
14

ELECTRICITY: A SYSTEMIC PROBLEM IN THE ELECTRICITY DELIVERY SYSTEM

A. Apt, L. B. Lave, S. Talukdar, M. G. Morgan, and M. Ilic

The record of the past 40 years shows that in the nation's system for generating, transmitting, and distributing electricity, some blackouts are inevitable. Natural hazards produce many local and regional blackouts (Table 14.1), and society has learned to cope with them. Power outages occur more frequently than theory predicts, however, and despite years of promises and technology development, the frequency of large blackouts has not decreased over time (Figure 14.1). Making cost-effective improvements in control and operation of the grid¹ is important; however, data suggest that reducing the frequency of these low-probability, high-consequence events will become increasingly expensive.²

The U.S. and Canada blackout on August 14, 2003, revealed that many private institutions are far ahead of the public sector in defining their critical missions and taking steps to protect them when the lights go out. During the one-day blackout, some hospitals and television stations in New York City, Toronto, Cleveland, and Detroit were able to stay open because they had backup generators. Services in other sectors, however, could not be delivered. Elevators in office buildings were stuck between floors, trains stopped between stations, traffic signals went dark, cell phones lost reception, and, in Cleveland, water ceased to flow and sewers overflowed when the electric-powered pumps stopped functioning. If the blackout had persisted for longer than a day, the

Portions of this work have appeared in the following publications: S. Talukdar, J. Apt, M. Ilic, L. Lave, and M. G. Morgan (2003). "Cascading Failures: Survival vs. Prevention."

16(9): 25–31. J. Apt, L. B. Lave, S. Talukdar, M. G. Morgan, and M. Ilic (2004). "Electrical Blackouts: A Systemic Problem." *IEEE Transactions on Power Delivery* 20(4):

55–61. J. Apt and M. G. Morgan (2005). "Critical Electric Power Issues in Pennsylvania: Transmission, Distributed Generation, and Continuing Services when the Grid Fails," Pennsylvania Department of Environmental Protection.

many tunnel ventilation fans would become inoperable. The study also found that three of the five Pittsburgh police zone stations do not have on-site backup generation. In addition, liquid fuel storage tanks, which rely on electricity to pump fuel, generally have no electric backup. Some fuel can be released from storage tanks via gravity flow, but the switchover from pump to gravity flow can be time-consuming.

The study found that Pittsburgh's natural gas system is highly reliable; possibly more so than the diesel supply chain. Although natural gas backup generators are typically more expensive than those powered by diesel, natural gas powered backup is a viable option for high value services, especially if the generators are used to produce electricity and heat during normal operating conditions. However, local law specifies in some cases that backup systems be fueled by diesel. Furthermore, critical service providers such as financial institutions prefer diesel – they can control their own fuel storage supply, independent of the natural gas supply. However, only a few days of diesel is usually on hand even in the best facilities. Propane can be used for backup fuel in certain locations.

disruptions and continue to operate (perhaps at a reduced level of service); and (3) pursue alternative strategies to keep services operating when power from the network is no longer available.

Because networked infrastructures are physically dispersed, there is no way to harden every piece against accidental or intentional disruptions, although increased protection for some system components would make sense.³ Researchers in cyber security understood the limits to system hardening many years ago. Indeed, it was the desire to produce a computer communication system that could continue to operate when parts of it were disrupted that led to the architecture of ARPAnet, the forerunner of today's Internet. Computer security theorists have therefore largely abandoned the model of a computer system as an impenetrable fortress. Rather, they seek to design a "survivable" system – that is, one that can fulfill its mission in a timely manner, even in the presence of attacks, failures, or accidents.⁴ Making the electric infrastructure similarly more robust is feasible, and many improvements are possible in operations and standards.

A focus on survival of missions stands in contrast to survival of the generation and transmission grid through approaches such as "islanding" (separating the survivable parts of a grid from those that are critically wounded), which have long been used. These are good tools, but their implementation over the past two decades has failed to eliminate low-probability, high-consequence outages, nor are they likely to do so in the future.

