Annual Safety En Banc
October 19, 2016

Case Study: The 2003 Northeastern Blackout

On August 14, 2003, large portions of the Midwest and Northeast United States and Ontario, Canada, experienced an electric power blackout. The outage affected an area with an estimated 50 million people and 61,800 megawatts (MW) of electric load in the states of Ohio, Michigan, Pennsylvania, New York, Vermont, Massachusetts, Connecticut, New Jersey, and the Canadian province of Ontario. The blackout began a few minutes after 4:00 p.m. Eastern Daylight Time (16:00 EDT) and power was not restored for 4 days in some parts of the United States. Parts of Ontario suffered rolling blackouts for more than a week before full power was restored. Estimates of total costs in the United States range between $4 billion and $10 billion (U.S. dollars). In Canada, gross domestic product was down 0.7% in August, there was a net loss of 18.9 million work hours, and manufacturing shipments in Ontario were down $2.3 billion (Canadian dollars).[1]

After transmission lines in Ohio came into contact with overgrown vegetation, a series of human and software errors caused the cascading outage. The blackout affected 50 million people, and shut down the region's large electric customers, including airports, public transportation systems, ATMs, cell phone towers, nuclear plants, municipal traffic control, pharmacies, hospitals, potable water systems, sewage systems, and manufacturers including automotive, steel, chemical, and pharmaceuticals.

According to the U.S.-Canada Power System Outage Task Force, for approximately 90 minutes at the beginning of the 2003 blackout, FirstEnergy control room operators were unaware of the magnitude of the event despite numerous inbound calls from Midwest Independent System Operator, PJM Interconnection, American Electric Power, and customers (including nuclear plants), because there was no evidence of a malfunction registering on their internal systems.[2]

The purpose of presenting this case study for discussion at this Safety En Banc is neither a post mortem on the response of control room operators during the blackout or an examination of how to prevent similar control room errors in California. The purpose is to gain a better understanding of potential cascading effects in order to prepare for an appropriate regulatory response, an appropriate stakeholder response, and most importantly an appropriate infrastructure provider response.

There are certain aspects of the blackout that are relevant to any discussion of interconnected infrastructure, including but not limited to:

The blackout affected at least eight oil refineries in the United States and Canada. In order to avert a gasoline shortage in Metropolitan Detroit, Michigan's Governor issued an Executive Order suspending

[1] U.S.-Canada Power System Outage Task Force Report, April 2004, at 1.
[2] U.S.-Canada Power System Outage Task Force Report, April 2004, at 65-66.

the environmental regulations applicable to gasoline in order to facilitate extra manufacture and imports of gasoline into Southeastern Michigan;[3]

Some areas lost water pressure when electricity-driven pumps lost power, depriving residents of potable water. New York City's water system is largely gravity-driven, but residents in high-rise buildings lost access to potable water when their buildings' pumping systems failed;[4]

After the blackout of 1977 resulted in large releases of untreated sewage, New York City installed backup generators in most of its sewage treatment plants, save one: the 13th Street Pump Station, allegedly due, in part, to community resistance. During the 2003 blackout, raw sewage was released from the 13th Street Pump Station and from other treatment facilities where the backup generators were faulty or inoperable;[5]

A 2006 study[6] of the New York City Department of Health and Mental Hygiene's (DOHMH) response to the blackout noted that, despite the presence of backup generators, four of New York City's seventy-five hospitals were temporarily without electricity;

In addition, DOHMH telephone systems lacked sufficient capacity and backup power to operate for the duration of the blackout, making it difficult for public health employees to determine where to report during the emergency;

Due to the blackout, Republic Engineered Products in Lorain, Ohio lost the ability to cool molten metal, which burned through the building, starting fires that were seen throughout the city;[7]

911 service was temporarily disrupted in New York City as Verizon's backup generators failed.[8]

Session 1 – Information & Communication between Interconnected Infrastructure Providers and Stakeholders

1. During the 2003 blackout, communications systems at New York's DOHMH failed due to the lack of adequate capacity and backup power. In addition to communications *between* infrastructure providers, do infrastructure providers and public safety officials have adequate communications capability for their own staff in the event of a prolonged power outage?
2. Does an entity need to be large or well-known in order to pose an interconnected infrastructure risk? With the speed of innovation, especially innovation in bits, not atoms, is there a possibility that a threat to interconnected infrastructure might not be known or knowable until it is too late?

