JAY APT
LESTER B. LAVE
SAROSH TALUKDAR
M. GRANGER MORGAN
MARIJA ILIC

Electrical Blackouts: A Systemic Problem

Although human error can be the proximate cause of a blackout, the real causes are found much deeper in the power system.

About every four months, the United States experiences a blackout large enough to darken half a million homes. As long ago as 1965, a massive blackout in New York captured the nation's attention and started remedial action. But that was almost 40 years ago, and still we have not ended blackouts nor even reduced their frequency significantly. Major advances in system regulation and control often evolve in complex systems only after significant accidents open a policy window. The recent blackouts in this country and abroad have created such an opportunity.

The day after the August 14, 2003, blackout, President George W. Bush and Canadian Prime Minister Jean Chrétien directed a joint U.S.-Canada Power System Outage Task Force to investigate the causes of the blackout and the ways to reduce the possibility of future outages. On November 19, the task force reported that the blackout was due to human error. In laying the blame on operators in two control centers, this interim report follows a long tradition of singling out individuals and companies who made the wrong decisions. Firing individuals and suing companies might be satisfying to those who suffered in the blackout, but it will do little to prevent future blackouts. Similar problems are common in generation and transmission companies, as examination of the frequency and geographic distribution of blackouts shows.

Promises to end blackouts have been made for decades, but they ignore the reality that complex systems built and operated by humans will fail. Congress and the Federal Energy Regulatory Commission (FERC) must implement a framework that recognizes that individuals and companies will make errors and creates a system that will limit their effects. Such a system would also be useful in reducing the damage caused by natural disruptions (such as hurri-

Jay Apt (apt@cmu.edu) is Distinguished Service Professor in Engineering and Public Policy and executive director of the Carnegie Mellon University Electricity Industry Center. Lester B. Lave (lave@cmu.edu) is Higgins Professor of Economics and codirector of the Carnegie Mellon University Electricity Industry Center. Sarosh Talukdar (talukdar@cmu.edu) is professor of electrical and computer engineering at Carnegie Mellon University. M. Granger Morgan (gm5d@andrew.cmu.edu) is Lord Professor and department head of Engineering and Public Policy and codirector of the Carnegie Mellon University Electricity Industry Center. Marija Ilic (milic@andrew.cmu.edu) is professor of electrical and computer engineering and engineering and public policy at Carnegie Mellon University.

canes) and is likely to improve reliability in the face of deliberate human attacks as well.

Fortunately, air traffic control provides us a guide to a system designed to minimize the effects of human error. The problems uncovered by the August blackout can be addressed by the kind of change that transformed the air traffic control system from one of frequent deadly accidents to a system that has provided a relatively accident-free environment, despite enormous growth in the number of daily flights and occasional errors by pilots and controllers.

August 14 and earlier blackouts

There were indeed many individual errors on August 14. A plant operator pushed one generator near Cleveland too hard, exceeding its limits and resulting in automatic shutdown at 1:31 that afternoon. With that generator lost, power flowed over transmission lines to fill the need in Cleveland. The utility failed to appreciate the seriousness of the situation, because it did not perform a contingency analysis after the loss of the plant to see if another failure would lead to serious trouble. Although the computer model that performs the contingency analysis was running and could have provided results in a few minutes, none of the operators consulted it at any time that afternoon, according to interviews cited in the report.

The transmission system operations center had trouble with its computer analysis tool starting at 12:15 p.m. Only a single analyst was on duty. That person fixed the problem by 1:07, but then went to lunch without setting the program to report automatically every five minutes. So the analysis tool was not available until 4:04 p.m.

At 2:02, one line failed because although it was carrying less than half the power it was designed for, it sagged into a tree that had not been trimmed recently, causing a short that took the line out of service. Accident analysts say most accidents are caused by a chain of events, and one weak link in this chain was the failure to recognize that tree-trimming is an essential part of the design of transmission systems.

