Understanding Failures in International Safety-Critical Infrastructures:
A Comparison of European and North American Power Failures

Chris. W. Johnson, DPhil;
Department of Computing Science, University of Glasgow, Scotland, UK.

Keywords: Critical Infrastructures, Blackouts, Power Distribution, V2 Analysis.

Abstract

The increasing integration of safety-critical infrastructures introduces vulnerabilities that extend across international borders. On the 14th August 2003, a domino-effect disrupted the power supply to more than 50 million people across the North-Eastern United States and Canada. Consequent losses were between (US) $5-10 billion and the failure was implicated in numerous accidents. Meanwhile on the 28th September 2003, a similar blackout affected more than 56 million people across Italy and areas of Switzerland. Knock-on effects propagated across France, Slovenia and Austria. Both incidents had similar technical causes triggered by large-scale transfers of electricity across aging distribution networks. Increased loads caused power lines to heat and sag until they hit trees. Both blackouts also stemmed from longer term vulnerabilities to do with the regulation and monitoring of energy transfers and the algorithms used to predict potential distribution problems. The European and North American failures had managerial and human factors causes; these arguably included an over-reliance on computer-based decision support systems. 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 the causal factor behind two of the most serious failures across international, safety-critical infrastructures.

Introduction

The increasing integration of complex safety-critical systems creates vulnerabilities across the power distribution, water supply and transportation industries. Failures quickly propagate across national borders. Further vulnerabilities arise because the exchange of monitoring information between countries has not kept pace with the physical transfers between national infrastructures. In consequence, individual states are often poorly equipped to deal with knock-on failures that stem from neighboring areas of a network. Problems also arise because previous research often focuses on the impact of failures within a particular state or region. The following pages, therefore, compare and contrast key insights from two recent incidents in which initial failures affected large areas of Europe and North America.

Summary of the Case Studies

The Italian Blackout: During the early morning of the 28th September 2003, a cascading series of line trips led to the isolation and eventual blackout of the Italian electricity distribution network. Although the most serious consequences were experienced South of the Alps, the immediate causes originated in the Swiss transmission system. A 380kV line between Mettlen and Lavorgo was loaded at 86% of its maximum capacity. The core temperature of the cable rose to a point where it began 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. Subsequent attempts to close the line were unsuccessful. This increased the loading on other areas of the network that were used to compensate for the initial failure. As might be expected, the increased demand on the remaining lines in the region led to an increase in core temperatures that eventually caused these cables to sag close to nearby vegetation. Attempts by the Swiss operators to reduce the loading on the 380kV Sils-Sosa line were insufficient to prevent another flashover.

These initial failures had a strong effect on the Italian power system, according to some estimates the national generation capacity was only able to support around 87% of its annual demand (SFOE, 2003). High domestic operating costs encouraged Italian suppliers to import electricity from other states. In consequence, the domino-effect created by the Swiss line failures led to a sudden loss of voltage. Automatic protection devices intervened to separate all remaining lines between the Italian grid and neighboring states. 56 million people lost power across Italy and areas of Switzerland. The disruption lasted for more than 48 hours as crews struggled to reconnect the networks. Although hospitals and other emergency centers were able to call upon reserve generators, there were significant knock-on effects across other critical infrastructures. The mobile phone system began to fail as transceivers lost power. Other areas of the networks became overloaded as customers tried to contact friends and family. The blackout also affected large areas of the Internet as UPS sources either failed or ran out of battery power (Cowie et al, 2004).

In order to understand the longer term causes of this failure, it is important to briefly explain recent changes in the structure of energy markets across Europe. Traditionally, many states relied upon a small number of vertically integrated utilities to generate and transmit electricity. The European Union (EU) argued that this created local monopolies; other companies could not access the distribution networks. This, in turn, prevented companies from supplying power to consumers in other member states. The EU, therefore, issued directives to open internal energy markets in 1996 and 2003. France and Italy developed national legislation to unbundle the transmission networks from the generating companies. They also set up regulatory organizations, the Italian Autorità per l'energia elettrica e il gas, (AEEG) and the French Commission de régulation de l'énergie (CRE), to govern the internal operation of their energy markets. Although the Swiss Federation remains outside the EU, their physical infrastructure and generating capacity continue to meet power needs across member states. They, therefore, participated in the European Union for the Co-ordination of Transmission of Electricity (UCTE). The UCTE is an association of transmission system operators across continental Europe. However, there is no widespread, independent means of verifying whether or not a state complies with UCTE requirements.

Italian, French and Swiss regulators developed a joint questionnaire that was sent to transmission companies to gather evidence. Technical, commercial and political differences emerged over the longer term causes. In particular, there were disagreements over the role of the UCTE. The Swiss urged the French and Italian regulators to accept the findings presented in the UCTE interim report. The Italian and the French regulators were concerned that the UCTE were both investigating the failure and were also responsible for setting standards for power transmission (page 5, AEEG, 2004). Relations between national regulators were further strained when the Swiss SFOE issued an independent report on the blackout. The integrated Swiss electricity companies then argued that all necessary information had been provided to the UCTE and SFOE. This deprived the Italian and French regulators of direct access to some evidence about the course of the blackout.