[3] http://www.michigan.gov/formergovernors/0,4584,7-212-57648_21974-73850--,00.html
[4] http://www.nytimes.com/2003/08/16/nyregion/the-blackout-water-up-on-the-top-floors-powerless-and-parched.html
[5] http://www.nytimes.com/2003/08/28/nyregion/sewage-spill-during-the-blackout-exposed-a-lingering-city-problem.html
[6] Blackout of 2003: Public Health Effects and Emergency Response, available at: http://www.ncbi.nlm.nih.gov/pmc/articles/PMC1497795/
[7] The Economic Aspects of the 2003 Blackout, Electricity Consumers Resource Council, April 2004, at 6.
[8] http://www.nytimes.com/2003/10/29/nyregion/after-blackout-a-call-for-a-911-overhaul.html

3. What do infrastructure providers need to know about one another in order to promote mutual reliability and safety?
4. Do infrastructure providers know what questions to ask?
5. Does a full understanding of interconnected infrastructure risk require the sharing of competitively sensitive information?
6. Are there any industries, particular segments of infrastructure, or political subdivisions that you are working with or wish you were working with to address shared challenges concerning interconnected infrastructure?
7. Would your answers to any of the questions asked today be different if the interconnected infrastructure risk or failure was caused by cyber-attack or other hostile act, rather than human error or overgrown vegetation? If the failure concerned a different type of infrastructure?

Session 2 – Managing Interconnected Infrastructure Risk during Technological Change

1. During the 2003 blackout, New York City's public transportation systems stopped working. Are there any aspects of public transportation systems (defined broadly) in 2016 that provide greater resilience in the event of a loss of interconnected infrastructure?
2. Smartphones; increased reliance on the internet for information and services; Wi-Fi hotspots; electric vehicles; TNCs; roof-top solar; how do these or other recent developments affect interconnected infrastructure risk?
3. Does an entity need to be large or well-known in order to pose an interconnected infrastructure risk? With the speed of innovation, especially innovation in bits, not atoms, is there a possibility that a threat to interconnected infrastructure might not be known or knowable until it is too late?
4. How do unknowns concerning technological change, including, e.g., software and hardware changes, market disruption, customer adoption, and regulatory response, affect the ability to plan for interconnected safety and reliability?
5. What strategies will ensure that interconnected infrastructure risk management matches the speed of innovation?
6. Are there any industries, particular segments of infrastructure, or political subdivisions that you are working with or wish you were working with to address shared challenges concerning interconnected infrastructure?
7. Would your answers to any of the questions asked today be different if the interconnected infrastructure risk or failure was caused by cyber-attack or other hostile act, rather than human error or overgrown vegetation? If the failure concerned a different type of infrastructure?

Session 3 – What is the Regulatory Response When Interconnected Infrastructure Risk Surrounds Regulated and Unregulated Industries?

1. Should government agencies have basic information ready for release immediately in case of infrastructure-related emergencies that may impact communications systems?
2. Should government agencies or elected officials convene unregulated stakeholder groups to review best practices for infrastructure management?

3. Should California's Governor or other government officials or agencies consider, in advance, whether certain laws should be temporarily waived in the event of an infrastructure-related emergency, in order to speed response time? If so, which ones? Is it possible, or desirable, to make such determinations in advance?
4. The Commission can compel some interconnected infrastructure providers to share information, but other providers are beyond the reach of the Commission's jurisdiction. When cascading risk between interconnected infrastructures is potentially catastrophic, is there a regulatory role for risk management even when an industry or provider is otherwise unregulated?
5. If so, what state or federal agency or agencies should play a role, and what should that role be? If not, what happens when an infrastructure provider does not want to share information?
6. Are there any industries, particular segments of infrastructure, or political subdivisions that you are working with or wish you were working with to address shared challenges concerning interconnected infrastructure?
7. Would your answers to any of the questions asked today be different if the interconnected infrastructure risk or failure was caused by cyber-attack or other hostile act, rather than human error or overgrown vegetation? If the failure concerned a different type of infrastructure?

Presentations – the questions above are intended to stimulate discussion during the separate breakout sessions. Each breakout session will have two presenters (a CPUC Commissioner along with an energy utility president) who will present their findings when the En Banc reconvenes in the auditorium. The presentations' focus must be this – if a situation similar to that which precipitated the 2003 blackout were to happen in California today:

Do interconnected infrastructure providers have the information they need about each other, and sufficiently robust lines of communications, to promote mutual reliability and safety and limit the impact of a cascading failure? (Breakout session 1);

Compared to 2003, do recent technological changes make it easier or more difficult to prevent cascading effects? What are the challenges and opportunities posed by the speed and unpredictability of technological change? (Breakout session 2); and

Are there steps that can be taken now at various levels of California government to ensure that, in the event of an incident, agency roles are clear and resources are available? (Breakout session 3)