With both the generator and the line out of commission, other lines were overstressed and failed between 3:05 and 3:39 p.m. That led to more failures and the blackout at 4:08. As the situation worsened, competing generating companies and power transmission line operators did not share data. Even some data that were shared could not be interpreted, because companies had not kept track of changes in the grid that had been made by others.

Meanwhile, back at the utility, the operators did not notice that their own alarms and graphs were disabled when the computers driving them froze at 2:14. Having no training in recognizing and reacting to failures of their computer systems, they believed their rosy frozen data even when calls came in reporting trouble. The control displays were hard to interpret, even after they began working again at 3:59. When it finally became clear that not enough electricity was being generated or transmitted to supply all customers, the operators made no attempt to shed load—that is, to black out a few customers in order to prevent blacking out 50 million.

The task force interim report concludes: "training was inadequate for maintaining reliable operation . . . internal control room procedures and protocols did not prepare them adequately to identify and react to the August 14 emergency."

It is tempting to assume that these were isolated errors made by one or two organizations. It is always easy to blame individuals, but such complacency is misplaced. Operators at consoles in 140 control centers around the country control the grid by calling for generators to ship power over the proper lines at just the right time to meet demand. These operators work for some of the 3,000 power companies and transmission operators in the United States, but they do not have timely access to the information they need to make wise decisions. "Most control facilities do not receive direct line voltage and current data on every facility for which they need visibility," the task force concluded. To make up for the lack of real-time data, they sometimes use computers to estimate the state of the grid. Use of such models is uneven in the 140 control centers. Says the report, "control areas that have them commonly run a state estimator [a computer tool used to estimate what is working and what is broken, since very little actual data is monitored] on regular intervals or only as the need arises (i.e., upon demand). Not all control areas use state estimators."

The task force also listed additional factors that contributed to the August 2003 blackout. They include, "inadequate interregional visibility over the power system; dysfunction of a control area's

SCADA/EMS [data system]; and lack of adequate backup capability to that system." This list of other factors is important, because it draws attention to underlying weaknesses in the system that could also be identified factors in earlier blackouts.

A few common themes emerge from investigations of the 2003 and earlier blackouts:

- Monitoring of the power grid is sparse, and even these limited data are not shared among power companies.
- Industry standards are lax; for example, vegetation under transmission lines is trimmed only every five years.
- Operators are not trained routinely with realistic simulations that would enable them to practice dealing with the precursors to cascading failures and the management of large-scale emergencies.
- Power companies have widely varying levels of equipment, data, and training. Some companies can interrupt power to customers quickly during an emergency, whereas others are nearly helpless.
- Decades-old recommendations to display data in a form that makes it easy to see the extent of a problem have been ignored. This was a contributing cause of the 1982 West Coast blackout, where "the volume and format in which data were displayed to operators made it difficult to assess the extent of the disturbance and what corrective action should be taken."
- Monitoring of the power system is everywhere inadequate, both within regions and between them.

How the grid is operated

The United States has attempted voluntary measures to prevent electrical blackouts for much of the past century. Originally, vertically integrated utilities planned for their own system reliability, with a few tie lines to neighboring utilities that might be helpful in some emergencies. It became clear in the 1965 Northeast blackout, when a failure in Ontario blacked out New York City 11 minutes later, that growing electric demand had made regional issues important. In the next two years, 10 voluntary regional reliability councils were established to coordinate the planning and operation of their members' generation and transmission facilities. In 1968, the North American Electric Reliability Council (NERC) was formed to coordinate the regional councils. One of NERC's primary functions is the development of reliability standards for the regional generation and transmission of power. According to its Web site, "NERC has operated successfully as a voluntary organization, relying on reciprocity, peer pressure and the mutual self-interest of all those involved."

Consumers of electricity may have a different definition of success. Despite the voluntary standards, large blackouts unrelated to storms occurred in Pennsylvania, New Jersey, and Maryland on June 5, 1967 (affecting 4 million people); Miami on May 17, 1977 (1 million); New York on July 17, 1977 (9 million); Idaho, Utah, and Wyoming on January 1, 1981 (1 million); four western states on March 27, 1982 (1 million); California and five other western states on December 14, 1994 (2 million); the Pacific Northwest on July 2, 1996 (2 million); 11 western states on August 10, 1996 (7.5 million); and San Francisco on December 8, 1998 (0.5 million).

