ESTABLISHING PUBLIC POLICY AS A PRIMARY CAUSE OF ENGINEERING FAILURE IN NATIONAL INFRASTRUCTURES

Christopher W. Johnson

Glasgow Accident Analysis Group[1]

Keywords: root cause analysis; market deregulation; electricity distribution.

Abstract

On the 14th August 2003, a complex combination of immediate events and longer term vulnerabilities led to a domino-effect in which 50 million people had their power supplies interrupted. Consequent losses were between $5-10 billion. It is, therefore, one of the most serious disruptions to a national power distribution network. The causes of this infrastructure failure included technical issues to do with network capacity and the algorithms used to predict potential distribution problems. It also had managerial and human factors causes; these arguably included an over-reliance on automated monitoring systems. The infrastructure failure also stemmed from governmental and regulatory intervention, which led to problems in the operation of the energy market. The following paper applies accident investigation techniques to represent and reason about the complex interactions between these causes. In particular, we use Violation and Vulnerability (V2) diagrams to map out arguments for and against market deregulation as a causal factor in engineering failures.

Introduction

The North American electricity network brings together some 3,700 utility organizations providing more than 320,000 kilometers of transmission lines. It provides more than 950,000 megawatts of generating capability for more than 100 million customers. The complexity of this system has led to considerable investment in infrastructure reliability. In spite of these precautions, a 'blackout' on the 14th August 2003 affected almost 50 million people and 61,800 megawatts of load in the US states of Ohio, Michigan, Pennsylvania, New York, Vermont, Massachusetts, Connecticut, New Jersey and in the Canadian province of Ontario. Power was lost for 4 days in parts of the United States and Ontario suffered rolling blackouts for more than a week [8].

This incident has been the subject of considerable controversy. Federal [9] and State investigations [7], commercial organizations [1], pressure groups [5] and media organizations [4] have all published alternate accounts. Harris [3] argues that it has become "a Rorschach test which every viewer interprets as evidence to support his or her concerns about the problems in today's electric industry". Many of the differences that distinguish these accounts stem from the authors' attitudes towards the impact that market deregulation has upon the reliability of complex systems. Some authors have argued that competition cannot be relied upon to provide social goods, including infrastructure reliability. They support closer Federal and State regulation. Others blame political intervention as a cause, rather than a remedy, of infrastructure failure. Very few of these accounts explain the mechanisms by which public policy created preconditions for the infrastructure failure. In contrast, the

[1] Glasgow Accident Analysis Group, Department of Computing Science, University of Glasgow, Glasgow, G12 8QQ, Scotland, U.K. johnson@dcs.gla.ac.uk, http://www.dcs.gla.ac.uk/~johnson

following pages use accident investigation techniques to sketch arguments for and against deregulation as a cause of the blackout. The intention is to cut through the rhetoric and look at the engineering consequences of different forms of market intervention.

Immediate Events

The North American distribution network was protected by an array of technical and organizational defenses. For example, the Midwest Independent System Operator (MISO) deployed State Estimation (SE) and Real Time Contingency Analysis (RTCA) systems shortly before the blackout. MISO was a reliability organization set up by a group of utility companies. The SE and RTCA software was intended to help MISO member companies meet North American Electric Reliability Council (NERC) Policy 2.A on Transmission Operations; "All CONTROL AREAS shall operate so that instability, uncontrolled separation, or cascading outages will not occur as a result of the most severe single contingency" [8]. The systems used Monte Carlo techniques to assess the N-1 state of the network. Information about the current state of N network components was used to predict the consequences if the network were reduced to N-1 components. RTCA software was intended to run automatically, checking the state of the system every five minutes.

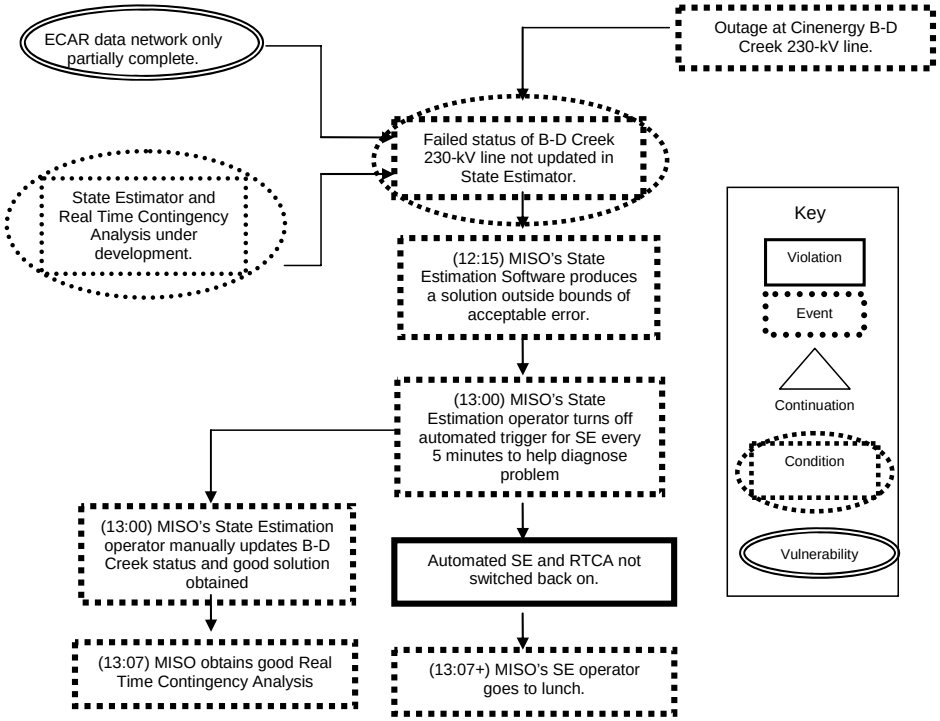

Figure 1: The Failure of MISO's State Estimator and Real-Time Contingency Analysis

Figure 1 uses V2 (violation and vulnerability) diagrams to model the loss of RTCA and SE, which "prevented MISO from promptly performing pre-contingency 'early warning' assessments of power system reliability over the afternoon of August 14" [8]. In this diagram, double ellipses denote the vulnerabilities that threaten safety. For example, the East Central Area Reliability Coordination Agreement (ECAR) network was only partially completed. This created a potential vulnerability because there was no way for the SE and RTCA software to automatically detect the state of some network components. The vulnerability was exposed when there was an outage on Cinenergy's Bloomington-Dennis (B-D) Creek 230-kV line. The failure of this network component is shown as an event denoted by a dotted rectangle. MISO's State Estimator did not have access to sensor data in this area and so it could not accurately model the state of the distribution network. The V2 diagram also shows how an operator turned off the SE software to identify the cause of the discrepancy between the model and the available sensor values. This led to a violation of standard

operating procedures, denoted by a bold rectangle, when the operator neglected to restart the automated SE and RTCA monitoring functions.

