hydro generation. This is for high power transfer from the Pacific Northwest to California, where the generator tripping prevents instability (loss of synchronousness among generators). Load tripping at the California end would have a similar benefit for stability.

The most complex scheme involves preventing separation of the 4,800 MW Pacific AC inter-tie where high-speed outage detection of around fifty 500 kV lines is installed (detection at both line ends). Outage detection is transmitted over redundant microwave or fiber-optic communications to BPA's two control centers. Fault tolerant (triple-redundant) programmable logic controllers are at the control centers. Each logic computer has the equivalent of around 1,000 logic gates to detect the many combinations of single, double, and triple line outages in the series/parallel transmission line path. Commands are then sent to generating plants. Besides hydro generation tripping in the Northwest sending end to reduce power transfer, the controls also switch 500 kV capacitor/reactor banks. If an intertie separation does occur, controlled separations of the northern and southern portions of the western interconnection into two electrical islands is initiated. Following a severe outage, control actions are executed in less than a second.

REFERENCES

Kundur, P., C. Taylor, and P. Pourbeik. (co-chairs and secretary). 2007. *Blackout Experiences and Lessons, Best Practices for System Dynamic Performance, and Role of New Technologies*. IEEE Special Publication 07TP190, July.

Nedwick, P., A.F. Mistr Jr., and E.B. Croasdale. 1995. "Reactive Management: A Key to Survival in the 1990s." *IEEE Transactions on Power Systems* 10(2): 1036–1043.

Taylor, C.W. 2007. "Power System Stability Controls." Chapter 12, *Power System Stability and Control* volume of *The Electric Power Engineering Handbook*. Boca Raton, Fla.: CRC Press/IEEE Press.

Taylor, C.W., D.C. Erickson, K.E. Martin, R.E. Wilson, and V. Venkatasubramanian. 2005. "WACS: Wide-Area Stability and Voltage Control System: R&D and On-Line Demonstration." *Proceedings of the IEEE* [special issue on energy infrastructure defense systems] 93(5): 892–906.

U.S.–Canada Power System Outage Task Force. 2004. *Final Report on the August 14, 2003, Blackout in the United States and Canada: Causes and Recommendations*. Natural Resources Canada and the U.S. Department of Energy. April.

Yang, B., V. Vittal, and G.T. Heydt. 2006. "Slow-Coherency-Based Controlled Islanding—A Demonstration of the Approach on the August 14, 2003, Blackout Scenario." *IEEE Transactions on Power Systems* 21(4): 1840–1847.

H

R&D Needs for the Power Delivery System

TABLE H.1 Research Area Options Primarily for the Existing Bulk Power (Transmission) System Architecture

		Objectives		
Technology/Operational Strategy Application	Research Areas	Thwart Attack	Reduce Vulnerability	Reduce Impact
System components that are less vulnerable to incursion, gun shots, or explosive devices	Physically robust towers, insulators, and conductors		X	
	Physically robust transformers, breakers, and switchgears	X	X	
	Low-cost undergrounding techniques	X	X	
New techniques for reducing stress by improving operation and maintenance	Integrated asset management			X
New monitoring and diagnostic techniques to reduce the impact of attacks and improve reliability	Non-intrusive monitoring			X
	Non-destructive evaluation			X
	Low-cost dissolved gas analyzers			X
Physically protective shields for substations and transformers	Advanced materials for shielding	X		
Recovery equipment (to recover from attacks)	Substation recovery (temporary) transformers			X
	Recovery breakers			X
Advanced protection devices to mitigate outages from attacks	Self-programming power electronic relays		X	X
Sensors and communication to increase monitoring, mitigate outages, and enhance response	Wide-area measurement		X	X
	Dynamic thermal circuit rating		X	X
	Video sag monitoring		X	X
	Integrated electricity and communication system architecture		X	X
	Precision high-speed time-stamped monitoring		X	X
	Enhanced visualization		X	X
Computational ability to monitor systems, mitigate outages, and better plan restoration	Topology estimating		X	
	CAR monitoring		X	
	[Truly] real-time analysis		X	
	Integrated engineering and economic methodology for power system operation		X	
	Market simulation		X	
	Fast simulation and modeling		X	
	Advanced training simulators		X	X
	Advanced date storage, management, and incident reconstruction		X	