The North American Blackout: Large portions of Ohio, Michigan, Pennsylvania, New York, Vermont, Massachusetts, Connecticut, New Jersey and the Canadian province of Ontario, experienced an electric power blackout on 14th August 2003. The outage affected approximately 50 million people and 61,800MW of electric load. Power was lost for 4 days with rolling blackouts continuing for more than a week (US-Canada Power System Outage Task Force, 2004). The causes of this incident were remarkably similar to those that triggered the European blackout. A number of failures affected lines feeding power into northern Ohio from eastern Ohio. These led to the loss of the Harding-Chamberlain 345-kV line, which in turn increased loading on the Hanna-Juniper 345-kV line. The rise in power loading caused increasing core cable temperatures that led the cables to sag and created the conditions for flashovers to occur. A chain reaction was established in which further flows were created by the loss of initial lines, these flows increased loading on the remaining network topology and led to further short circuits. In other areas of the network, automated protection devices cut-in. This did more to exacerbate rather than reduce the problems faced by transmission companies.

As with the Italian blackout, this incident has been the subject of considerable controversy. A joint US and Canadian commission was established to identify the causes of the power failure (US-Canada Task Force, 2004). Federal (US Government Accountability Office, 2005) and State investigations (Commonwealth of Massachusetts, 2004), commercial organizations (Delgado, 2005), pressure groups (Hughes, 2005) and media organizations (Hogan, 2004) all published alternate accounts. These reports reflect different attitudes towards the impact that market deregulation had upon the reliability of complex, safety-critical systems. There are striking similarities with the longer term causes of the European failure. In 1978, the U.S. Congress passed the Public Utility Regulatory Policy Act (PURPA). The aim was to encourage investment in newer, more efficient technologies and, in consequence, to lower costs. These regulations enabled new entrants into the market to sell energy to utilities without many of the reliability obligations that governed established companies. Traditionally, companies had been vertically integrated within particular regions where they owned and operated generation, transmission and distribution. PURPA companies could sell power without necessarily providing guarantees about continued service provision. There was no assumption that they would invest in, for instance, the transmission infrastructure. These moves to open access to the energy markets 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 that directly generated the supply. The creation of ‘open access’ tariffs for the distribution network had a profound impact on the North American wholesale energy market. Energy marketers were able to trade power over increasing distances in response to pricing changes. Similarly, the utilities themselves began to trade power regionally both to gain revenue from their generation capacity and also to obtain additional power at lower costs. These trades created some of the preconditions for the August 2003 blackout as it became increasingly difficult for network operators to predict and resolve congestion problems.

Analysis of the Italian Blackout

The previous summary has identified initial similarities between both the North American and European blackouts. The following pages extend this analysis using techniques derived from accident investigation to represent and reason about the causes of these failures in international infrastructures. Figure 1 presents a V2 (violation and vulnerability) analysis of the initial events leading to the failure in the Italian distribution system. Dotted boxes represent events that lead towards a failure. For example, an event is used to denote that the Transmission System Operators (TSOs) exchanged their schedules for energy transfers for the following day at 18:30 on the 27th of September. TSOs can be thought of as the organisations that transmit electrical power from generation plants to the regional or local electricity distribution operators. Colour and shading are used to distinguish events that involve different countries. The first parentheses of each event provide timing information and, where appropriate, the second parentheses denote country information. Hence an event that begins with the label (03:01:21)(Ch) refers to something that took place at one minute after 3am and principally affected the Swiss networks.

