National Aeronautics and Space Administration

System Failure Case Studies

DECEMBER 2007 Volume 1 Issue 10

POWERLESS

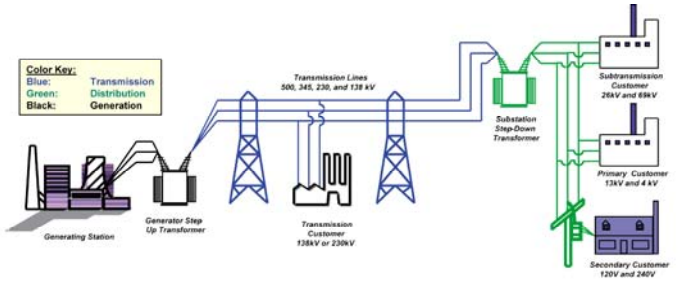
On August 14, 2003, the United States and Canada experienced the largest electrical power blackout in North American history. It was a massive power outage that affected parts of the northeastern U.S. and eastern Canada. Approximately 40 million people in eight U.S. states (about one-seventh of the population of the U.S.) and 10 million people in the Canadian province of Ontario (about one-third of the population of Canada) were impacted. The cost of financial losses related to the outage was estimated at $4 to $10 billion. The shutdown was the result of a monitoring and diagnostic systems failure coupled with communications problems between operations and support staffs, and a lack of systems understanding and planning by utility operators.

BACKGROUND: "THE GRID"

The North American power grid is one large, interconnected system, considered to be one of the greatest engineering achievements of the past 100 years. Its infrastructure is valued at more than $1 trillion, with more than 200,000 miles of transmission lines operating at 230,000 volts and greater, 950,000 megawatts of generating capability, and 3,500 utility organizations serving well over 283 million people.

The electrical power system or grid produces electricity from fuel sources, such as nuclear, coal, oil, natural gas, hydro power, geothermal, etc. Low voltage electricity from the generators (10,000 - 25,000 volts) is "stepped up" to higher voltages (230,000 - 765,000 volts) for transmission over power lines. Transmission lines are interconnected at switching stations and substations to form a network. Electricity flows through the network following the laws of physics—along "paths of least resistance," the same way that water flows through a network of canals. When the power arrives near a load center, it is stepped down to lower voltages for distribution to residential customers (120 and 240 volts) or larger industrial and commercial customers (12,000 - 115,000 volts).

Electrical power cannot easily be stored over extended periods of time, and is consumed immediately after being generated.



Basic Structure of the Electric System.

The demand load on any power grid must be matched by its supply and ability to transmit that power. Any significant overload of a power line or underload/overload of a generator requires utilities to disconnect the line or generator from the grid to prevent hard-to-repair and costly damage.

Although the power system in North America is commonly referred to as the grid, it is actually a group of three distinct power grids or that are electrically independent from each other. They are: the Eastern Interconnection, which includes the eastern two-thirds of the continental U.S. and Canada; the Western Interconnection; and the state of Texas.

In August of 2003, the largest blackout in North America occurred, affecting 50 million people at an estimated cost of $4 - $10 billion

Proximate Causes:

- Load imbalance caused by generator shutdown triggered cascading transmission line failure

Underlying Issues:

- Poor communication of software failures
- Inadequate system planning and understanding
- Tree overgrowth near high voltage lines
- Lack of thorough operator training

What Should Have Happened?