After the passage of the Public Utilities Regulatory Policies Act in 1978 and the Energy Policy Act of 1992, the electricity industry became a hybrid of vertically integrated utilities and new structures of multiple forms. "Merchant generators," independent of utility companies, installed their own plants and sought customers anywhere in the country. Aggregators bargained for better rates on behalf of large numbers of customers. Energy brokers used the open market and long-term contracts to buy and sell power.

Restructuring has transformed the operation of the electricity system. Utilities formerly transmitted power from a nearby generation plant to customers. Now, industrial customers can buy power from plants hundreds of miles away, putting major burdens on the transmission system and increasing the likelihood of a blackout. That has made a huge difference: The number of times that the transmission grid was unable to transmit power for which a transaction had been contracted jumped from 50 in 1997 to 1,494 in 2002. This metamorphosis has done little to improve the physical system of transmission or its control systems. The burden of making the new system operate reliably has instead fallen on people.

No organization that generates, transmits, or distributes electric power wants low reliability. But in a deregulated competitive electricity market, companies have to pay for investments out of the revenues they earn. Unless companies can find a way to bill

customers for reliability, or unless regulators mandate reliability investments and ensure that they are reimbursed, no investments will be made. None of the 19 states that have implemented electric restructuring has figured out how to pay for investments to prevent low-probability events such as blackouts.

Eight years ago, reacting to that summer's two large outages in the West, NERC's chief executive officer wrote that, "[a new model] must include universal participation, more detailed and uniform reliability standards that can be put in place quickly, independent monitoring of reliability performance, and the obligation to support, promote, and comply with NERC's policies." In 2002, NERC incorporated many of the new market participants that emerged after restructuring (such as brokers and aggregators) in developing its voluntary reliability standards. In 2003, NERC stated that, "the existing scheme of voluntary compliance with NERC reliability rules is no longer adequate for today's competitive electricity market." However, both a 1998 Department of Energy report and a complaint to FERC in 1997 question NERC's authority to make its standards mandatory.

NERC has supported federal legislation that would establish an Electric Reliability Organization (ERO) with power to establish and enforce mandatory standards. A NERC panel put forward this proposal first in January 1997. Eight months later, it was endorsed by a task force chartered by the Department of Energy as a response to the 1996 blackouts. It was part of the energy bill that passed the House on April 11, 2003, and subsequently appeared in Section 1211 of the conference committee language. The proposed ERO would be industry-led and could level penalties for violations of standards, but its authority over grid operations (as distinct from planning standards) is still to be defined.

Reducing blackouts

We can apply lessons from the history of air traffic control [see sidebar] to the electric utility industry. Just as in air traffic control in the early 1960s, the time for ad hoc fixes and finger-pointing has passed. The United States needs a national plan implemented through an organizational structure that recognizes that human beings make mistakes and that preventing those mistakes requires checks and balances.

A long-range plan should take into account engineering improvements. These could include ways to control exactly where power flows through the lines, electrical compensation for the strain on the system when a customer spins up a large motor, and direct current transmission lines (which reduce the loss of energy that occurs in transmitting alternating current power long distances). Generating electricity in relatively small plants located close to consumers, rather than in large central generation plants, will reduce blackouts. This distributed generation holds promise, but for the foreseeable future the system will rely on the existing transmission grid. Other technologies, such as robust automatic control systems to reduce dependence on human operators, might be feasible in a decade.

Long-range planning should not distract us from the significant improvements we can make within the next few years. Some elements of such a near-term plan are clear.

