

To appear in The Electricity Journal, Dec. 2003

Cascading Failures: Survival vs. Prevention

Sarosh N. Talukdar, Jay Apt, Marija Ilic, Lester B. Lave, and M. Granger Morgan

Abstract

Measures can be taken to reduce the number of large-scale power losses due to failures of the generation and high voltage transmission grid such as the August 14, 2003 blackout. However, such failures cannot be eliminated. The survival of essential missions is a more tractable problem than the prevention of all large cascading failures, and its solutions are verifiable. We propose that serious attention be directed towards assuring the continuation of essential missions even after the grid has failed. We outline a program to lower the social costs of power failures through successful preservation of those essential missions.

Introduction

The blackout of August 14, 2003, was caused by a cascading failure — a succession of transmission and generation outages, one precipitating another — that spread through Northern Ohio, much of Michigan, Ontario and New York, as well as parts of Pennsylvania and Connecticut.

Much of the policy discussion concerning blackouts has centered on the goal of preventing cascading failures from happening, or at least, drastically reducing their rate of occurrence.

Proposed preventive measures include: adding transmission capacity, improving regulations, more coordination, better training for human operators, better automatic control systems, more data collection, more data processing, load management, and more programs to promote conservation. Changes such as these can increase the integrity of the high voltage and extremely high voltage transmission backbone and some may reduce the frequency of large cascading failures. However, plausible blackout mitigation measures can have unexpected effects, sometimes increasing the frequency of events they were designed to prevent¹. Cost-effective changes which can be shown to reduce the frequency of power failures should be made, but they are unlikely to eliminate all failures.

In what follows, we will argue that framing the problem solely in terms of prevention has two fatal defects. First, the problem is in a formal sense incomplete, since it lacks the technical apparatus to test and verify its solutions. Without verification, we cannot be sure of detecting and eliminating major flaws from solutions, nor of even reliably distinguishing good solutions from bad ones. Second, the prevention problem is exceedingly large. The high voltage part of the grid spreads over 157,000 miles and contains thousands of nodes. It is difficult to imagine hardening so massive a structure against random, natural disturbances; it is almost inconceivable that it could be hardened against deliberate and intelligent attacks.

Inevitably, there will be future cascading failures. Instead, of trying to completely eliminate them, we propose that essential missions which are normally carried out by grid-delivered power be accomplished in emergencies by other methods. In other words, we suggest solving a set of much smaller and simpler survival problems whose goals are to identify vital services and arrange for them to continue despite the failure of the grid.

Probability of Power Failures

In comparison to ordinary (single) failures, cascading (multiple) failures² are rare, though the really big ones are not quite as infrequent as one might first expect. The North American Electric Reliability Council (NERC) lists 533 transmission or generation related outages over the period 1984 through 2000³. These are not distribution system losses: the users are affected because the generation and transmission system has failed. Forty-six of the events, or nearly three per year, are losses of 1,000 MW or greater. It has been understood for some time that the probability of smaller power losses follows an exponential curve, while that for larger losses (those above roughly 500 MW) is described by a power law⁴. As shown in Figure 1, a Weibull distribution fitted to the lower wattage losses grossly under-predicts the probability of large losses.