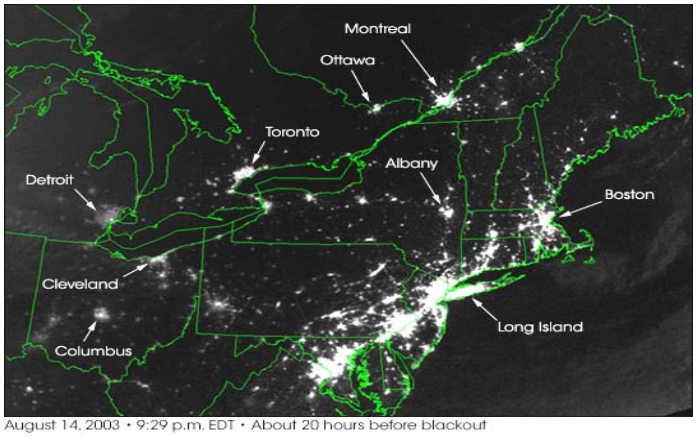
Power lines usually grow longer and sag between transmission towers when they get hotter as they carry more power, reaching a pre-determined height above the ground at a specific power level. To prevent sagging lines from contacting nearby trees resulting in short circuits, the trees are pruned. If the lines touch the trees, they are disconnected by systems which detect the sudden change in power flow from the short circuit. Power changes from an out-of-service line can sometimes cause cascading failures in adjacent areas as other parts of the system see the power fluctuations. These are normally controlled by delays built into the shutdown process and by robust power networks with alternative paths for power to take, which help reduce the size of the ripples. Utility operators at control centers ensure that the power supply, loads (customers' power demand or use), and transmission line capacity, are balanced so that the system is in a state where no single fault can cause it to fail. If a failure occurs, operators are required within 30 minutes to obtain more power from other regions or shed load (meaning cut power to some areas) as a last resort to prevent a system collapse.

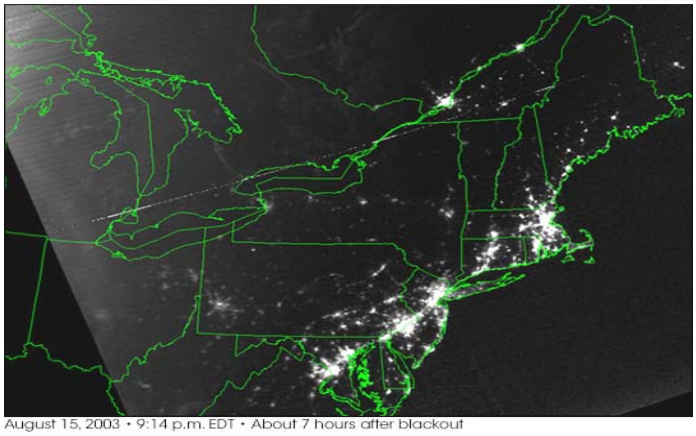
Operators use sophisticated monitoring and control computer systems with backups, which issue alarms when faults occur in the transmission or generation system. They also employ power flow modeling tools to help them analyze their grid's status, find parts that are overloaded, and predict worst possible failures, so as to prevent any transmission or generator damage. If their primary and backup computer systems fail, operators are required to monitor their networks manually and invoke pre-planned contingencies if needed. They also notify adjacent area operators of their status so that they determine the effects of the failures on their systems. Backing up the operators are regional coordinating centers which collect information from adjacent areas and perform further checks on the system, looking for possible failures and alerting operators in different systems.

WHAT HAPPENED?

The Ohio Connection

The blackout started with a series of events in Northern Ohio between 12:15 and 4:06 p.m. on August 14, 2003. It was a normal day – the electrical load was moderately high due to the air conditioning demand on a hot summer day. Shortly after noon, Eastlake 5, a power station generator unit owned by FirstEnergy Corporation, an electrical utility servicing the Ohio area, tripped and shut down automatically. The unit tripped when an operator attempted to increase the unit's reactive power output but the power output exceeded the protection system limits and shut down automatically. This supply drop caused a 1,500 megawatt load imbalance to the Cleveland and Akron areas. FirstEnergy's monitoring system failed to alert operators, who were not able to see the problem and correct the imbalance. The imbalance strained and overheated several Cleveland-Akron 345-kV and 138-kV transmission lines, causing them to sag and fail after touching overgrown trees. The multiple failures resulted in a large decrease in available power which caused a heavy power surge to a key 345-kV transmission line called the Sammis-Star line, which later failed after contacting trees.





Satellite Photos of Northeastern U.S. and Canada Before and After the Blackout.

Cascading Failures

The loss of the Sammis-Star line instantly created major and unsustainable burdens on other transmission lines throughout northeastern Ohio and triggered cascading failures throughout Northeastern U.S. and Canada. The cascade started at 4:06 p.m. and spread `in less than seven minutes throughout an area of roughly 9,300 square miles, bounded by Lansing, Michigan, Sault Ste. Marie, the shore of James Bay, Ottawa, metropolitan New York and Toledo. Automatic protective relays in lines and power generating units located in Cleveland, Toledo, New York City, Buffalo, Albany, Detroit, and New Jersey were tripped. More than 508 generating units at 265 power plants, including 22 nuclear power plants, shut

down during the massive outage. FirstEnergy's operators' lack of situational awareness of the events happening in the Cleveland–Akron area was such that they did not execute their contingency plans or alert neighboring control centers to stop the cascade.