Ensuring the fulfillment of critical missions is also different from either a traditional vulnerability assessment approach or the approach of making the electricity delivery system 100 percent reliable.⁵ Invulnerability is not only very expensive, but it is also impossible to test and probably impossible to achieve for a complicated system like the electric grid. Rather, a fresh approach is needed to prevent society from incurring large costs during the inevitable next blackout or from attempting to entirely prevent such a blackout.

SEVEN STEPS TO ASSESSING READINESS

The goal of a socially oriented approach is to lower the social costs of grid failures, rather than preventing all of them. More specifically, the goal is to reduce the costs of the inevitable grid failures by assuring the continued availability of critical services and subsystems, such as traffic signals in urban cores, pumps for water and sewer systems, urban mass transit, emergency service systems, subway and elevator egress, and crucial economic functions.⁶ Verification could be accomplished in a number of ways, including actual tests conducted on the services and subsystems (something that cannot be done on the full grid).

The first step in defining and verifying solutions to the survivability of critical missions would be to determine a set of design reference events that

Table 14.2. Design reference events for a power system.

Reference event	Duration	Geographical location	Frequency	Load affected
Reference event 1	4 hours	1 circuit (about 1,000 people)	1 in 22 months	Load shedding, weather
Reference event 2	2.5 days	400,000 people	1 in 6 years	Weather, disruption of transmission or generation
Reference event 3	2 weeks	All of a region	1 in 50–100 years	Weather, terrorism

would mimic outages of varying lengths and geographical locations. The system would be evaluated on the basis of whether it fulfills critical missions during these design events. An example of a set of design reference events is given in Table 14.2.

The second step would be to define the missions that must be fulfilled. This step would result in enumeration of life-critical and economically important missions that are provided by electric power, together with a list of missions which, if unfulfilled, would have important socio-economic consequences (such as reducing gross domestic product or inducing terror).

The third step would be to prioritize the missions. The priority list would be different for different design reference events. For example, a 12-hour outage from a cascading grid failure would have different priorities than would a month-long blackout from a severe ice storm or human attack on system components. Similarly, some services, such as delivering potable water, could carry on uninterrupted for a day or more because of water stored in the system. Thereafter, however, water delivery would be far more problematic. Other services, such as sewage treatment and disposal, might be an immediate problem.

The fourth step would be to determine which missions are already protected (e.g., hospitals and navigation aids for air traffic). Weak links in the chain would be identified at this step. For example, while the New York City area's Newark and Kennedy airports quickly restored power for passenger screening and other boarding functions the day after the 2003 blackout, LaGuardia could not because it had insufficient backup power, and its grid power was slow to be restored. As a consequence, East Coast air traffic was snarled by the closing of a busy hub.

The fifth step would be to determine which missions require procedural changes or new hardware.

The sixth step would focus on the missions in step five that require new hardware. This step would seek cost-effective technologies that could fulfill critical missions during the design reference events. For example, light-emitting

diodes (LEDs) could produce traffic signals with only a small fraction of the energy required to light the incandescent bulbs currently housed in traffic lights. Inexpensive batteries and trickle chargers of LED traffic signals could ensure that lights could continue to operate without additional electricity for days during a power outage. Other cost-effective devices might include those that make elevators return to the ground floor or allow subways and elevated trains to creep to the next station. Some devices would be attractive for private investment (for example, tenants may be willing to pay higher rent for a building that has its own micro-grid with backup power). For public goods at this stage, the costs of fulfilling the missions would be compared with the value of the missions, and alternative methods of fulfilling the missions could be evaluated. Effects of the candidate solutions on the nominal and recovering grid would be assessed and verified during this step by building and testing prototypes where necessary. For example, loads would be tested for their smooth transfers from distributed power systems to and from the grid to ensure that the transfer would not affect grid stability – this could require hardware and operations changes and would certainly require tariff changes.⁷

The seventh step would be to build a system for allocating competing resources required for these missions during an extended blackout. This is often the first step considered by managers trained in emergency response, but it would be much more effective if preceded by steps one through six.