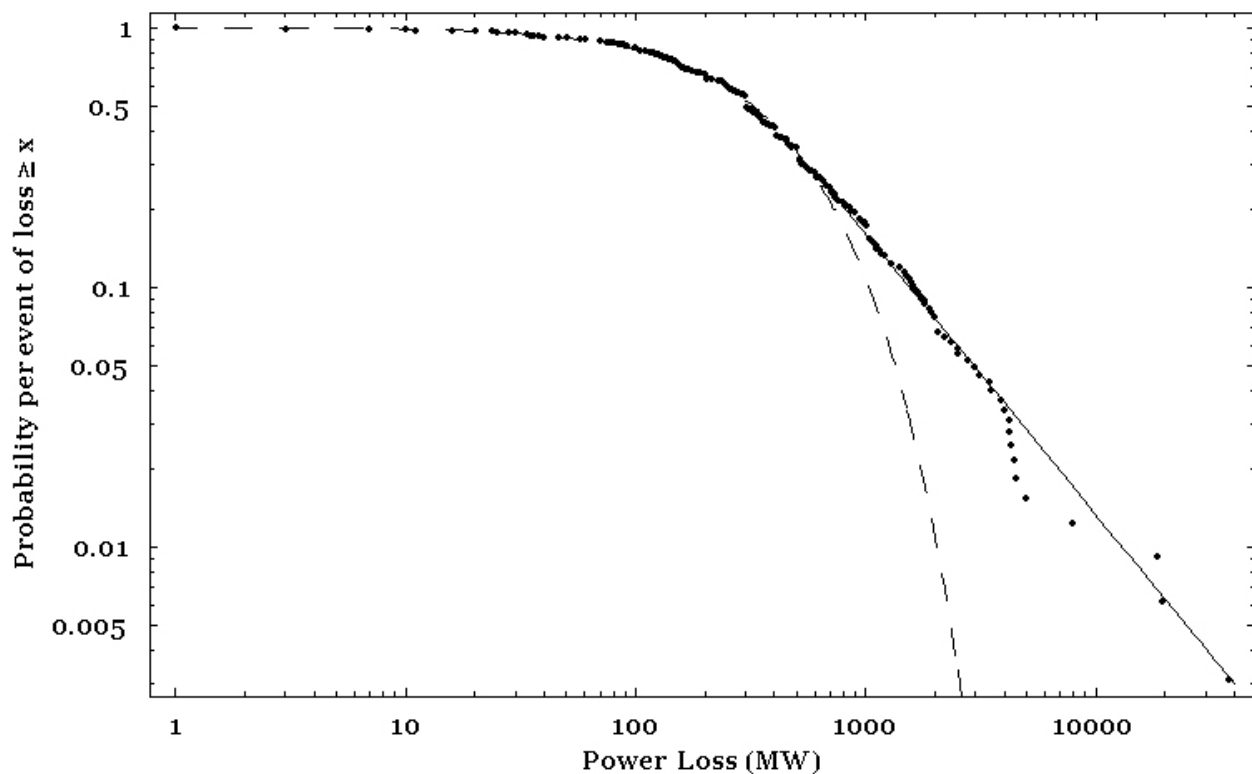


Figure 1. Cumulative probability of transmission and generation related failures. Points are data as compiled by NERC for the period 1984-2000. The dashed line is an exponential (Weibull) distribution fit to the failures below 800 MW loss. The solid line is a power law fit to the NERC data over 500 MW loss.

Carreras and co-workers have attributed this power law distribution to dynamical coupling between small and large blackouts⁵, and have written that “apparently sensible attempts to mitigate failures

in complex systems can have adverse affects and therefore must be approached with care¹.” They have also observed that if the small and large blackouts were uncorrelated, the probability would fall off exponentially rather than with a power law. Their work has pointed out that a) large blackouts happen relatively frequently, and b) their probability distribution exhibits the power law property of other coupled dynamic systems such as forest fires⁶ and that such systems have power laws with exponents between -1 and -2.

Analysis and Prediction of Cascading Failures

Predicting the evolution and effects of cascading failures has proven difficult. The difficulties have four sources. First, cascading failures are hybrid phenomena; their dynamics involve periods of continuous change punctuated by switching operations that produce discontinuities. Second, the evolution of any cascading failure depends on the initial conditions of the network, and there are a great many possibilities for these conditions. Third, electric grids contain many nonlinearities, such as power flows (products of voltage, current, and the cosine of the included angle) and saturation effects in transformers. Fourth, there are profound uncertainties in the grid’s response, such as the uncertainties in the reliability and thresholds of protective devices, in hidden failures, and in the interventions of human operators. The response of the grid is exquisitely sensitive to some of these uncertainties. A slight lowering of the threshold of a single protective device, causing it to operate when otherwise it would not, can completely change the course of a cascading failure.

There are two classes of methods for dealing with hybrid phenomena: analytical methods^{7,8} and simulation methods. Both classes have limitations. The analytical methods can handle the multitudes of initial conditions reasonably well but not the nonlinearities and uncertainties. The simulation methods can handle the nonlinearities well, but not multitudes of initial conditions, or uncertainties. As just one illustration, consider initial conditions and simulation. The space of these conditions is $S \times C$, where S is the space of possible initial states of the grid and C is the space of its possible initial configurations. Since a grid can contain over 100,000 devices, and each can be either “off” or “on,” the size of C alone is about $2^{100,000}$, far too big to be checked thoroughly.