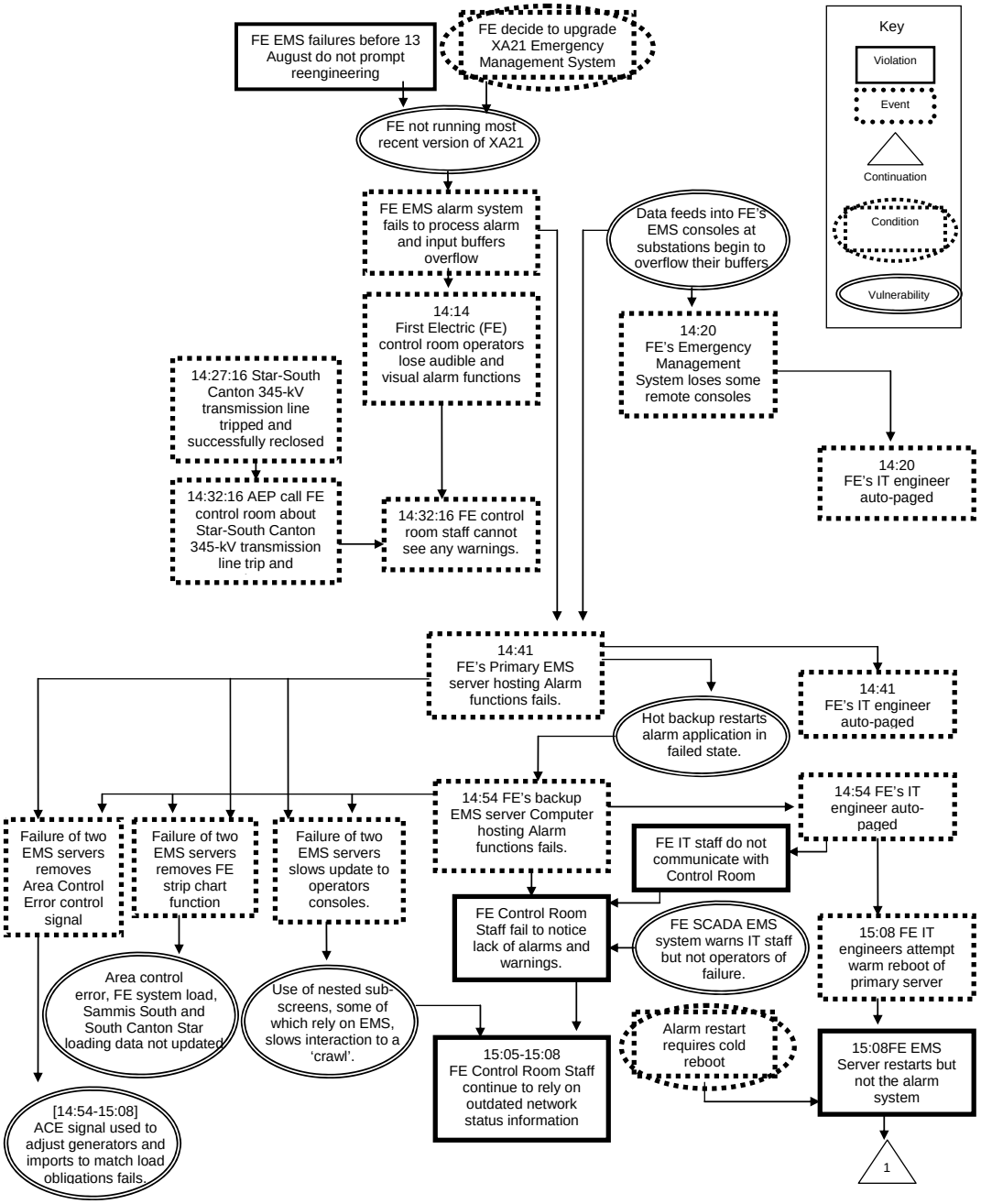

Figure 2: The Failure of First Electric (FE's) Emergency Management System

The loss of MISO's monitoring systems was compounded by events illustrated in Figure 2. In addition to MISO's SE and RTCA applications, the First Electric generating company also operated an Emergency Management System (EMS). Previous reliability problems had persuaded the utility to upgrade their EMS. In the meantime, FE was not running the most recent version of the software. Shortly before the blackout, substation consoles began to experience buffer overflows. By 14:20, FE's IT engineer had been 'autopaged' to restore the EMS terminals. Meanwhile, further buffer overflows on the central EMS system disabled warnings to control room staff about potential network failures. In consequence, operators could not use their systems to substantiate warnings from other companies when the Star-South Canton 345-kV line tripped at 14:27. The lack of EMS warnings together with the failure of MISO's SE and RTCA applications gradually eroded the situation awareness of staff monitoring the generation and power distribution systems. A 'hot backup' server took

over FE's EMS while their IT engineer was again automatically paged. However, the hot restart used duplicate software. The original buffer overflows went unresolved so the redundant server failed in the same way as the primary EMS system. The FE IT engineers eventually attempted a 'warm' reboot of the primary EMS server. This did not automatically restart the alarm system, which required a cold reboot.

FE's IT staff did not pass on information about the EMS failures to control room staff. Figure 2 represents this violation of standard operating procedures. It also shows how the EMS server failures slowed updates to the operators' screens. The loss of the EMS servers also removed FE's strip chart function which provided users with an overview of network loading. It also disabled the Area Control Error Signals that helped to control automated adjustments in generating and importing capacity.