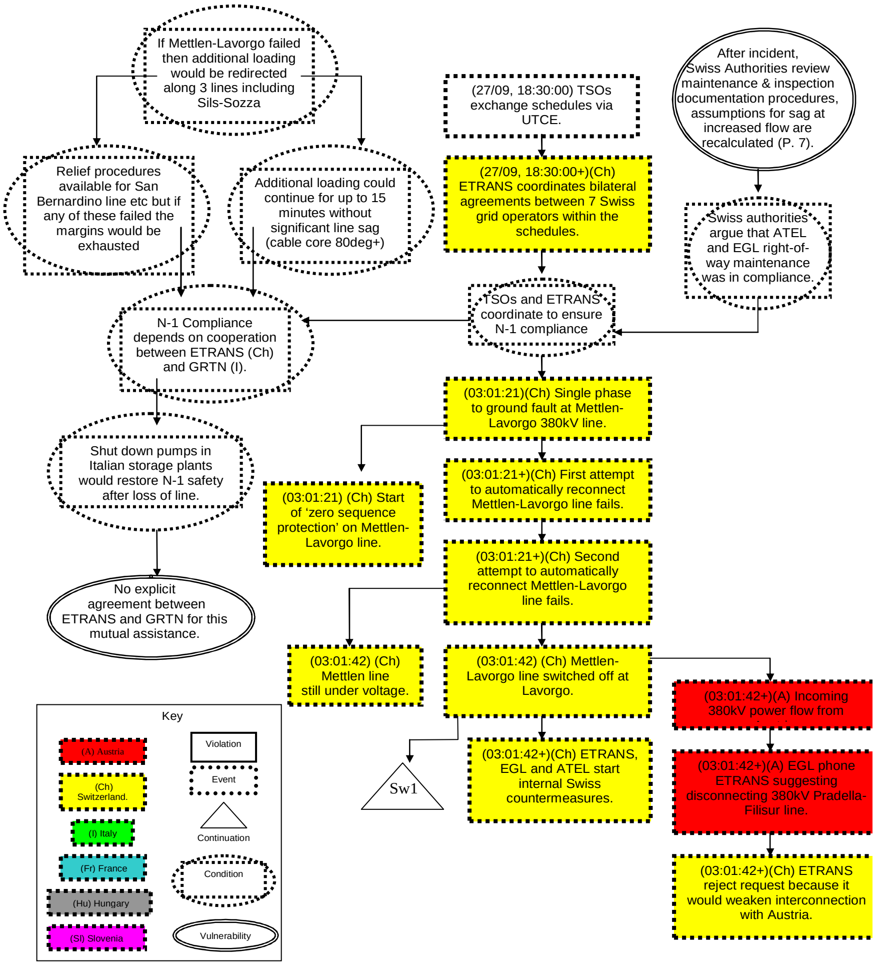

Figure 1: Initial Events Leading to the Italian and Swiss Blackout

Dotted ellipses represent conditions. For example, Figure 1 records the observation that the TSOs had to cooperate with the Swiss network operator (ETRANS) to ensure N-1 compliance. Under UCTE requirements, transmission systems must be operated so that the loss of any 1 node from the N that are currently available will not interrupt supply. Solid ellipses represent vulnerabilities that threaten complex systems. Figure 1 shows that the Swiss authorities took steps to revise their maintenance and inspection procedures in the aftermath of the blackout. Figure 1 also uses a vulnerability node to show that there was no explicit agreement between the Swiss company ETRANS and the Italian network operators GRTN to shut down Italian storage pumps during any line overloading. These pumps helped store power by transferring water to high reservoirs when overnight electricity prices were low. The water could then be released using gravity to generate electricity as demand rose during the day. These pumps were close to the Swiss-Italian exchange points and hence had an important impact on loading.

The right hand sequence of events in Figure 1 illustrates attempts by the Swiss ETRANS operators to coordinate load-shedding through their Austrian colleagues. However, the lack of any explicit agreement to coordinate the shut-down of the Italian pumping stations created further vulnerabilities. Attempts were also made by ETRANS and the two immediate line operating companies EGL and ATEL Netz AG to reduce the load on the Sils-Soazza 380kV line. ATEL altered the transformer tap at Lavorgo and EGL switched off another 380/220 transformer. However, this did little to reduce the overload and ate into the 15 minute 'safety margin' for increased loading on this area of the network. Many of these problems arose from a lack of situation awareness. There was only one ETRANS operator monitoring the network and they failed to appreciate the urgency of reducing the loading on Sils-Soazza. Eventually at 03:10:45, they asked the Italian operator GRTN to reduce imports by 300MW. This request was made informally over the telephone. Standard Operating Procedures stated that this request should be made by fax after a previous failure in September 2000. Operators failed to realise that this 300MW reduction could only provide temporary relief. Staff in the Italian operator, GRTN, did not have access to the same real-time data flows that were available to the Swiss ETRANS operators. Poor situation awareness was exacerbated by the lack of joint training between Swiss and Italian dispatchers.