Proximate Cause

The unexplained shutdown of a generation unit at Eastlake 5 station resulted in a load imbalance that went unnoticed by operators. The imbalance strained transmission lines and eventually triggered a cascade of line shutdowns as heavy power surges overheated wires, causing them to sag, contact trees below and fail.

Underlying Issues

Failed Response to Software Errors

A "race condition" or software timing error in FirstEnergy's UNIX-based XA/21 energy management computer was found to be the primary cause of the grid event alarm failure. After the alarm system failed silently, the unprocessed events started to queue up and crashed the primary server within 30 minutes. This triggered an automatic transfer of all applications, including the stalled alarm system, from the primary to the backup server, which likewise became overloaded and failed. By 2:54 pm, all energy management applications on both servers stopped working. As a result the screen refresh rate of the operators' computer consoles slowed down from 1-3 seconds to 59 seconds per screen.

FirstEnergy IT personnel knew of the system crashes but did not notify the operators. They responded to the system's automatic pages after the primary system crashed and performed "warm-reboots" on both primary and back-up systems. However the reboots were not successful in refreshing the operators' display consoles. The operators only determined they had problems when data from phone calls received from customers, nearby utilities, and their regional coordinating center calls did not match the information on their screens.

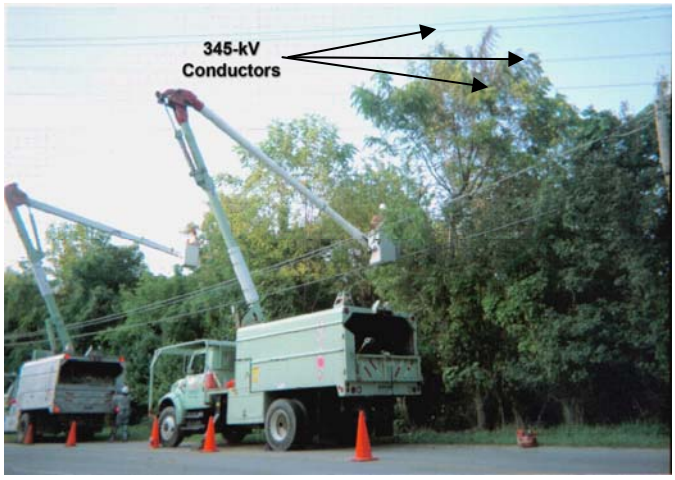
THE BLACKOUT MIGHT HAVE BEEN PREVENTED IF FIRSTENERGY'S OPERATORS ONLY KNEW WHAT WAS HAPPENING WITH THEIR GRID

Inadequate System Understanding and Planning

FirstEnergy operators and its regional coordinating center counterparts did not have a macro-view understanding of their system, leaving them unprepared to manage incidents or contingencies. Long-term operational planning studies and simulations conducted by FirstEnergy in 2002 and 2003 were not thorough enough to understand the Cleveland-Akron grid vulnerabilities and its effects on operations, particularly the 1,500 megawatt power loss from the Eastlake 5 generator. They incorrectly assumed that all transmission lines would be in service at all times. Sensitivity analyses that would have revealed that the voltage criteria triggering their alarms were set too low and severely undermined their entire monitoring system were never performed. They had no emergency response plan in place to deal with failures such as the five transmission lines and the Eastlake 5 generator shutdowns.

Overgrown Trees

FirstEnergy failed to follow its own tree trimming policies (also known as vegetation management), which resulted in the failure of the three 345-kV transmission lines and one 138-kV line in its Ohio service area.



345-kV Lines Contacting Overgrown Trees in Ohio.