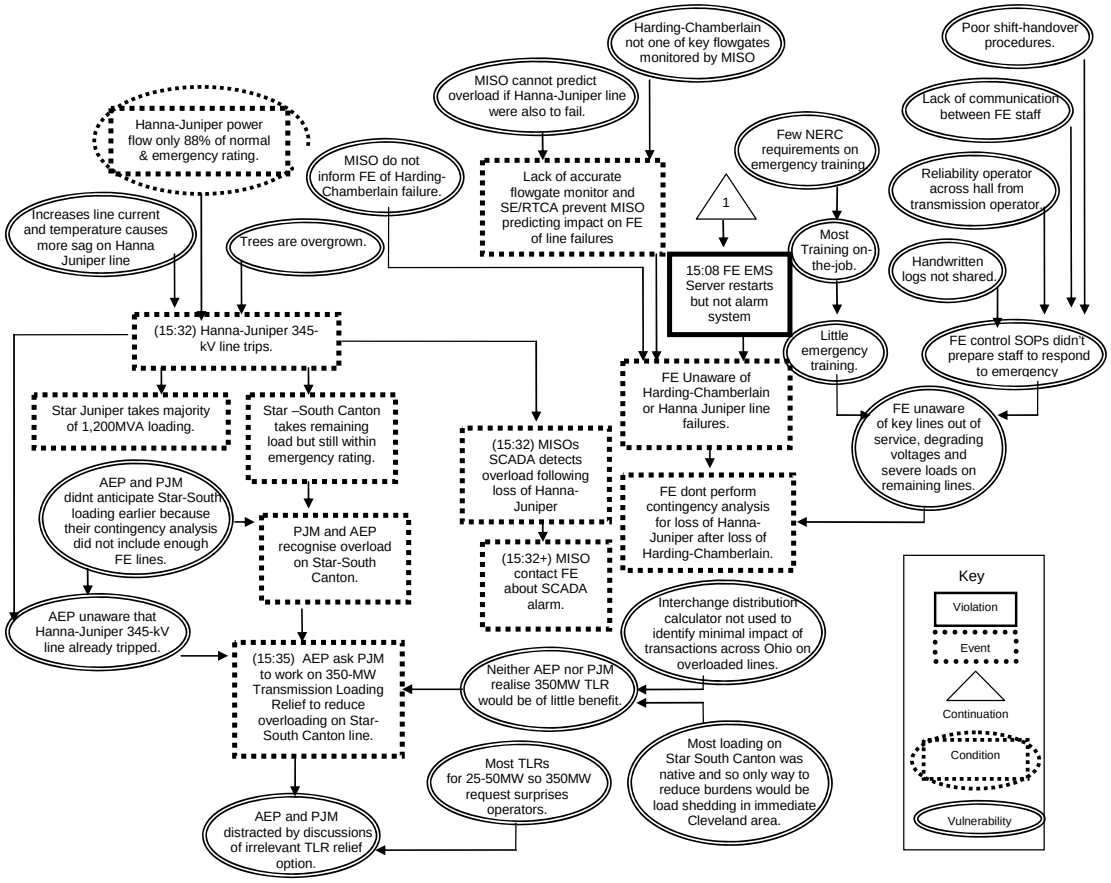

Figure 3: Consequent Network Failures and Attempts to Relieve Transmission Loading

Figure 3 shows how FE operators' situation awareness was further compromised by the lack of shift handover procedures, the difficulty in sharing handwritten logs, the lack of communication between key staff. It also shows how the lack of training in emergency procedures may have stemmed from limited NERC guidance. This provides an initial example of the ways in which public policy may have contributed to particular events leading to the blackout. In this case, the NERC's self-regulatory framework arguably did not provide sufficient guidance for the utilities in how to prepare their operators for the events that unfolded on the 14th August.

The V2 diagram also shows how the loss of monitoring equipment prevented operators from observing a series of line failures. The initial loss of the Harding-Chamberlain 345-kV line increased loading on the Hanna-Juniper 345-kV line. The rise in power loading caused increasing core cable temperatures on the Hanna-Juniper network that led the cables to sag.

This reduction in cable tension made short-circuits more likely as the lines came into contact with vegetation, which had not been cut back enough over the previous Summer months.

MISO's Supervisory Control and Data Acquisition (SCADA) system detected the overload and staff began to warn FE. However, the failure of Hanna-Juniper after the loss of Harding-Chamberlain placed increased loads on the Star-Juniper and Star-South Canton lines. Another utility company, AEP, and their associated reliability organization, PJM, recognized the increased loading on the Star-South Canton line. However, they were not alerted to the potential consequences of this failure. Their N-1 contingency software did not have access to the necessary data about the state of FE's lines to clearly predict the consequences of these different failures in the AEP and FE networks. AEP attempted to reduce the load on Star-South Canton by asking their reliability coordinator for Transmission Loading Relief (TLR). Such procedures can take more than an hour and usually involve 25-30MW rather than the 350MW requested. The AEP request was, therefore, delayed by repeated requests to confirm the size of the TLR.

The Star-South Canton 345-kV lines tripped as a result of the increased loading created by the failures of the Harding-Chamberlain and Hanna-Juniper lines. Voltage levels began to degrade and flows increased on the 138-kV system towards Cleveland and on the Sammis-Star line which remained the only 345-kV route into the city from the South. The failure of South-Star Canton lines forced a complete revision of the AEP and PJM contingency planning. They had worried about the consequences of a Sammis-Star failure on South-Star Canton rather than the impact of the loss of South-Star Canton on the Sammis-Star lines. As the 138-kV system started to trip both organizations began to realize the extent of the emergency but could not identify viable solutions. Calls from customers also began to alert FE staff to the problems in their section of the network. These were confirmed by direct observations from substations. Eventually, after 15:45 the FE shift supervisor informed their manager that they may be 'losing the system'. The failure of the Sammis-Star 345-kV line following South-Star Canton, Hanna-Juniper and Harding-Chamberlain led to weak voltages in Ohio and power flows that created a further domino effect that extended across North America.