We need national standards for telemetry data on power flows and transmission system components. Competitive pressures and changes in the way the grid is used have led to a very sparse data system, and market pressures are not likely to improve matters. Operators can no longer be expected to make the right decisions without good data. Today's hodgepodge of individual capabilities resembles the rudimentary air traffic control system of 1934-37, which was operated by a few airlines. Control centers must have displays and tools that allow operators to make good decisions and to communicate easily with operators in different control areas. There must be backups for power and data, and clear indications to all operators that data are fresh and accurate. The emphasis should be on data and presentations that support decisions. The present representations of system state, particularly indicators of danger, are too complex. They stress accuracy over clarity. Grid operators need much clearer metrics of danger and suggestions for action (like collision avoidance alarms in aircraft and in air traffic control centers), even if they are a little less accurate. If the existing 157,000 miles of transmission lines in the United States were fitted with $25,000 sensors every 10 miles, and each sensor were replaced every five years, the annual cost would be $100 million. This would increase the average residential electricity bill (now 10 cents per kilowatt-hour) to 10.004 cents per kilowatt-hour. The total would be roughly one-10th the estimated annual cost of blackouts.

Lessons from air traffic control

Electricity is not the only critical infrastructure in which safety conflicts with economics. It is instructive to consider the history of the air traffic control system as a framework that could reduce the errors leading to blackouts.

Federal regulation of air transportation expanded steadily through the mid-20th century as traffic increased. Federal licenses for pilots and mechanics were required in the late 1920s. In 1934, when planes began flying through clouds, the Bureau of Air Commerce asked the airlines to develop rules to control and separate air traffic, but in 1937 the government took direct control of the system, and air traffic control for planes flying through clouds became mandatory. The bureau and its successor the Civil Aeronautics Authority (CAA) had authority for operating the system and investigating accidents and other mishaps.

Radar had demonstrated its value to air travel during World War II, but it was not required for civilian flights until 1956, when a crash over the Grand Canyon killed 128 people and spurred the government to build a national radar-based air traffic control system for high-flying planes. Safety was the goal, but radar also had the immediate effect of improving airway capacity, because accurate data allowed the distance between aircraft to be decreased from 30 miles to 5 miles. The government later expanded the radar system to cover low-flying planes near airports.

During and after World War II, the Army argued successfully that the CAA should control only civil aircraft. Two parallel control systems—civil and military—persisted until 1958, when two collisions between military jets and civil aircraft killed 61. Later that year the new Federal Aviation Authority (FAA) was established with a mandate to coordinate all civil and military air traffic at high altitude. At about the same time that it was adding operational responsibility for FAA, the Department of Transportation moved investigative authority to a new National Transportation Safety Board to eliminate the possibility of conflict of interest.

In 1961, President John Kennedy told the FAA to prepare a long-range plan for the air traffic network and to perform associated R&D. The resulting study recommended a system that could monitor aircraft throughout their flights and improve information displayed on screens to give operators better data and to make it much easier to interpret. Throughout the 1960s, the 21 regional control centers retained wide flexibility to formulate rules appropriate to their local conditions, but by 1970 it was clear that the system needed a national coordination center. As a result, airliners have takeoff and landing slots and are held at the gate, not in the air, until it is safe to fly. Aircraft delays due to air traffic congestion fell by two-thirds after the opening of the national command center. The safety and efficiency of this large national network have been improved by federal standards for data, displays, and certification.

These improvements in air safety have been costly. Beginning with the Airport and Airway Revenue Act of 1970, funding for the system, as well as for improvements to airports, has been raised largely by taxes on airline tickets and fuel. But the money appears to have been well spent. In 1960, U.S. air carriers had 44.2 fatalities per 100 million aircraft miles. In 2000 the rate was 1.2. Although the goal of preventing all air crashes will never be achieved, increases in safety have been impressive, because the incident investigations have sought ways to make the system safer, not just to blame pilots for crashes or near misses.