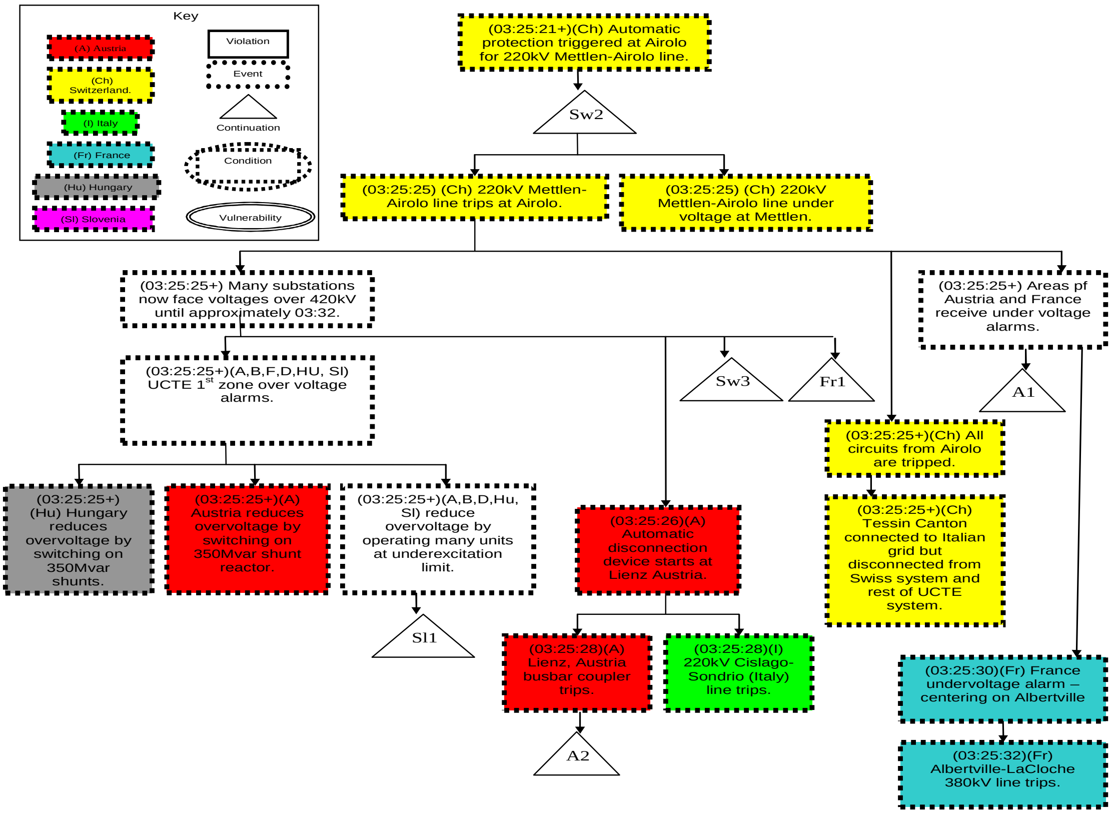

Figure 2: The Failure of Sils-Soazza Propagates Trips in Austria, Switzerland, France and Italy

Figure 2 presents the immediate consequences of the Sils-Soazza failure. Automatic protection device on the 220kV Mettlen-Airolo line functioned as intended. However, it left many substations under increasingly heavy voltage as the available power found the route of least resistance across the remaining network. 'Over voltage' alarms began to propagate across Austria, Belgium, France, Germany, Hungary and Slovenia. The Austrian network incorporated a range of protection devices that were intended to safeguard their infrastructure during overload conditions. These devices began to separate the Austrian network from its Italian interconnections. In contrast to these areas of high voltage, Figure 2 also shows that some areas of France and Austria suffered from 'under voltage' alarms.