Public Policy and Failures of Infrastructure Engineering

Public policy is defined to be guidelines or rules that results from the actions or lack of actions of governmental and quasi-governmental entities. These rules directly created the conditions that led to the blackout on August 14th 2003. For example, the NERC was established following the Northeast blackout in 1965 as a non-governmental mechanism for using 'peer pressure' to establish reliability standards. They coordinate the development of tools to enhance infrastructure reliability, including data exchange systems. Their objectives include maintaining a balance between generation and demand as well as limiting the thermal stresses that arise from dynamic power flows through network components. NERC policies influenced the events, illustrated in previous V2 diagrams. For instance, Figure 4 uses a V2 diagram to show how their role in promoting reliability training can be linked back to vulnerabilities in Figure 3. FE personnel lacked emergency training that might have prepared them for the failures they faced on the afternoon of 14th August.

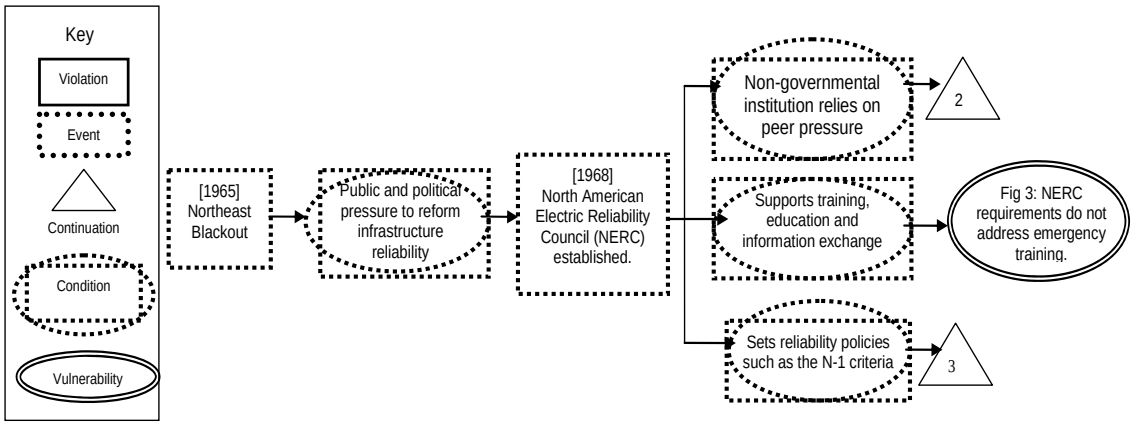

Figure 4: Conditions Created by the Development of NERC

In 1978, the U.S. Congress passed the Public Utility Regulatory Policy Act (PURPA). The aim was to encourage investment in more efficient technologies and, in consequence, to lower costs. These regulations enabled new entrants to sell energy without many of the reliability obligations that governed established companies. Delgado (2005) argues that this increased competition reduced the earnings of existing utility companies. They then had fewer profits to reinvest in infrastructure projects. The changes in market structure also fuelled investor uncertainty over infrastructure initiatives. The uncertainty continued in 1996 with Federal Energy Regulatory Commission (FERC) Order 888. New industry participants, known as energy marketers, gained access to the distribution grid under the same conditions as the utilities' native generating loads. Figure 5 uses the V2 notation to characterize some of these changes in public policy. As can be seen, the FERC order and PURPA were intended to 'reduce costs by increasing competition', to encourage 'external investment in new technology', to ensure that 'new entrants didn't have the same vertical integration with the distribution network' and to provide access to the gird 'under the same terms as utility's native generating loads'.

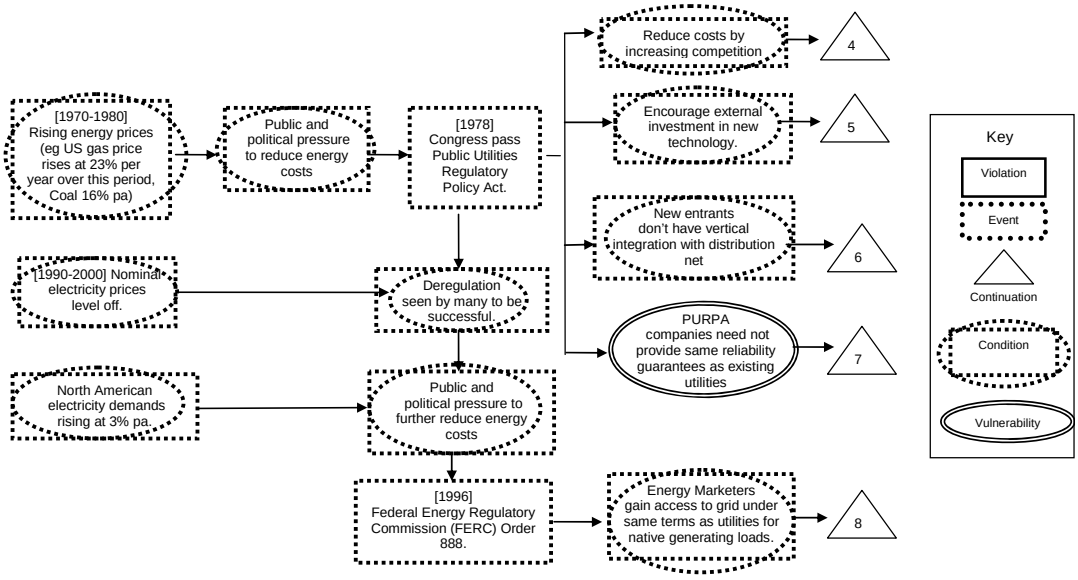

Figure 5: Changes to the North American Electricity Market Structure

Figure 6 sketches links between the public policy issues of Figure 5 and the particular engineering events that took place during the blackout of August 14th. The changes introduced by PURPA and Order 888 arguably made it more difficult for reliability organizations, such as MISO and PJM, to predict energy movements. This led to the drafting of Transmission Loading Relief (TLR) procedures. The previous V2 diagram includes a link

between the development of these procedures and the request at 15:35 from AEP to PJM to work on a 350-MW TLR to reduce the burdens on Star-South Canton line. This shows how our analysis can identify positive as well as negative outcomes from public policy decisions. The development of TLR procedures in response to market changes provided the transmission and reliability companies with ways of seeking relief under the uncertainties of the market. It was unfortunate, as we have seen from figure 3, that these procedures were insufficient to address the particular problems that arose on August 14th. Under other circumstances, with sufficient warning from RTCA tools, it might well have been possible to use the TLR procedures to mitigate the growing problems in the network.