Difficulties Inherent In Designing an Invulnerable Grid

The problem of designing or modifying a system, such as an electric grid, is *complete* in the formal mathematical sense of that word if it has three parts: a set of goals (what the system is to do — objectives and constraints), a design-space (what the system is to be made from — a space of variables that describe the structural alternatives or possible solutions), and a mapping of design-space into the goals accurate enough for verification (a way to compute and check the values of the goals for any solution)⁹.

The process of obtaining a good solution to a complete design problem can be thought of as a two-step iteration. The first step is to search the design space for a promising solution. The second step is to verify this solution, thereby establishing what, if anything, is wrong with it. The iterative process helps refine solutions and remove the flaws that raw, unverified solutions invariably contain.

For some problems, the search is more difficult than the verification. But for many design problems, not only is the search difficult, but the verification is much more so. For such problems it is easier to obtain promising solutions than to verify them. The problem of preventing cascading electrical failures is of this type. Indeed, as we have argued, verification is impossible with the analytical and simulation technologies available today.

Without verification, it would be unrealistic to believe that investment in a particular solution would prevent all future failures.

To summarize, the defects of the prevention problem are: The problem is exceedingly large. It is not certain that it has any good solutions. Even if it does and someone were to propose the perfect solution, we lack the verification methods to identify it as such. An unverified solution, even one that appears to be eminently reasonable, could in some cases increase the chances of cascading failures. Finally, some measures taken to prevent cascading failures could probably be defeated by an intelligent and determined attacker.

Problem Formulation In Terms Of Essential Missions

While making reasonable improvements in the structure and operation of the grid, a fresh approach is needed to prevent society from incurring large costs during the inevitable next blackout or by attempting to entirely prevent such a blackout.

We must come up with a formulation that covers the disruptions from cascading failures, but whose solutions can be verified, and then proceed to find good solutions to this formulation.

The goal of this formulation is to lower the social costs of grid failures, rather than to prevent all of them. More specifically, the goal is to reduce the costs of those inevitable grid failures by assuring the continued availability of critical services and subsystems, such as traffic lights in urban cores, pumps for water and sewer systems, urban mass transit, emergency service systems, the ability to exit from subways and elevators, and crucial economic functions¹⁰. 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).

Computer security theorists have largely abandoned the model of a computer system as an impenetrable fortress: rather, they seek to design a system which can fulfill its mission even when an attacker has penetrated the system's defenses. *Survivability* is defined in this context as the ability of a system to fulfill its mission, in a timely manner, in the presence of attacks, failures, or accidents¹¹. This focus on survival of missions is in contrast to survival of the generation and transmission grid through approaches such as "islanding" (separating the survivable parts of a grid from those critically wounded) which have long been used. These are good tools, but have not eliminated low probability, high MW outages, nor are they likely to do so in the future.

The steps in defining and verifying solutions to the survivability formulation are as follows.

The first step is to define the missions which must be fulfilled (in power systems parlance, "ride through" the event). These include, for example, urban vehicle traffic control, water, sewer and

natural gas pressure, and ability to exit from electric-powered transportation. This step results in enumeration of life-critical and economically important missions that are provided by electric power, together with a list of missions which, if unfulfilled, have important socio-economic consequences (such as inducing terror).

The second step is to determine a set of design reference events, such as the geographical extent and duration of an outage. The system is evaluated on the basis of whether it is able to fulfill the critical missions during these design events.

The third step is to prioritize the missions. The priority list will be different for different design reference events (a 12-hour outage from a cascading grid event will have different priorities than a month-long blackout from a severe ice storm or terrorist attack on critical system components).

The fourth step is to determine which missions are already protected, e.g., hospitals and navigation aids for air traffic. Weak links in the chain are identified at this step. For example, while Newark and Kennedy airports quickly restored power for passenger screening and other boarding functions the day after the August 2003 blackout struck, LaGuardia could not; as a consequence, east coast air traffic was snarled.

The fifth step is to determine which missions require new hardware (such as light-emitting diode traffic signals with trickle-charge batteries or onboard energy storage systems which return elevators to the ground floor) or procedure changes.