Performing the tasks outlined in these steps can yield an up-to-date assessment of the readiness of the system to respond to challenges. Knowing the available hardware and procedures, governing authorities can estimate which missions could be accomplished and where the greatest trouble spots are likely to be.

7.2.1.1 A E A D - ELIC I E E I \ C I A L L C I I C A L I I

During a large power outage such as one caused by a hurricane or ice storm, the best that government agencies can do by way of social services is to provide a limited number of shelters and very limited distribution of water. Most of the organizations in a position to assure that important social services continue during a power outage are private companies. While it might be to the collective benefit of society for these organizations to make investments that will make services more robust, it is often not in their private interest to do so. In other cases, the investments may be in the interest of private entities but not properly identified as an opportunity. Or it might be possible to provide incentives or information to make these investments more attractive to private entities.

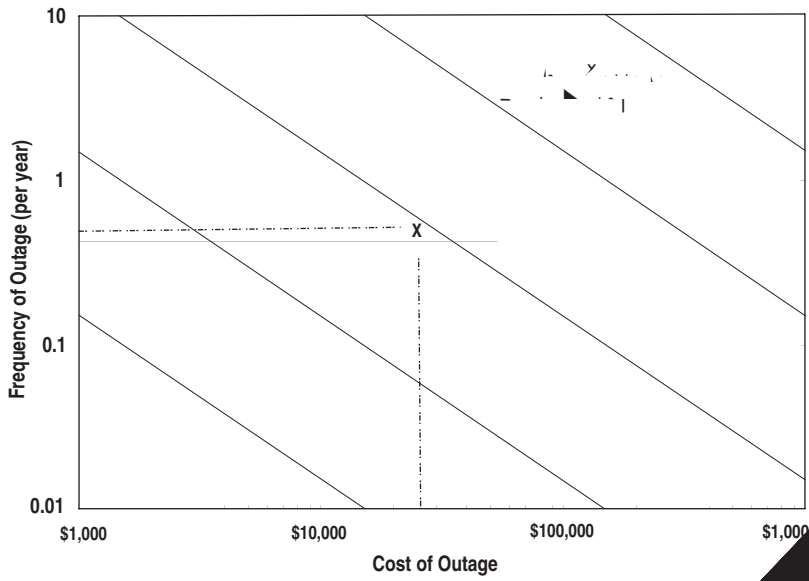
Private entities such as supermarkets and gas stations have no responsibility to secure their operations to make them more robust to blackouts – they are responsible only for their owners. If it is possible to avoid loss or increase profits during a blackout, a profit-maximizing firm will do so. For example, the decision for a private company to install a backup system involves the calculation of the cost of a backup system, how often it would be needed, and whether it would generate net benefits.

Most backup systems required to provide services independent of grid power have associated capital and maintenance costs. When a purchase of a given capital expense is contemplated, the decision maker estimates the frequency of power outages at the location being considered, and the cost of the power outage. If a 100-kilowatt generator (appropriate for a heat treating furnace, for example) costs \$76,000 and is financed over its 12-year lifetime, the annual cost of capital to purchase the generator at an interest rate of 7 percent is \$9,400. Operations and maintenance costs for this size generator, if properly maintained and operated at full load once a month, are approximately \$1,900 annually, for a total yearly backup cost of \$11,300. If the generator is used during a power outage to back up a service that incurs losses of \$25,000 (perhaps in lost product during a furnace heat-treating cycle), then the generator would be a sensible purchase if the company expects the power to fail long enough to ruin production more frequently than once every two years. Figure 14.2 illustrates the decision process.

As another example, a multi-story apartment building owner with a typical small traction elevator faces a product differentiation backup decision. The elevator would be backed up by a 12-kilowatt generator, with capital cost of \$13,200 and annual maintenance cost of \$240. Using a discount rate of 7 percent and a 12-year equipment lifetime, the amortized monthly cost of the backup would be \$160. For a five-floor apartment building with six apartments per floor, a monthly rent increase of less than \$5 would pay for the backup. While some tenants might not value this service, others might seek out such a building and willingly pay the increase.