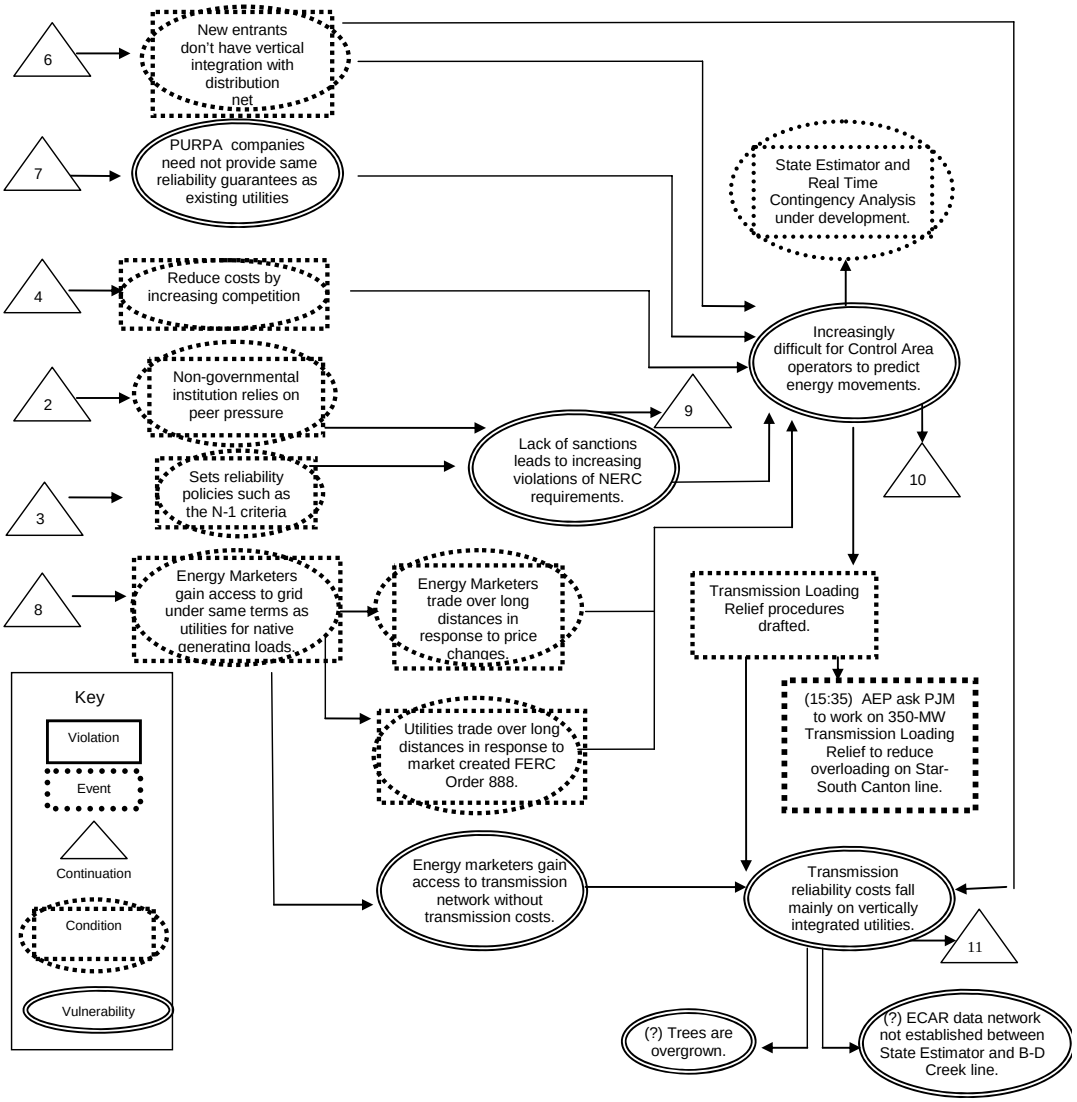

Figure 6: Instabilities in the Market Structure Prior to 2003

Figure 6 captures further links between public policy and infrastructure engineering. Vertically integrated utilities were caught between the demands of reducing costs in a competitive market place while at the same time meeting reliability obligations that were different from those of their competitors. The resulting commercial pressures may have contributed to problems in vegetation management near power lines. The impact of this failure is represented in Figure 3's V2 diagram. Similarly, a fairer distribution of reliability costs may have financed full integration of the sensor data network, for instance between the MISO State Estimator and Bloomington-Davis Creek 230-kV line. The question marks used to annotate Figure 6 indicate that additional evidence is required to support these arguments.