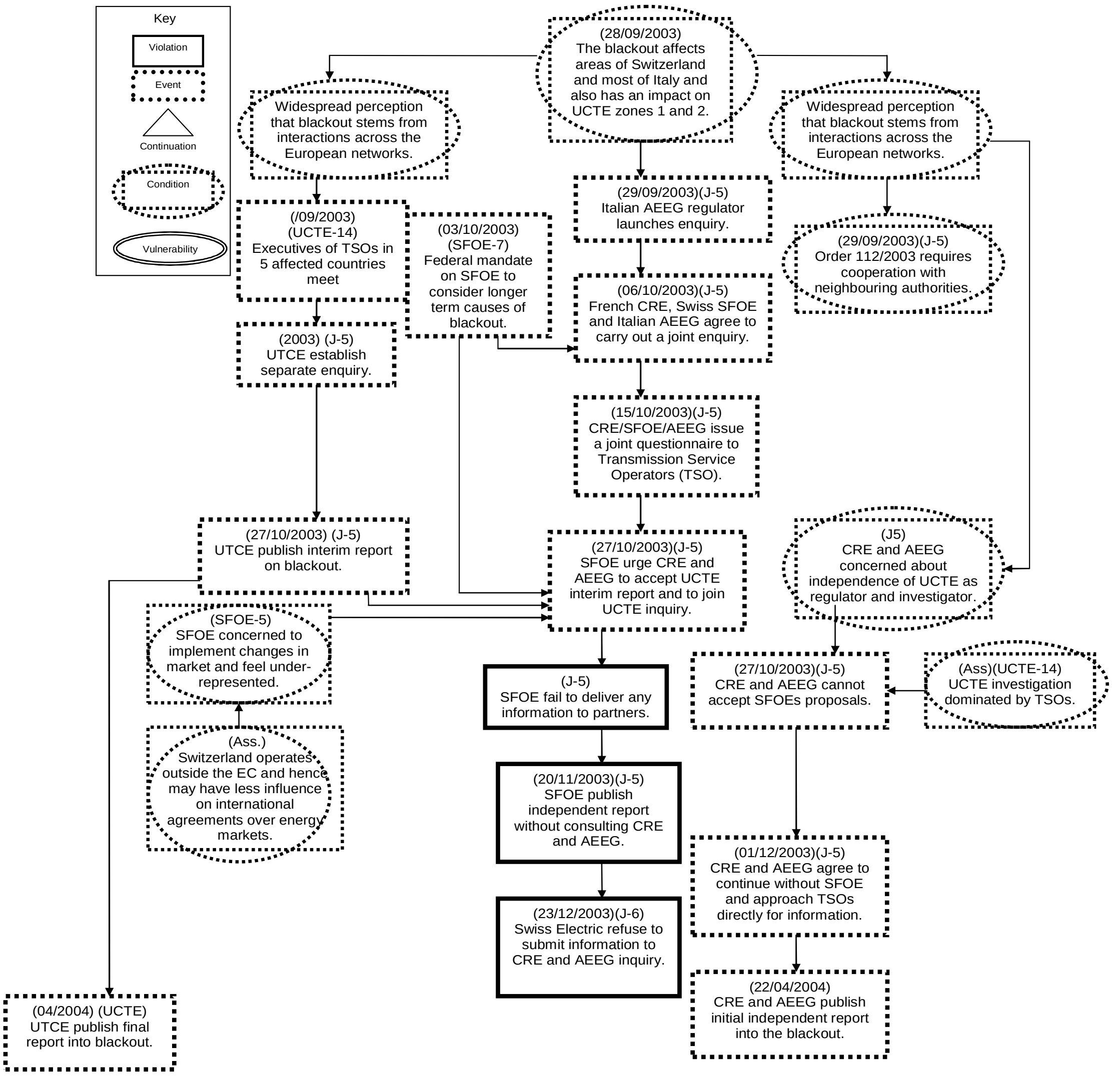

Figure 3: Tensions Leading to Schisms over the Investigation of the Blackout

Figure 3 represents different phases in the investigation of the Italian blackout. (SFOE-5) refers to information that was presented on page 5 of the SFOE report (2003). Similarly, (J-6) refers to evidence presented on page 6 of the joint report published by the French, CRE, and Italian, AEEG (2004), regulators. (UTCE-14) cites information from page 14 of the UTCE (2004) report. These references are important when there are significant differences over the causes of the blackout. As mentioned, the Italian AEEG and the French CRE were concerned that the UCTE were investigating the failure and were also responsible for setting standards for power transmission (page 5, AEEG, 2004). Relations were further strained when the Swiss regulator, SFOE, issued an independent report on the blackout without consulting their Italian or French counterparts. Figure 3 denotes this as a violation of the previous joint agreement. The Swiss utility companies then argued that all necessary information had been provided to the UCTE and SFOE. This deprived the Italian and French regulators of evidence about the course of the blackout.

The Swiss regulators, SFOE, argued that the blackout stemmed from the ground fault caused by vegetation encroaching on the Mettlen-Lavorgo line. They also criticised inadequate communication between the Swiss transmission company, ETRANS, and the Italian network operator GRTN. Finally, they pointed to inherent instabilities in the Italian network. They were, however, careful to stress that these were not the underlying causes. SFOE argued the main problems stemmed from "unresolved conflicts" between the trading interests of particular countries and the physical capacity of the networks through which those trades might be realized. Elements of the Italian generating infrastructure were relatively old. The Italian industry also suffered from relatively high costs. In contrast, the deregulation of supply and the promotion of EC energy markets together with the relatively low costs of generation in other European countries provided disincentives for future investment in Italian domestic generation. These various factors combined to fuel a steady growth in energy imports. The rising demand necessarily had an impact on the Swiss networks, either directly through exports from Swiss generating companies or indirectly as a transmission route for other generators. However, the SFOE argued that Switzerland had little influence on the regulatory and political decisions that created this situation because they were not an EC member state. The SFOE also argued that French electricity traders had been allocated export volumes that exceeded the physical transmission capacity between France and Italy. This situation was contrasted with the position of Swiss electricity traders who operated within the limits imposed by the physical transmission capacity between Italy and Switzerland.

In contrast, the French, CRE, and Italian, AEEG, argued that Swiss operators took 'inappropriate measures' and made 'operational mistakes' after the initial fault on the Mettlen-Lavorgo line. They also argued that the events of the 28th September revealed a need for greater coordination between transmission companies in planning for the real-time control of interconnected distribution networks. There were further differences between the SFOE and the joint AEEG/CRE reports. The French and Italian account looked less at the relationship between market movements and physical transmission capacity. Instead, they focused on the actions of the Swiss operators to anticipate and then respond to potential problems. They argued that the Swiss companies did not comply with UCTE operating rules on the night of the blackout. They concluded that compliance should be legally binding and subject to independent verification. They went on to argue that the Swiss government should construct a legal and regulatory framework that is consistent with EU legislation in order to ensure the safety and security of the European grid.

Analysis of the North American Blackout

The North American distribution network was protected by procedures and practices that were very similar to those in Europe. For example, North American Electric Reliability Council (NERC) Policy 2.A on Transmission Operations states that "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" (US-Canada Power System Outage Task Force, 2004). This embodies the N-1 criteria described in previous sections as a corner stone of European policy. Individual operators deployed monitoring systems to ensure compliance with these requirements. For example, the Midwest Independent System Operator (MISO) had developed State Estimation (SE) and Real Time Contingency Analysis (RTCA) software. MISO was set up by a group of utility companies to help monitor and improve the reliability of their operations. The SE and RTCA systems used information about the current state of N network components to predict the consequences if the network were reduced to N-1 components using Monte Carlo simulations. RTCA software was intended to run automatically, checking the state of the system every five minutes.