SUGGESTED POLICY CHANGES TO ASSIST INVESTMENT

Policies to encourage survivable services can be win-win situations. At present, however, institutional or informational barriers inhibit more widespread installation of backup systems, even when they generate net benefits. State and local governments could encourage or require private parties to improve the reliability of important social services in a number of ways. For example, governments could modify electricity tariffs to permit load serving entities to recover costs associated with designing, installing, testing, and maintaining backup on-site power systems for individual customers who sign up for this service.



release inventory has induced many companies to cut emissions, such postings might induce companies to take steps to make their critical services more robust.

Changes to building codes and other legal requirements could also change business practices. For example, a decade ago some U.S. cities adopted a building code that requires elevators in newly constructed buildings of more than seven stories to have backup 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 for a percentage of these services to remain operational in the event of a power outage.

Governments could also provide tax incentives, subsidies, or grant programs to support the development of needed facilities. Given limited resources, this option should be used sparingly. Some circumstances, however, such as certain upgrades to emergency rooms of private hospitals, may warrant modest assistance.

Finally, communities could facilitate the construction, interconnection, and operation of distributed generation systems, and the operation of competitive micro-grid systems. In much of the United States today, rules granting utilities exclusive service territories make such micro-grids illegal; these rules could be changed.⁸

State and local governments could also encourage or require public and non-profit parties to improve the reliability of important social services. For example, information and suggestions to local governments and non-profit organizations could help them see how they might benefit from strategies that would make their services more robust in the face of power outages.

However, because most power outages arise from failures in the local distribution system, some jurisdictions have adopted regulatory requirements to foster retail competition based on reliability. This is most prevalent in New Zealand and Australia, where up-to-date reliability indices are posted on utility and government websites.⁹ Transparency of this sort aids consumers, but it is uncommon in the United States.

Electric Infrastructures

Electric infrastructures have been targeted for destruction by, for example, the North Atlantic Treaty Organization (NATO) in the southern Yugoslav province of Kosovo, the Farabundo Marti National Liberation (FMLN) in El Salvador, radical environmentalists in the United States and the Czech Republic, and labor movements and disgruntled landowners in several countries. They have also proven to be tempting targets to hunters practicing their sharp shooting. Iraqi insurgents have attacked European and U.S.-manufactured hardware in

Iraq, and presumably some information on vulnerable features has been shared with groups outside Iraq.

Several general areas of vulnerabilities may be tempting targets for sabotage. For example, often many of the main transmission lines feeding cities travel over a single corridor, providing a target for both natural hazards and human disruption. A 2002 study by the National Research Council identified large transformers as a critical area of vulnerability, because they are often unique and take many months to construct.¹⁰ Spare relays transformers are

While completely eliminating blackouts is an unrealistic (and expensive) goal, it is quite possible to improve upon the current record of blackouts while at the same time decreasing the extent of cascades caused by deliberate human actions.

Investigations of blackouts such as those listed in Table 14.1 reveal a number of common problems that need to be addressed.¹⁶ Significant improvements can be made within the next few years. We recommend a near-term plan based on our analysis of what has worked in other interconnected systems. These proposed improvements recognize that real people make mistakes, and that the system should be designed to reduce both the number and effect of those mistakes. Some of these recommendations are hardware-related, but all are designed to reduce both accidental and deliberate large blackouts.

MONITORING AND DATA COLLECTION

every five years, the annual cost would be \$100 million, or roughly one-tenth the lower bound of the estimated annual cost of blackouts. From a consumer's standpoint, the cost would increase the average residential electricity bill (now approximately 10 cents per kilowatt-hour) to 10.004 cents per kWh.