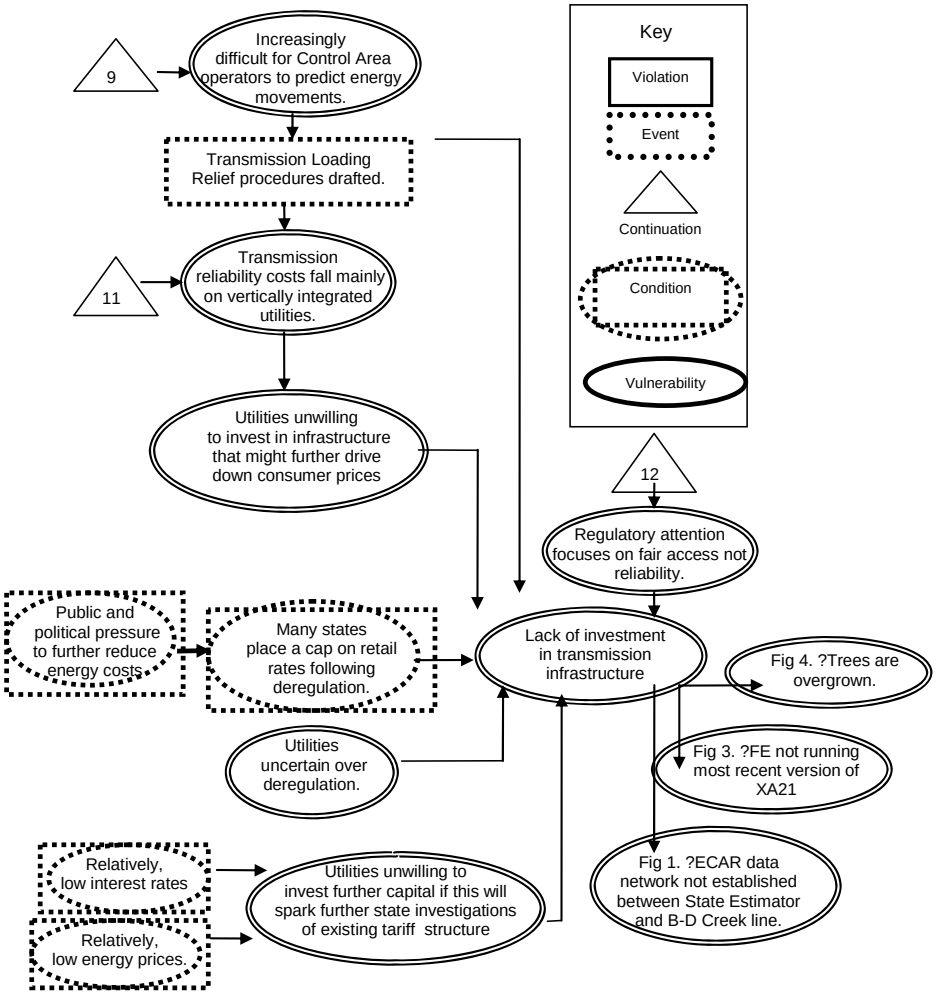

Figure 7: Deregulation as a Causal Factor in the August Blackout

Hughes [5] has argued that "deregulated companies are averse to building new generation that will drive down consumer prices and, therefore, their profits". Figure 7 builds on this argument to show how market deregulation created the conditions that led to the 14th August blackout. Utilities were dissuaded from commissioning infrastructure improvements because they might have been forced into a more general review of their rate structure in order to justify any additional funding. They were reluctant to trigger these reviews in a partially-deregulated market, given relatively low interest rates and oil/gas prices. Further barriers to investment were created by the cap that many states placed on retail rates following deregulation. This limited the utilities' ability to recover investments in new transmission through price increases to retail customers. The regulatory focus on ensuring open access to deregulated markets also diverted attention on reliability issues. These factors combined to create the conditions for the engineering failures introduced in the first half of this paper. Figure 7 shows how deregulation arguably starved the industry of necessary infrastructure investment. This affected everything from the development of IT data networks, such as the ECAR system introduced in figure 1, through to the provision of EMS systems and vegetation management, illustrated in Figure 3.

Many supporters of deregulation reject the arguments captured in Figure 7. Harris has argued that "competition enhances, rather than compromises, grid reliability. Competition, supported by regional grid managers brings stronger information, grid management tools and locational prices that make all market participants partners in reliability protection and reinforce and improve grid reliability" [3]. In this view, the changes of the 1980s and 1990s helped utilities to lower costs and increase efficiency. The reduction in capital outlay by the utilities in the

years immediately before the blackout can be explained in terms of a reduction in *over capacity* from earlier investments based on over-estimates of future demand. Increased energy flows were not caused by increased competition but by artificial rate caps imposed by States at a time when the costs of fossil fuels were rising. Environmental pressure groups also prevented generating capacity from being developed close to the point of need. Existing utilities had to look for cheaper energy sources from other regions. This created the large electricity flows that increased pressure on the distribution infrastructure.

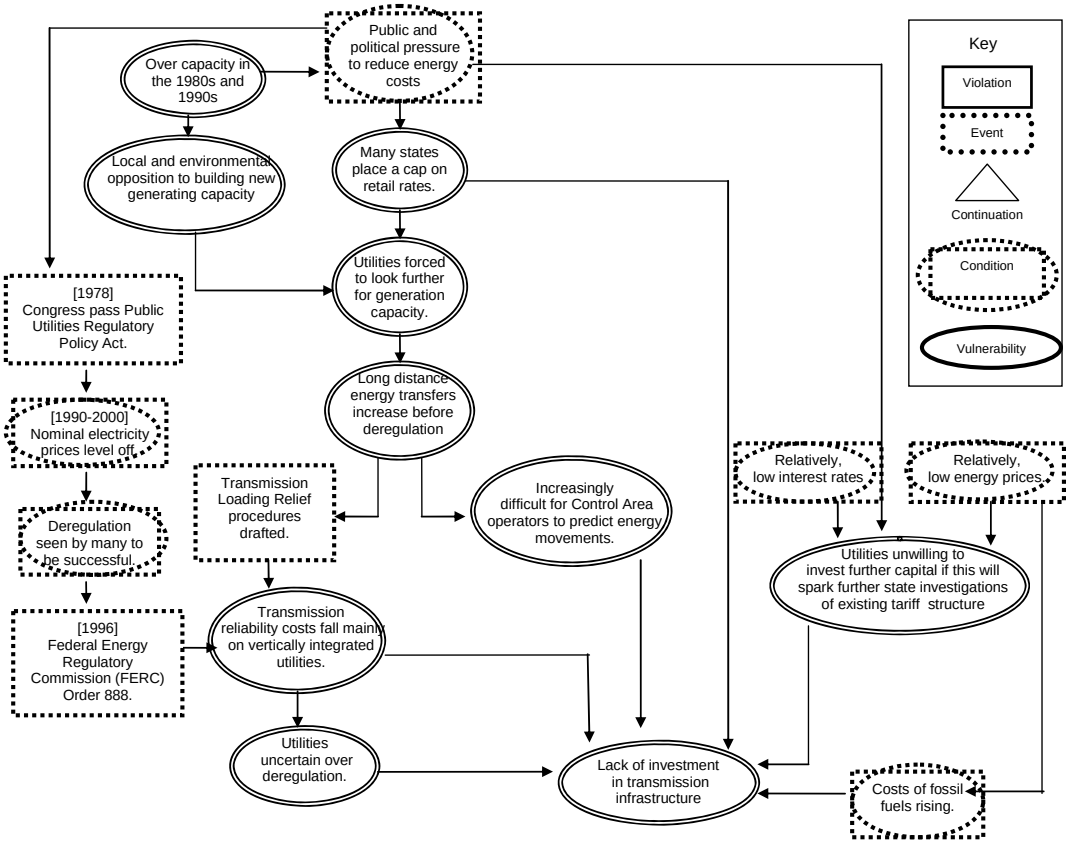

Figure 8: Counter-Arguments to Deregulation as a Causal Factor in the August Blackout