Figure 4 denotes that MISO's SE and RTCA systems could only access data about part of the distribution network. This vulnerability was exposed when there was an outage on Cinenergy's Bloomington-Dennis (B-D) Creek 230-kV line. MISO's State Estimator did not have the information necessary to accurately model the state of this network component. 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 remaining sensor values. This led to a violation of standard operating procedures when the operator neglected to restart the SE and RTCA software. It is important to note that violations can be inadvertent. For instance, operators may not know about applicable rules and regulations or, as in this case, they may stem from inattention and fatigue. Violations can also be deliberate and may, in some cases, be justified.

This happens when, for instance, rules and procedures fail to take into account particular environmental conditions that would further jeopardize safety if operators were to follow them.

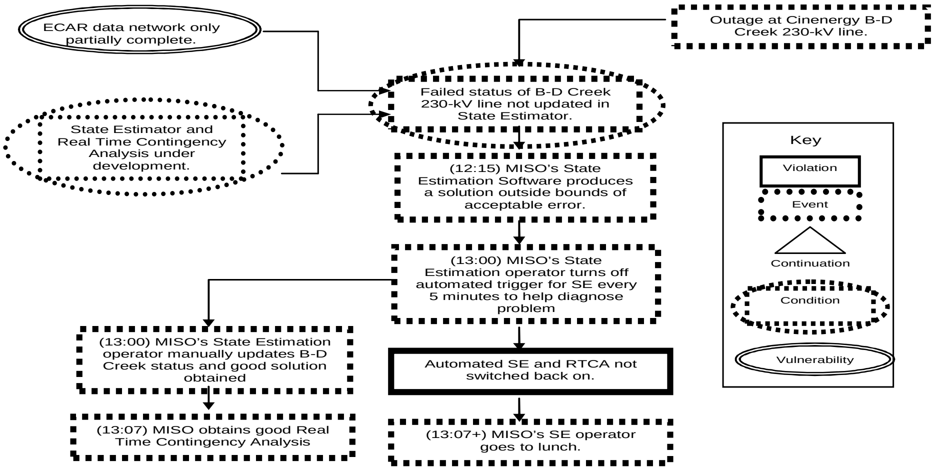

Figure 4: The Failure of MISO's State Estimator and Real-Time Contingency Analysis

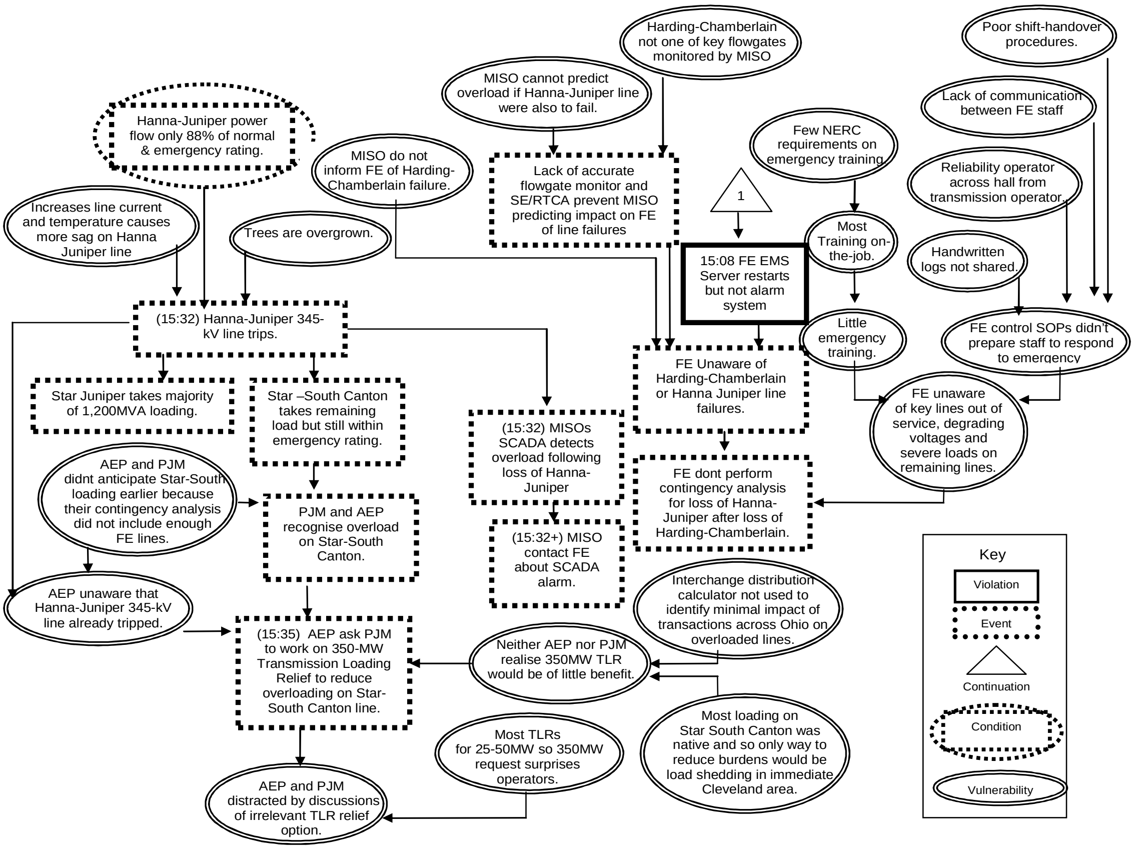

Figure 5: Consequent Network Failures and Attempts to Relieve Transmission Loading