We draw the following lessons from the history of air traffic control:

- *The federal government assumed control of a system that could not be handled by state and local government or by a voluntary system run by the airlines.*
- *The system moved beyond panic responses to a crash to a comprehensive system that included R&D and facilities to handle future issues.*
- *A single agency should not be responsible for both operation and investigation.*
- *Comprehensive monitoring of data is crucial, and so is the ability to interpret the data in real time and take remedial action.*
- *Many of the actions are local or regional, but a national coordination center is required to bring the controllers together.*
- *As a result of all these remedies, an extremely complicated and potentially deadly system of air transport has been made very safe, much safer than driving.*

All grid operators must be trained periodically in contingency recognition and response using realistic simulators. These simulations must include all operations personnel in a way that exposes structural deficiencies, such as poor lines of authority and insufficient staffing. The goal should be to recognize and act on signs of extreme system stress that may be well outside daily operations experience. The description of flying as "years of boredom interrupted by moments of stark terror" applies also to grid operations. Grid operators must have the systems and training that only realistic simulations, using their specific control center configuration, can provide. Federal standards for training, licensing, and certification of grid operators and control centers are warranted to ensure that a single weak control center does not bring down a large area. No federal entity now mandates such realistic training for grid operators, but the owners of nuclear generation plants proved (after Three Mile Island) that it can be done.

Operations control centers must be able to control. The patchwork ability to shed load is not appropriate to the current interdependent transmission grid. Some systems do it automatically, but some cannot even do it manually from the control center. Shedding of load in the near term will probably be in the form of blacking out large areas. Some power companies have customers who have agreed to be blacked out in emergencies, but this practice is not uniform. A decade hence it may be possible on a large scale to provide signals to consumers to shed parts of their load in exchange for lower tariffs, but this partial load reduction solution has not been economically feasible with current systems.

Just as air navigation aids are monitored and flight-checked periodically, sensors, load-shedding devices, and other system components must be checked on a much more systematic basis than they are at present. In a competitive environment, chief financial officers will frown on such periodic testing, which is why it should be mandated by national standards.

Industry standards for such items as tree-trimming under transmission lines must be set with the costs of failures in mind, not just by the competitive constraints of the immediate marketplace. Companies that do not comply should be penalized. These standards will vary by region and should be set by regional bodies such as the Regional Transmission Operators.

A national grid coordination center should be established and run as a national asset by a private body. It would stimulate R&D for the data needed for grid monitoring. It would also monitor the situation at regional and larger levels, provide national flow control, and perhaps act as a backup for computer failures in individual control regions. As in air traffic control, the roles and responsibilities of the local and national centers will be neither perfectly optimum nor static, but they will complement each other so that we can avoid the complete lack of situational awareness seen in so many blackouts.

A permanent government investigation body, including professional accident investigators who are trained to look for systemic as well as discipline-related causes, should be an entity separate from the operators or regulators of the grid.

How can we evolve to such a system?

The current electricity reliability system was created and developed in an environment of voluntary participation. Trying to get all companies to participate and comply with the recommendations has meant that standards have not been stringent. They have also, demonstrably, not worked. Creating a better system is not simply a matter of making the current rules mandatory. Mandatory rules are necessary but not sufficient. We need to set rules for operations as well as for engineering by clarifying the goals of the transmission and generation systems and the responsibilities of each party. The NERC standards here are not at all specific, mandating only general guides such as "return the system to a secure state." What will emerge from the rule-setting is unlikely to have policy or engineering purity or complete coherence, but it will be better than the present fuzzy goals that provide little guidance on difficult tradeoffs.

The new rules for engineering and operations must be informed by the current state of technology and the technology improvements that are likely in the next few years. The size and complexity of any of the three U.S. interconnection regions mean that the new system has to be flexible and adaptive, since there is no mathematical formula that can be developed for so large a system. The need for innovative thinking suggests that an expert commission should be created to advise the body setting mandatory standards. The commission should have experts from op-

erating companies, systems operators, FERC, and academia to take a fresh look at how to design both engineering and operations standards that will satisfy the goals.