As described in more detail in Chapter 13, the data systems that monitor and control the grid in most large utilities formerly were proprietary systems with limited or no connections to the rest of the world. However, partly in response to cost pressures, some system functions in some utilities are no longer isolated. This leaves these systems vulnerable to cyber attack. Because the arcane nature of proprietary systems no longer protects utilities that adopt a common system, they must pay much more attention to the threats posed by hackers who can develop one exploit and use it on many power systems.

TRAINING

Another issue to address is operator training. Training, as with monitoring, varies widely between power companies. Most 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.

All grid operators must be trained periodically in contingency recognition and response using realistic simulations. 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 upon signs of extreme system stress that may be well outside daily operations experience. The description of piloting an aircraft as "years of boredom interrupted by moments of stark terror" applies also to grid operations, and training should be as rigorous as that undergone by pilots. Grid operators must have the systems and training that only realistic simulation, 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 against a single weak control center bringing down a large area. No federal entity mandates such realistic training for grid operators, but the owners of nuclear generation plants proved (after Three Mile Island) that it can be done.

EQUIPMENT

Power companies widely vary in their system abilities and equipment sophistication. Some companies can interrupt power to customers quickly during an emergency, whereas others are nearly helpless. This patchwork ability to shed load is not appropriate to the current interdependent transmission grid.

Some systems can interrupt power automatically, but some cannot even do it manually from the control center. Operation control centers must be able to actually control.

Shedding of load in the near term would probably take the form of preemptively blacking out large areas. Some power companies have customers who have agreed to be blacked out in emergencies, but this practice is not uniform. In a future decade, 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 in the United States.

Sensors, load-s(a0)TJT:91 0.24(225)Tj/TD-0.0o

The sort of information needed to assist governments in the decision-making process can be summarized in three groups: (1) models of the storage, transportation, and consumption of fuel and other goods during a blackout; (2) catalogs of the electrical needs and generating abilities of facilities, agencies, businesses, and communities; and (3) quantification of the criticality of different services during design reference power interruptions.

Obtaining the information necessary to assess the vulnerability of important services in the face of power outages and proposing solutions may be at odds with the desire of many organizations, especially those involved with homeland security, to keep information about vulnerabilities out of the public domain so that pernicious persons or groups cannot exploit those vulnerabilities. The problem is that if groups performing system-level analysis for state or local governments cannot access important information, it is extremely difficult for policymakers to develop rational policies to reduce future vulnerabilities. We encountered such difficulties when we performed a preliminary analysis for one agency of the state of Pennsylvania and found that even with the state's assistance it was impossible to obtain important data from other state agencies.

Public utilities are particularly protective of information about their emergency preparedness. For example, community water systems have prepared vulnerability assessments and emergency response plans. When questioned about any aspect of emergency operations at water system facilities (including the number and size of generators, the amount of fuel stored at pumping stations, or the parts of the water system that will first lose service in a crisis), facility managers will most likely answer by saying that the information is contained in the emergency response plans. These documents are reviewed but not retained by the states before being sent to the federal level. They are not available to the public.

This lack of information sharing is a problem even for responsible government agencies: one county emergency management coordinator described hitting an information "roadblock" when requesting information from local utility companies in an attempt to develop a critical infrastructure plan. A 2003 survey of public utility commissioners found that 54 percent "believe that utilities are either somewhat or very reluctant to share their security infor-

action. For example, a 2004 Associated Press report describes the process by which landline phone networks must alert federal regulators of service outages and report how the problems will be avoided in the future, a process that Federal Communications Commission (FCC) asserts has improved the landline phone networks; however, attempts to apply the same process to the wireless and cable phone networks have met with opposition.²⁰ Neither the companies themselves nor the Department of Homeland Security want the information made available to the public for fear the information will provide “blueprints for terrorists bent on wrecking U.S. communications systems.” Rather than filing with the FCC and allowing public access, the reports would be filed with the Department of Homeland Security.