The sixth step focuses on the missions in step five that require new hardware. This step seeks cost-effective technologies which can fulfill the critical missions during the design reference events. Some missions will be attractive for private investment (for example, high-rise tenants may choose to locate in a building with higher rents if the building has its own micro-grid with backup power). For public goods, the costs of fulfilling the missions are compared at this stage with the value of the missions, and alternate methods of fulfilling the missions can be evaluated. Effects of the candidate solutions on the nominal and recovering grid are assessed and verified during this step, by building and testing prototypes where necessary. For example, loads must have smooth transfers from distributed power systems to and from the grid, without affecting grid stability (this may require hardware and operations changes, and will certainly require tariff changes¹²).

The seventh step is 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 will be much more effective if preceded by the above steps.

This formulation should provide an up to date assessment of the readiness of the system to respond to challenges. Knowing the available hardware and procedures, the governing authority could estimate which missions could be accomplished and where the greatest trouble spots are likely to be. With greater investments, more of the important missions could be accomplished during a blackout.

Conclusion

Ensuring the fulfillment of critical missions is very different from either a traditional vulnerability assessment approach, or the approach of making the electric delivery system 100% reliable. Invulnerability is not only very expensive, it is also impossible to test and probably impossible to achieve for a complicated system.

The power carried by the transmission system has increased since FERC Order 888 in 1996 opened the system to customers buying power from remote generators. Reliability (as measured by such indices as transmission loading relief events) has decreased. Since 1965, the amount of electricity generated in the USA has tripled¹³, while the transmission system has grown at half that rate¹⁴ because there were insufficient incentives to induce more investment. Once a framework for meeting the basic survivability mission without relying on the EHV/HV transmission grid is in place, the problem of managing the transmission grid itself during normal conditions will become more tractable. On-line monitoring and coordination of power delivery across large geographical areas in support of electricity market needs under restructuring has the potential to improve the overall efficiency of power production, consumption, and delivery at the wholesale level¹⁵. Investments in transmission are required to make deregulated electricity markets work¹⁶, but if our investment is confined to more miles of transmission lines, increasing redundancy in the current system, and more intelligent communication and control, we will not completely eliminate future blackouts.

In parallel with reasonable improvements to the grid (which are needed in any event to support deregulated shipping of power), the nation needs a fresh approach to reducing the social disruption and costs of cascading failures: we should give serious attention to finding ways to fulfill the critical missions of the system during a power blackout. In our judgment, this could be accomplished at affordable cost and would protect us from the social costs of natural disasters, disgruntled employees, and terrorists.

***Sarosh N. Talukdar** is Professor of Electrical and Computer Engineering at Carnegie Mellon University (CMU). **Jay Apt** is Executive Director of the Carnegie Mellon Electricity Industry Center at CMU's Graduate School of Industrial Administration and the Department of Engineering and Public Policy, where he is a Distinguished Service Professor. **Marija Ilic** is Professor of Electrical and Computer Engineering and of Engineering and Public Policy at CMU. **Lester B. Lave** is a University Professor at CMU; The Harry B. and James H. Higgins Professor of Economics and Finance; Professor, Engineering and Public Policy and The H. John Heinz III School of Public Policy and Management; Director, Green Design Initiative and co-Director of the Carnegie Mellon Electricity Industry Center. **M. Granger Morgan** is Head of the Department of Engineering and Public Policy at CMU, where he is a University Professor; Lord Professor of Engineering; Professor in The H. John Heinz III School of Public Policy and Management; and co-Director of the Carnegie Mellon Electricity Industry Center.*

This work was supported in part by the Alfred P. Sloan Foundation and the Electric Power Research Institute through the Carnegie Mellon Electricity Industry Center (www.cmu.edu/electricity), and by the U.S. National Science Foundation through the Power Systems Engineering Research Center.

¹ B.A Carreras., V.E. Lynch, D.E. Newman, and I. Dobson, *Blackout Mitigation Assessment in Power Transmission Systems*, Proceedings of the 36th Hawaii International Conference on System Sciences, Maui, Hawaii, January 2003, available at <http://eceserv0.ece.wisc.edu/~dobson/PAPERS/publications.html>.

² The mechanisms underlying cascading failures are poorly understood. In an ordinary failure, a disturbance such as a tree brushing against a transmission line damages or endangers a piece of equipment; protective devices open switches to de-energize the equipment; nearby voltages and currents oscillate. Eventually the oscillations die out and the grid returns to a steady state. In a cascading failure, either the oscillations are so large as to endanger other equipment (which trips off line), or the steady state that results places the grid under so much stress that further protective switching operations occur, which leads to more oscillations, still more switching, and so on.