Further problems undermined the situation awareness of key staff following the loss of the State Estimator and Real Time Contingency Analysis software. Figure 5 shows how the MISO reliability organisation's Supervisory Control and Data Acquisition (SCADA) system detected the initial overload. Their staff began to warn colleagues in the

First Electric (FE) generating company. However, critical information was not passed between different shifts within FE. The North American Electric Reliability Council (NERC) provided limited guidance on training to coordinate the response to major failures. The operators in another utility company, AEP, and their associated reliability organization, PJM, also recognized that the initial failures had increased the loading on the Star-South Canton line. However, their N-1 contingency software did not have access to accurate real-time data about the state of FE's lines. They could not, therefore, predict the knock-on effects for their own 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. The TLR was, therefore, delayed by repeated requests to confirm that AEP really did want 350MW.

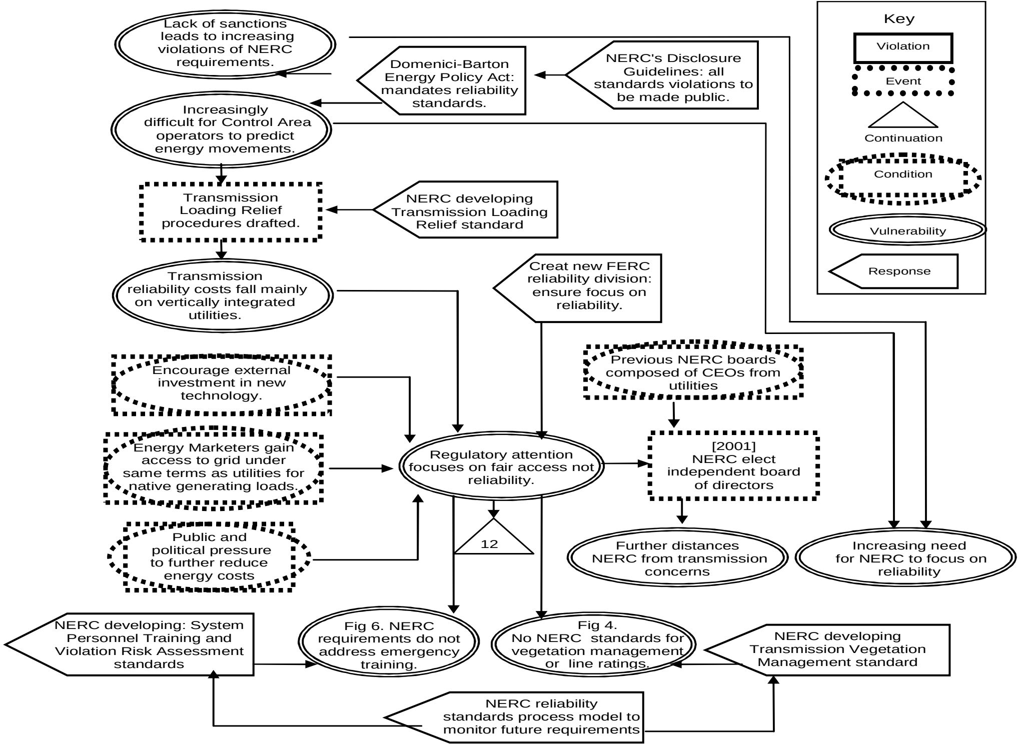

Figure 6: Responses to the August 2003 Blackout

In August 2005, the Electric Reliability Organization (ERO) was created to enforce standards throughout the United States, Canada and Mexico. Figure 6 shows how this and other Federal enforcement actions address the violations of NERC reliability requirements in the months before the blackout. The intention is that by encouraging compliance with NERC standards, regulatory organizations can make more accurate predictions about 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 these initiatives increase compliance with NERC requirements and whether, in turn, this will help reliability organizations to anticipate energy transfers across national and international infrastructures.

Conclusions and Further Work

On the 14th August 2003, a domino-effect resulted in an interruption to the power supplies for more than 50 million people across the North-Eastern United States and Canada. Meanwhile on the 28th September 2003, a similar blackout affected more than 56 million people across Italy, Switzerland, France, Slovenia, and Austria. There were significant knock-on effects across other critical infrastructures, for example, 30,000 people were trapped on trains. Both blackouts had similar causes as distribution networks struggled to meet increasing energy transfers within and between national infrastructures. This paper has applied accident analysis techniques in order to identify further similarities between the detailed causes of these infrastructure failures Further analysis is urgently required to identify further lessons from the comparison of these two major international failures in critical infrastructure:

1. *Deregulation of Energy Generation and Transmission.* It can be argued that both failures arose from 'systemic failures' in public policy as governments struggled to introduce market reforms through deregulation. By providing market access, the European Commission and the Federal Energy Regulatory Commission encouraged bulk energy transfers from low cost generators that were some distance away from the point of use. The terms governing these transfers arguably did not adequately consider the costs associated with infrastructure reliability. Equally it can be argued that the development of regulatory agencies distorted the operation of the free market and the blackouts were the result of government intervention so that companies were unsure of their responsibilities.
2. *Physical Infrastructure Maintenance.* Both blackouts were either triggered or exacerbated by aspects of infrastructure maintenance. This not only refers to a need for sustained investment in network technologies to keep pace with increased demand for access to distribution networks. It also refers 'rights of way' maintenance; vegetation was allowed to grow close to the transmission lines creating the potential for arcing to occur when loadings and core temperatures began to rise.
3. *Intervention of Automated Protection Devices and Increasing Systems Integration.* The initial fault on the Swiss Mettlen-Lavorgo line triggered the intervention of automated systems that failed to reconnect the service. Conversely, several of the Austrian networks and generating nodes were protected by automated devices that acted promptly to isolate their systems, exacerbating the problems for the Italian operators. In the North American case study, automated devices also acted to cut off subnetworks and generators, thereby, also increasing the load on the remaining network topology. These automated protection devices act on purely local information. An important insight from our analysis is that such local actions often increase global instability.
4. *Human Factors Issues and Decision Support Tools.* The State Estimator and Real Time Contingency Analysis software failed because the ECAR data network did not provide sufficient coverage for operators to monitor contingencies across their distribution network. Similarly, there were extremely limited data flows between the Swiss ETRANS company and the Italian GRTN. In consequence, it was difficult for operators to derive an accurate overview of the state of the networks.
5. *Lack of Situation Awareness.* There were several opportunities for staff in generating and distribution companies to mitigate the consequences of the failures in Europe and North America. However, it took some time before the Swiss ETRANS operator asked the Italian GRTN operator to reduce load after the Sils-Soazza line became overloaded. Similarly, there were considerable delays before First Electric staff appreciated the significance of the problems affecting the Hanna-Juniper line. In both cases, it seems as though inadequate situation awareness undermined the effectiveness and timeliness of their response. There was very little joint training between different North American companies, such as AEP, FE and PJM. Similarly, there were few attempts to conduct joint exercises between Swiss and Italian dispatchers even though they operated integrated systems across national borders.
6. *Lack of Coordination.* Previous sections have mentioned some of the problems in establishing agreement for regulatory provisions across North America and between member states in Europe. This lack of coordination at a political level is mirrored by operational problems during the blackout. The delays in reducing Italian imports and the confusion over the use of faxes between companies in Italy (GRTN), France (RTE) and Switzerland (ETRANS) illustrate these issues. Similarly, problems in communication between North American reliability organisations (MISO and PJM) were mirrored by delays in implementing loading relief between operations teams in the companies (AEP and FE). In both incidents, loading relief was 'too little and too late'.

Many of the reports that were published after the European and North American blackouts of 2003 refer to a 'failure of imagination'. We were unprepared for the infrastructure vulnerabilities that have been created through the development of national and international energy markets. Almost five years have passed since these two incidents. In that time, similar failures have occurred in both Europe and North America. On the 4th November 2007 an initial failure in Cologne, Germany propagated across parts of France, Italy, Spain and Austria. Belgium, the Netherlands and Croatia were also affected. Three million US homes were without power between 16th and 29th July 2006. Severe heat and storms affected distribution networks from New York to Pennsylvania, St. Louis, Missouri and California. In spite of these reminders, there is a danger that we will forget the lessons of 2003 while the infrastructures that we depend upon become more and more integrated across national boundaries.

References

Autorità Per L'energia Elettrica E Il Gas (AEEG), Report On The Events Of September 28th, 2003 Culminating In The Separation Of The Italian Power System From The Other UCTE Networks, April 22nd, 2004

Cowie, J.H., Ogielski A.T., Premore B.J., Smith, E.A. and Underwood T., Impact of the 2003 Blackouts on Internet Communications, Renesys Corporation. March 1, 2004.

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

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.

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

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.

Swiss Federal Office of Energy (SFOE), Report on the blackout in Italy on 28 September 2003, Berne Switzerland, November 2003.

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.

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.

UCTE, Final Report of the Investigation Committee on the 28 September 2003 Blackout in Italy, 2004.

Biography

Chris.W. Johnson, DPhil, MA, MSc, FBCS, CEng, CITP, Department of Computing Science, University of Glasgow, Glasgow, G12 8RZ, Scotland, UK, telephone +44 (141) 330 6053, facsimile +44 (141) 330 4913, e-mail – Johnson@dcs.gla.ac.uk, web page http://www.dcs.gla.ac.uk/~johnson

Chris Johnson is Professor of Computing Science at the University of Glasgow in Scotland. He heads a small research group devoted to improving the reporting and analysis of incidents and accidents across safety-critical domains ranging from healthcare, to the military to aviation and rail.