Lack of Training and Operator Error

There was a lack formal training by the operators in handling major disturbance situations which contributed to their hesitation to pursue appropriate courses of actions. FirstEnergy's regional coordination center, (Midwestern Independent System Operator or MISO), was not able to warn them of the impending situation since its diagnostic systems had problems that day. The on-duty reliability analyst at MISO had to turn off their system's auto trigger and alarm functions to troubleshoot the system but forgot to turn them back on afterwards until after the blackout.

Aftermath

A year after the blackout, FirstEnergy took several steps to fix their systems. They replaced the GE XA/21 computer system with another system that included features such as: improved alarm functions for tripped transmission lines; faster and more accurate diagnosis and contingency analysis modules; and an improved user interface with visual cues to help operators identify transmission line problems faster. The reliability coordination center system was also upgraded with a user interface that visu-

ally shows grid status and key lines, generators and equipment failures. Parallel processing was incorporated in its contingency analysis program to produce results more quickly. A dynamic "map board" was installed in control centers for wide-area system visualization by controllers. Finally, backup system control centers were designed and built to address the unavailability of primary control centers.

Furthermore, FirstEnergy rewrote its operator procedures and training programs to reflect the new systems, created a certification program to ensure operators fully understand their networks and systems as well as improve their reactions to emergency situations. It established new communication protocols for computer system repair and maintenance downtimes between their operations and IT staffs. An emergency response plan was created that focused on controlled load reductions of up to 1,500 megawatts for the Cleveland-Akron area. Tree trimming procedures and compliance were tightened.

Applicability To NASA

Project management and mission teams regularly face challenges integrating hardware/software system design, operator interface, and communication sub-systems. Overall design requirements must incorporate mission support needs and provide accurate, real-time, system wide operational status. It is also important for users of mission critical computer systems to verify output with other reliable, trusted data to mitigate input device or processing anomalies. Modeling and simulation studies must be robust enough to determine and understand how well space missions are planned and how systems work in both nominal and off-nominal environments. Considering all possible scenarios of a mission increases team situational awareness and helps in developing effective contingency plans. Formal education, on-the-job training, and mission rehearsals should go hand-in-hand in imparting knowledge and skills to personnel as well as developing the right instincts to emergency situations. Certification provides greater confidence that operators know how their system works. Lastly, the value of team communications cannot be overemphasized especially when lives and mission success are at stake.

Questions for Discussion

- How robust are your emergency plans? Have all possible accident and/or contingency scenarios been considered?
- How do your systems and their operators perform in off-nominal situations?

Questions for Discussion (cont)

- How can situational awareness be improved in relation to mission operations and maintenance?
- How well and frequent is communication between your team members with different mission roles?

References:

"Northeast Blackout of 2003." Wikipedia, The Free Encyclopedia. <http://en.wikipedia.org/wiki/2003_North_America_blackout>.

"Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations." U.S.-Canada Power System Outage Task Force. <https://reports.energy.gov/ BlackoutFinal-Web.pdf >.

"The August 14, 2003 Blackout One Year Later: Actions Taken in the United States and Canada To Reduce Blackout Risk." Natural Resources Canada and the U.S. Department of Energy. <http://www.nerc.com/~filez/blackout.html >

"August 14, 2003 Blackout - Summary Based on Interim Report of the United States – Canada Power Outage Task Force November 19, 2003." U.S.-Canada Power System Outage Task Force. <http://www.iwar.org.uk/cip/resources/blackout-03/Blackout-Report-Presentation-11-19-03.ppt>

"EO Newsroom: New Images - Blackout Leaves American Cities in the Dark." Earth Observatory. <http://earthobservatory.nasa.gov/Newsroom/NewImages/images.php3?img_id=16273 >.

"NERC Recommendation Verification Team MISO Report - July 12, 2004." North American Electric Reliability Corporation (NERC). <ftp://www.nerc.com/pub/sys/all_updl/docs/blackout/MISO_Report_0704.pdf>.

"NERC Recommendation Verification Team FirstEnergy Report - July 13, 2004." North American Electric Reliability Corporation (NERC). <http://earthobservatory.nasa.gov/Newsroom/NewImages/images.php3?img_id=16273 >.

System Failure Case Studies
A product of the NASA Safety Center

Executive Editor: Steve Wander stephen.m.wander@nasa.gov

To view this document online and/or to find additional System Failure Case Studies, go to http://pbma.nasa.gov