TABLE H.1 Continued

Technology/Operational Strategy Application	Research Areas	Objectives: Thwart Attack	Objectives: Reduce Vulnerability	Objectives: Reduce Impact
Passive technology to increase power flow on existing rights of way to reduce the potential impact of events	Reconfiguring (new bundles, higher voltages, etc.)		X	X
	High-amperage conductors		X	X
	High-temperature superconducting cables		X	X
	Composite structures		X	X
Short-circuit current limiters to reduce the possibility of cascading outages	Power electronics based		X	X
	Superconducting		X	X
Enhanced control of the existing system to reduce vulnerability and enhance recovery	Reducing the cost of current-generation FACTS devices		X	X
	Voltage-source converters		X	X
	Asynchronous rotating machines		X	X
	Advanced systems control		X	X
Developing software that thwarts cyber attacks	Hardening energy management systems against cyber attacks	X		
	Developing secure firewalls for the variety of intelligent devices, relays, and controls at substations that can be controlled remotely	X		

TABLE H.2 Research Area Options for Enabling New Bulk Power (Transmission) System Architecture

Technology/Operational Strategy Application	Research Areas	Objectives: Thwart Attack	Reduce Vulnerability	Reduce Impact
Technologies to enable complete control of the power system to mitigate outages and enhance restoration	Advanced power electronic devices		X	X
	Advanced DC back-to-back		X	X
	Low-cost FACTS		X	X
	Power electronic breakers		X	X
	Intelligent universal substation transformers		X	X
	Multi-layered control strategies		X	X
	Distributed autonomous agents		X	X
	Integrated control strategies		X	
	Complete system automation		X	X
	Self-healing topology		X	X
	Object models for all digital devices		X	
Technologies to enable smaller synchronous or DC systems to operate in an integrated fashion so as to reduce system vulnerability	Microgrids		X	X
	Distributed generation		X	X
	Renewables		X	X
	DC distribution		X	
	Electric storage at high-voltage levels		X	
Technologies to greatly increase power flow to reduce stress and mitigate outages	AC superconducting cables		X	
	DC superconductivity		X	
	The IntelliGrid		X	
Innovative computational ability technologies	Fast modeling and simulation		X	
	Local and global optimization and control algorithms for power controllers		X	X
	State estimation and optimization functions between local systems		X	
	Optimized system decomposition		X	X
	Reconfiguration and protection coordination for reliability management		X	X
	Optimization functions incorporating local generation, load control, and central generation		X	X
	Advanced market structures to seamlessly incorporate local systems into overall generation/load/mix		X	

TABLE H.3 Research Area Options Primarily for Existing Distribution System Architecture

Technology/Operational Strategy Application	Research Areas	Objectives: Thwart Attack	Reduce Vulnerability	Reduce Impact
Asset management to reduce system stress	Integrated asset management			X
	Tighter voltage control			X
	Monitoring of capacitor banks			X
Increased power flow to reduce stress on the system	Reconfiguring and increasing voltage		X	
	Superconducting cables		X	
	Low-sag conductors		X	
Improved reliability and system vulnerability	Reducing underground construction costs		X	
Enhanced control to reduce stress and enhance restoration	Power electronics network protectors		X	X
	Short-circuit current limiters (medium voltage)		X	X
	Tie and feeder circuit reclosers		X	X
Reconfigured network grids in large cities	Submersible fast switches	X	X	X
	Low-voltage switches and smart fuses for reconfiguration and isolation		X	

TABLE H.4 Research Area Options for Enabling New Distribution System Architecture