Figure 8 represents arguments in favor of market forces. As can be seen, this interpretation draws upon many of the events and conditions used in the critical analysis of deregulation. However, an additional vulnerability is introduced by the overcapacity of the 1980s and 1990s. This led to public pressure to reduce costs and is one reason for local and environmental opposition to building additional generating capacity. Public pressure to reduce costs encouraged states to intervene further in the market by introducing the price caps, mentioned above. This market intervention acted as a direct restraint on investment. It also created additional structural vulnerabilities; utilities were forced to look further for lower cost generating sources. The increased transmission of power from those sources contributed to network instability. Further barriers to investment came not from deregulation itself but from the manner in which that deregulation was implemented; utilities were uncertain about their long term viability as they bore transmission costs for new entrants.

Engineering Recommendations and Public Policy Responses

Many different lessons have been drawn from the August 2003 blackout. For example, the Federal Energy Regulatory Commission (FERC) created an energy reliability division. This helps to form policy and standards as the generation and distribution industries respond to changing market conditions. Figure 9 illustrates how the creation of the new division can be seen as a response to some of the vulnerabilities that were identified from the blackout. The

creation of new organizational structures within FERC is intended to: "Allow prompt recovery of prudent expenses to safeguard reliability, security and safety; oversee the development and enforcement of grid-reliability standards; work with other agencies to improve infrastructure security; work with the states to support robust programs for customer demand-side participation" [2]. It is important not to underestimate the value of the simple annotations illustrated in Figure 9. They denote the relationship between the causes of an adverse event and the recommendations that are intended to avoid future recurrences. These links must be drawn if we are to prevent organizations from using previous incidents to justify recommendations that have little relationship to the detailed engineering failures.

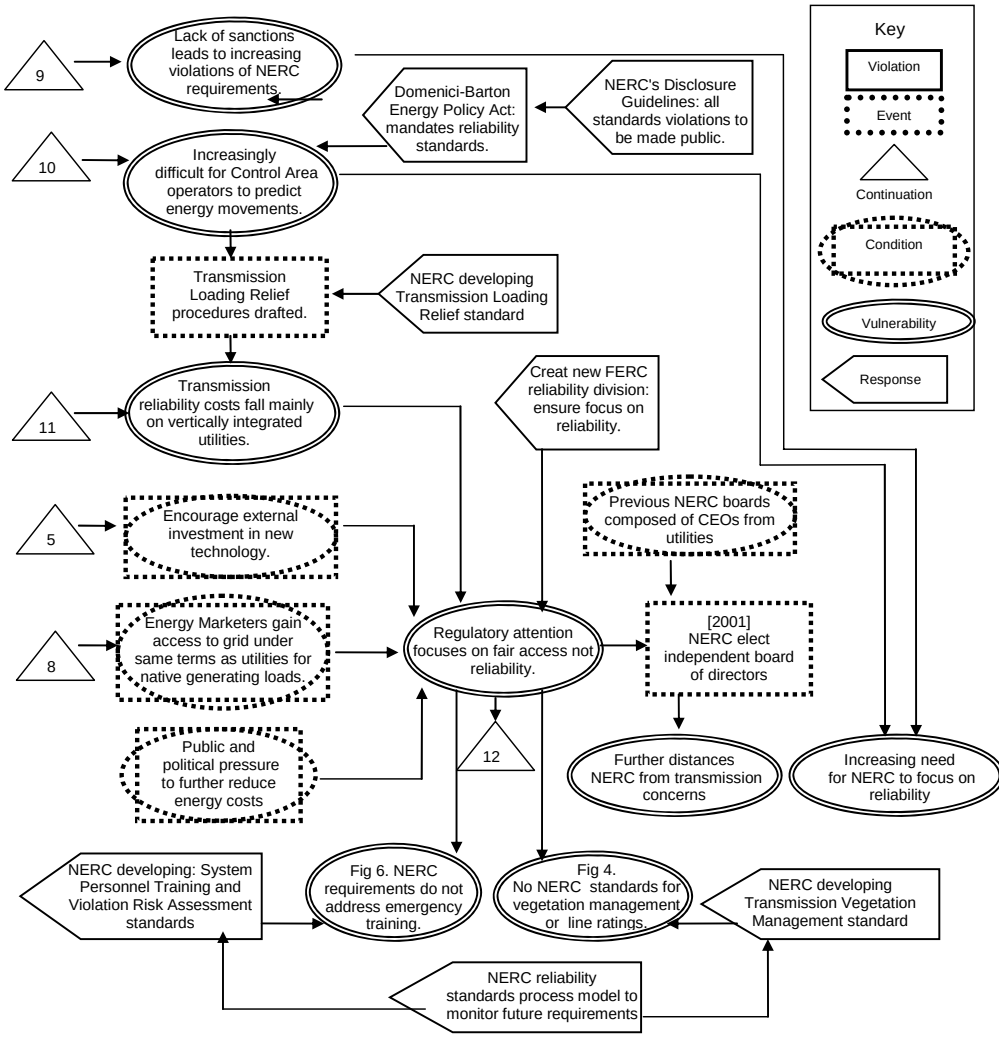

Figure 9: Responses to the August 2003 Blackout

In August 2005, President Bush approved the Domenici-Barton Energy Policy Act. This created the Electric Reliability Organization (ERO) to enforce standards throughout the United States, Canada and Mexico [5]. Figure 9 shows how this and other Federal enforcement actions address the violations of NERC reliability requirements in the months before the blackout. By encouraging compliance with NERC standards, enforcement actions help regulatory organizations to predict energy movements. The V2 diagram also helps to identify audit requirements by explicitly linking recommendations to particular vulnerabilities. In this example, it is important to identify metrics to determine whether or not the Domenici-Barton Energy Policy Act increases compliance with NERC requirements. Similarly, Figure 9 illustrates the need to determine whether these compliance actions help reliability organizations make more accurate predictions about energy transfers.