This is analogous to the long-range air traffic control study President Kennedy ordered in 1961. But the experience of the air traffic control system also provides insights about likely problems to avoid. Although its operations have produced an admirably safe system, its investments in technology and infrastructure have been far from satisfactory. This suggests that infrastructure decisions should be informed, but not dominated, by current operations decisions. The electricity industry has its own technology issues. Industry funding of its Electric Power Research Institute has dropped by half since restructuring began. Both R&D tax credits and detailed regulations have been proposed as stimuli for lagging innovation.

Industry is struggling to avoid detailed federal oversight (through FERC) of the transmission and generation of electricity. NERC is not a federal entity, and FERC has very little authority to perform oversight of its voluntary policies. FERC has limited jurisdiction over reliability issues, such as reserve generation capacity requirements, and over the real-time operations of the transmission grid. FERC is exploring its rather limited authority on reliability and indicated in late 2003 that it would require public filings of any violations of the existing voluntary grid reliability standards, which are overseen by NERC. These standards deal with the planning of adequate generation and transmission capacity to meet expected load.

The new FERC proposal does not appear to require reporting of noncompliance with NERC's operating standards (which themselves do not require that data be collected on the status of the grid more often than every 10 minutes). Even this innocuous-sounding FERC proposal was opposed vigorously on January 9, 2004, by the Edison Electric Institute, whose members (large utilities) want the industry's NERC, not the federal government, to have responsibility for standards. Three days later, FERC's chairman told the Wall Street Journal that he "intends to hire 30 engineers in coming months to conduct performance audits and bird-dog the work done by the reliability council."

If the legislation to create an ERO passes, it will be interesting to watch the experiment of an industry organization chartered by the federal government to enforce with penalties standards it develops. The experiment aside, this provision is only a start. If a body such as this is to make real progress, its authority should be expanded to include certification of transmission operators and systems to meet national standards of data and control, training, and periodic testing.

The Federal Aviation Administration's (FAA's) certification and training standards as well as its air traffic operations have been admirable. However, the FAA and its predecessors have found the management of new technology systems challenging. Better control center computers and precision upgrades for landing navigation systems have been decades behind schedule. It seems reasonable that a grid control system should be managed privately. Nevertheless, the past 40 years have shown us that voluntary standards and individual operating practices are not appropriate for the grid. Just as the FAA sets standards for airlines and national standards for navigation data and control centers, a body (either the proposed ERO or a federal agency) should set operations requirements and police them. The same body could operate the national grid coordination center. A separate agency, such as the Department of Energy, should house the permanent investigation personnel.

The gross revenues of the electric sector and the airline sector are very similar. FERC is currently funded by user fees, and the improvements in the national grid control system that are required could be funded in a manner similar to the air traffic control system, and would add perhaps one-10th of a percent to the typical electric bill.

The best parts of the air traffic control experience can be incorporated, and the worst parts avoided, by implementing a strong set of mandatory federal rules and certifications covering the seven elements discussed above. Unfortunately, pending legislation misses most of these key points. The battle between industry and FERC is not likely to be resolved without comprehensive legislative attention to reliability, with the debate taking into account the lessons of related critical infrastructures.

A plan comprising these elements, one recognizing that failures of complex systems involve much more than operator error, better reflects reality and will help keep the lights on.

Recommended reading

U.S.–Canada Power System Outage Task Force, *Interim Report: Causes of the August 14th Blackout in the United States and Canada, November 2003* (https://reports.energy.gov/).

Western Systems Coordinating Council Disturbance *Report for the Power System Outage that Occurred on the Western Interconnection August 10, 1996* (ftp://www.nerc.com/pub/sys/all_updl/docs/archives/AUG10FIN.pdf).

National Research Council, *Flight to the Future: Human Factors in Air Traffic Control* (Washington, D.C.: National Academy Press, 1997) (http://books.nap.edu/catalog/5493.html).

A Call to Action, letter from NERC CEO Richard J. Grossi to utility executives, October 28, 1996 (ftp://www.nerc.com/pub/sys/all_updl/docs/archives/ceoltr.pdf).

Final Report of the Secretary of Energy Advisory Board Task Force on Electric System Reliability, September 29, 1998 (http://www.seab.energy.gov/publications/esrfinal.pdf).