Technology/Operational Strategy Application	Research Areas	Objectives: Thwart Attack	Reduce Vulnerability	Reduce Impact
Advanced distribution automation (DA)	Advanced DA architecture		X	X
	Object models for all digital distribution devices		X	
	Fault anticipator		X	
	Intelligent universal transformer		X	
Power electronics technologies to manage demand and improve reliability	Inductive (contactless) charging		X	
	Active harmonic filters		X	
	Embedded solutions		X	
	Voltage restoration devices			X
	Intelligent universal transformer		X	
	High-efficiency DC-DC converters		X	X
	Low-voltage and medium-voltage smart power controllers		X	
	DC breaker and controllers		X	
	Low-cost motor drive controller in chip		X	
Distributed energy resources	Integration of distributed energy resources		X	X
	AC-DC converters		X	
Distributed generation technologies	Photovoltaics		X	X
	Concentrating solar		X	X
	Solid oxide fuel cell		X	X
	PEM fuel cell		X	X
	Microturbines		X	X
	Stirling engines		X	X
	Carbon nanotubes for hydrogen storage		X	
	High-pressure electrolyzers		X	
	On-board fuel reformers		X	
	Combined heat and power for residential applications		X	
	Radioisotope photovoltaic generator		X	
	Thermoelectric generators		X	X
	Direct methanol fuel cell		X	X
	Microelectromechanical systems (MEMS) power sources		X	X
	Micro solid-oxide fuel cell		X	X
Electric energy storage devices	Lead acid battery		X	X
	Nickel-metal hydride battery		X	X
	Lithium-ion battery		X	X
	Vanadium redox flow battery		X	X
	Zinc-bromine flow battery		X	X
	Sodium-sulfur battery		X	X
	Hydrogen storage		X	X
	Flywheel energy storage		X	
	Ultracapacitors		X	X
	Miniature compressed air energy storage		X	X
	Metal air battery		X	
	Lithium-ion battery		X	X
	Lithium-sulfur battery		X	X
	Superconducting magnetic energy storage		X	X
Communication technologies	Broadband over power line		X	X
	WiMax wireless high-speed communication		X	X
	Consumer portal		X	X
	Standardized object models		X	X
	Power line carrier/wireless for local communication		X	X
	Standardized LAN/WAN technology		X	X
Technologies to enhance control	Power electronic breakers		X	X
	Custom power devices		X	X

TABLE H.5 Research Area Options Primarily for Existing Device and Building Systems

Technology/Operational Strategy Application	Research Areas	Objectives: Thwart Attack	Objectives: Reduce Vulnerability	Objectives: Reduce Impact
High-efficiency lighting systems	Photoluminescence material		X	
	Daylight harvesting		X	
	Integrated lighting		X	
	High-intensity discharge		X	
	Advanced fluorescent lamp systems		X	
	Light-emitting diodes		X	
High-efficiency motors and motor drives	Soft-switching adjustable speed drives		X	
	Low locked-rotor current single-phase machines		X	
	High-efficiency axial air gap motors		X	
	New motor designs		X	
High-efficiency space conditioning	Water loop heat pumps		X	
	Ground-coupled heat pumps		X	
	Dual path HVAC systems		X	
High-efficiency water heating	Heat pump water heaters		X	
	Heat recovery water heaters		X	
High-efficiency refrigeration	High COP refrigeration system		X	
Efficiency industrial electrotechnologies	Infrared heating devices		X	
	Microwave-assisted chemical synthesis		X	
	Radio frequency drying and curing		X	
	Advanced programmable logic controllers		X	
	Ultraviolet curing		X	
Building systems technologies to reduce demand and consumption	Smart thermostats		X	X
	Building-integrated PV		X	X
	Building and process energy management systems		X	X

TABLE H.6 Research Area Options for Enabling New Device and Building Systems Architecture

Technology/Operational Strategy Application	Research Areas	Objectives: Thwart Attack	Objectives: Reduce Vulnerability	Objectives: Reduce Impact
Technologies to integrate end-use devices and buildings into the power delivery system	Consumer portal		X	X
	Smart appliances and devices		X	X
	Power quality monitoring		X	
	Automated meter reading		X	
	Outage monitoring		X	X
	Energy management system integration		X	X
	Advanced demand response		X	X
	Smart meters		X	X
Technologies to enable buildings to operate independently	Low-cost power conditioning		X	
	Small distributed generation		X	X
	Electric storage technologies sized for buildings		X	X
	Appliances “hardened” against disturbances		X	X
	Solid-state transfer switches		X	X