The problem, of course, is that the Department of Homeland Security and other similar organizations have neither the resources nor the authority to develop and implement most of the changes that would be needed to make important social services less vulnerable. Those resources and responsibilities are widely distributed among state and local governments and in the private sector. It would help if the Department of Homeland Security and other similar organizations at sub-national levels could develop a greater ability to engage in system-level analysis that considers and balances a range of legitimate but perhaps conflicting social objectives. They would also need a greater ability to think about problems in terms of preserving social services as opposed to a unitary focus on protecting “critical network services.” Furthermore, the department would benefit from having a greater ability to develop and promote a range of alternative policies that states and private entities might adopt to promote viable solutions to reduce vulnerabilities. Finally, the department would need to provide arrangements that allow informed independent analysis by academic and other groups following the lead of other agencies that deal with

deelop

to

totthat

21

assumptions of attack frequency will change these estimates greatly. If attacks on the grid succeeded in causing blackouts every three years (with no additional protection), then the justifiable expenditure for additional protection would be \$300 million annually.

Whatever level of expenditure on new protection is agreed upon, mechanisms must be in place to decide on whether a particular expenditure should be made, and to allocate its costs. O'Hanlon and colleagues argue that the most efficient mechanism to allocate costs is "a combination of regulatory standards and antiterrorism insurance" whose premiums would be shared between the government and the users.

willingness to pay for preventing future incidents of terrorism through the mail should be based on the combined economic, institutional, psychological, and public health damage that such mischief can inflict. . . . Before committing

Non-electric public utilities	Water treatment	Extended duration	Typically very limited	Risk of illness if system pumps untreated water	Incapacitation and workforce productivity
	Drinking water	Extended duration; immediately in areas with wells	Limited gravity-fed areas; some pumps have backup power	Risk of dehydration and/or disease, especially during hot weather	Incapacitation and workforce productivity
	Sewer treatment	Medium and extended duration	None in most areas	Risk of disease from untreated sewage in water supply	Incapacitation and workforce productivity
	Sewer pumping	Short duration, high use periods (morning, evening); long duration	Very limited	Risk of disease from sewage buildup in low elevation areas	Incapacitation and workforce productivity; damage to buildings in low-lying areas
	Natural gas	All outages (including some critical backup generation fueled with natural gas)	Most pipelines use the materials being transported as the pumps; in-home furnaces require power for pilot lights and fans	Significant health risk for customers using gas heat during cold weather	Pipes may burst in cold weather if homes/buildings are left without heat
Communications	Radio broadcast media	Medium and extended duration	Most stations have backup systems with several days of stored fuel	Radio is important for distributing emergency information; risk of chaos if stations fail to disseminate information	Increased chaos costs from decreased communications
	Television broadcast media	Medium and extended duration	Many stations have backup power systems with several days of stored fuel	Less vital than radio communications as most TV sets require electricity	Most risk is borne by broadcasters and advertisers
	Cable television and broadband services	Medium and extended duration	Minimal	Less vital than radio communications as most TV sets require electricity	Risk for businesses that rely on cable broadband services

()

A. 14.A (continued)

	Security lighting	All outages	Varies	Varies by location	Potential for high economic losses
	Street lighting	All outages	None typically	Increased accident risk when roads are unlit	Indirect costs
Retail grocery	Cash registers, lighting, refrigeration, security	Medium and extended duration	Varies with location and firm preferences	Risk of food and emergency supply shortage during an extended outage	Large social costs resulting from insufficient access to food and supplies
	Wholesale grocery distribution networks	Medium and extended duration	Generally minimal	Risk of food and emergency supply shortage during an extended outage	Large social costs resulting from insufficient access to food and supplies
Financial	Cash machines	Medium and extended duration	None typically	Minimal	Significant social costs resulting from inadequate access to cash
	Bank branches	Medium and extended duration	Only for security systems	Minimal	Minimal risk, if some other access to cash exists
Financial	Credit card systems	Extended duration	Some backup power typically	Minimal	High risk during an extended outage (if also a shortage of cash)
	Pipeline and pumping systems	Medium and extended duration	Full for natural gas (because the system uses its own gas), typically none for other products	Indirect risk for vital services if fuel pumps fail to supply	from stress
Fuel infrastructure					