There is little to be gained from Federal initiatives to ensure compliance with inappropriate standards. The NERC is reviewing many different standards following the events of August 2003. In particular, Figure 9 illustrates the relevance of NERC drafting standards on vegetation management and emergency training by linking them to causes of the blackout. Similarly, any new standard on Transmission Loading Relief must clarify those situations in which this procedure will be used. As we have seen, PJM and AEP spent valuable time trying to negotiate a TLR that would have had a very limited impact upon the developing failure. Similarly, Figure 9 illustrates the relevance of the NERC's proposed reliability standards process model. This framework describes the validation processes for standards developed following August 14th. Specific revisions to Transmission Loading Relief procedures or to vegetation management requirements only address the symptoms of the blackout. In contrast, the new process model addresses the underlying problem of ensuring relatively complete and consistent reliability standards for a deregulated market.

The V2 diagram in Figure 9 sketches the interactions between different initiatives from commercial, regulatory and governmental organizations. This helps to ensure the 'joined-up' thinking that is often lacking with piecemeal public policy reforms to highly technical, infrastructure provision. In this instance, there is a danger that the provisions of the Domenici-Barton Energy Policy Act would be ineffective if organizations were reluctant to disclose NERC violations. Figure 9, therefore, also illustrates the importance of the NERC's new Guidelines for Reporting and Disclosure. This is intended to ensure that all confirmed violations of NERC standards are made public.

Conclusions and Further Work

There are continuing interactions between public policy and infrastructure engineering in North America. There has been considerable pressure to reinforce the self-regulatory framework that is intended to support US infrastructure reliability. Greater attention is being paid to the FERC's role within a deregulated market. In particular, there seems to be growing public and political interest in ensuring the effective policing of NERC standards. It seems likely that any further reliability problems will trigger greater market intervention and regulation.

The relevance of this work extends beyond North America. The liberalization of European energy markets has created conditions that are similar to those in the United States before 2003. Recent fluctuations in gas prices have made some countries reluctant to pass supplies across national borders without first ensuring the security of their own provision. This prevents transmission companies, utilities and regulators from making accurate predictions about future supplies. Similarly, plans to allow for the symmetric distribution of electricity by plants that consume power at some times but then generate electricity at others using renewable sources, will only work if we have a reliable and stable information technology infrastructure. This IT infrastructure must balance the supply and demand of base and reactive power. It must also provide for transparent and equitable systems of payment for both generators and infrastructure providers.

The August 14th blackout continues to inform and motivate Federal intervention, including FERC reliability requirements for network analysis, transactions scheduling, grid forecasting etc. These regulations are forcing utilities and reliability organizations to develop more complex information technology infrastructures to support their existing transmission networks. However, initial studies have revealed important differences across the energy market; "a few very large utilities have invested in development and installation of the sophisticated, complex software tools identified as best practices needed for reliable grid operations" [3]. In contrast, many smaller utilities retain "old, patched EMS, state estimator and contingency analysis software that does not allow precise, near-real-time evaluation of grid conditions and threats". Such technological disparities create the preconditions for future

failures. You do not need to look far within the current market structure to realize that it contains the seeds of tomorrow's failures.

References

[1] Delgado, J., The Blackout of 2003 and its Connection to Open Access, *Issue Papers on Reliability and Competition*, Technical Workshop on Competition and Reliability in North American Energy Markets, US Department of Energy and Natural Resources Canada, Washington DC, August 2005.

[2] FERC, Division of Reliability, Presentation at Federal Energy Regulatory Commission Open Meeting, Washington, DC, October 6, 2004 by Joseph H. McClelland, Director, Division of Reliability, Office of Markets, Tariffs, and Rates. Available on http://www.ferc.gov, FERC's Strategic Plan, last accessed 21st January 2006.

[3] Harris, P.G., Relationship between Competitive Power Markets and Grid Reliability: The PJM RTO Experience, *Issue Papers on Reliability and Competition*, Technical Workshop on Competition and Reliability in North American Energy Markets, US Department of Energy and Natural Resources Canada, Washington DC, August 2005.

[4] Hogan, W.W., Shedding Light, Wall Street Journal, Commentary, Page A20, 19th April 2004.

[5] Hughes, J.P., Reliability Risks during the Transition to Competitive Electricity Markets, *Issue Papers on Reliability and Competition*, Technical Workshop on Competition and Reliability in North American Energy Markets, US Department of Energy and Natural Resources Canada, Washington DC, August 2005.

[6] Johnson, C.W., A Handbook of Incident and Accident Reporting, Glasgow University Press, Glasgow, UK, 2003.

[7] Massachusetts, Commonwealth of, Report of the Governor's Task Force on Electric Reliability and Outage Preparedness, March 2004, Available on http://www.mass.gov/dte/225repgtf.htm, last accessed 21st January 2006.

[8] United States-Canada Power System Outage Task Force, Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations, April 2004.

[9] United States Government Accountability Office, Electricity Restructuring: Key Challenges Remain, Report to the Chairman, Subcommittee on Energy and Resources, Committee On Government Reform, House Of Representatives, GAO-06-237, November 2005.

Biography:

Chris Johnson is Professor of Computing Science at the University of Glasgow in Scotland. He heads the Glasgow Accident Analysis Group, this small team of multi-disciplinary researchers is interested in understanding the role of computer applications in the failure of complex systems. He has held a NASA fellowship for his work on incident investigation techniques and helped to author incident reporting guidelines for European Air Traffic Management. He has published over 100 peer reviewed papers, including a Handbook of Accident and Incident Reporting that can be downloaded from his web site. He coordinated the EC ADVISES Research Training Network supporting human factors approaches to the design of safety-critical systems.