³ The NERC Disturbances Analysis Working Group database can be found at www.nerc.com/dawg/database.html.

⁴ B.A Carreras, D.E. Newman, I. Dobson, and A.B. Poole, *Evidence for Self-Organized Criticality in Electric Power System Blackouts* and J. Chen, J. S. Thorp, and M. Parashar, *Analysis of Electric Power System Disturbance Data*, (both in Proceedings of the 34th Hawaii International Conference on System Sciences, Maui, Hawaii, January 2001) analyzed data from 1984 – 1998 and 1984 – 1999, respectively. We have included the year 2000, and there is no significant difference from the earlier analyses. The NERC database contains 533 logged events; for 491 of these an entry has been made for the amount of power lost; 324 had non-zero power losses. We used both a 2-parameter Weibull exponential distribution and a power law, finding that the probability per event of a loss of greater than MW megawatts is fit by a power law function of the form $P=280/(MW^{1.08})$ for losses above 500 MW. The power law fit is a factor of 7 higher than the Weibull distribution for probabilities of loss of 2000 MW or greater (of which there were 25 events over the 17-year period), and a factor of 325 higher for losses of 4000 MW or more (11 events).

⁵ B.A. Carreras, V.E. Lynch, I. Dobson, and D.E. Newman, *Critical points and transitions in an electric power transmission model for cascading failure blackouts*, CHAOS, 2002, 12 (4), at 985-994.

⁶ B. Drossel and F. Schwabl, *Self-organized critical forest-fire model*, PHYSICAL REVIEW LETTERS, 1992, 69, at 1629-1632.

⁷ M. Ilic and J. Zaborszky, *DYNAMICS AND CONTROL OF LARGE ELECTRIC POWER SYSTEMS* (New York, NY, John Wiley & Sons, 2000).

⁸ C.L. DeMarco, *A Phase-Transition Model for Cascading Network Failure*, IEEE CONTROL SYSTEMS MAGAZINE, December 2001, 21 (6) at 40-51.

⁹ E. Subrahmanian, A.W. Westerberg, S.N. Talukdar, J. Garrett, A. Jacobson, C. Paredis and C. Amon, *Integrating Social Aspects and Group Work Aspects in Engineering Design Education*, INTERNATIONAL JOURNAL OF ENGINEERING EDUCATION, 2003, 19 (1), at 75-80.

¹⁰ A.E. Farrell, M. G. Morgan, and L. B. Lave, *Bolstering the Security of the Electric Power System*, ISSUES IN SCIENCE AND TECHNOLOGY, Spring 2002, 18 (3), at 49-56.

¹¹ H.F. Lipson and D. A. Fisher, *Survivability — A New Technical and Business Perspective on Security*, Proceedings of the 1999 New Security Paradigms Workshop, Caledon Hills, Ontario, Sept. 21–24, 1999, Association for Computing Machinery, New York, NY, available at <http://www.cert.org/research/>.

¹² M.G. Morgan and H. Zerriffi, *The Regulatory Environment for Small Independent Micro-Grid Companies*, THE ELECTRICITY JOURNAL, 2002, 15 (9) at 52-57.

¹³ U.S. Energy Information Administration *Annual Energy Review 2001*, Table 8.2a Electricity Net Generation: Total (All Sectors) 1949-2001, accessed February 28, 2003 from <http://www.eia.doe.gov/emeu/aer/txt/ptb0802a.html>.

¹⁴ Cambridge Energy Research Associates, *Electric Transmission Advisory Service, 2000*, as reproduced in http://www.pserc.wisc.edu/cgi-pserc/getbig/generalinf/presentati/presentati/thomas_march_2003.pdf.

¹⁵ As one example, an information technology-based support of economic trading during normal conditions, separable from the basic survivability mission that is accomplished closer to the end users at the lower voltage levels, could improve the efficiency of use of the EHV/HV system and its resources.

¹⁶ J. Apt and L. B. Lave, *Electric Gridlock: A National Solution*, PUBLIC UTILITIES FORTNIGHTLY, October 1, 2003, 141 (18), at 14-16.