Volume 8 – Spring 2012
djim.management.dal.ca

Managing Current Complexity: Critical Energy Infrastructure Failures in North America

Abstract: This paper applies the theories of High Reliability Organization (HRO) and Normal Accidents Theory (NAT)—two competing views of risk management in highly-complex and tightly-coupled systems—to analyze the 1998 Ice Storm in order to identify the vulnerabilities in North America's critical energy infrastructure (CEI). Inferences are then made and used to draw lessons for public managers regarding the protection of CEIs. As CEIs are highly-complex and tightly-coupled systems, failures stemming from complex and uncertain risks are inevitable. In addition, there is an increasingly low tolerance for failure in energy infrastructure because society's critical infrastructures have become increasingly interdependent. Public managers must regulate CEIs in order to ensure an emphasis is placed on safety and security while also finding ways to reduce unnecessary complexities. It is through the adoption of such measures that public managers can minimize the cascading effects of inevitable failures.

About the Author(s): Colin Macdonald, Melissa Oldreive, and Eric Pegolo are Master of Public Administration students at Dalhousie University's School of Public Administration. An elongated form of this paper, prepared for a course on public sector strategic management, was awarded first runner-up at the 2012 Atlantic Conference on Public Administration.

Colin Macdonald holds a Bachelor of Arts degree in English from Dalhousie University. Colin has worked in the Nova Scotia provincial public service and also in a variety of positions at commercial banking institutions.

Melissa Oldreive holds a Bachelor of Arts degree in English and Canadian Studies from Dalhousie University. Melissa currently works in the Nova Scotia provincial government focusing on renewable electricity initiatives.

Eric Pegolo holds Bachelor of Arts degree at the University of Guelph, where he completed his honours thesis, "Public Sector-Private Sector Partnerships during the Common Sense Revolution: The Business Transformation Project and the 407." He has worked in Ottawa for the federal public service and two cabinet ministers in the Government of Ontario.

Introduction

Providing reliable electricity can be an immensely complex and technical challenge. It requires the effective control and coordination of thousands of generators, transformers, and distribution networks that move electricity through an interconnected network of transmission lines.[1] This paper examines a particular subsection of the North American power grid, known as the Eastern Interconnect, an area covering much of the northeastern United States, Ontario, and Québec, in order to highlight the inherent risks that critical energy infrastructure (CEI) is exposed to in North America. Specifically, this paper focuses on a notable failure within this electrical grid, the 1998 Ice Storm, through the lens of two notable theories of organizational control and risk management—High Reliability Organization theory and Normal Accidents Theory. Highlighting the central tenants of these theories, this paper will demonstrate the importance of establishing a reliable environment where risks are omnipresent and as such, failures are inevitable. Furthermore, this paper will argue that because of the low tolerance for failure within the energy industry, strict regulations are required to prevent unnecessary system interdependencies and complexities. This analysis will conclude with lessons for public managers and, more generally, the energy industry. It will provide recommendations for future energy infrastructure management in the Canadian context in light of the explored theoretical approaches to system management.

Theoretical Approaches

The seemingly opposing theories of High Reliability Organizational theory (HRO) and Normal Accidents Theory (NAT) represent two approaches to understanding vulnerabilities and controlling potential hazards in today's "tightly-coupled" and complex organizations. Tightly-coupled systems are those in which a failure in one area or "component" leads almost immediately to a failure in another. "Complex systems" identify a connection between components that is far more intricate and complicated than a linear or causal process (Perrow, 1999). Such systems are prevalent in today's society, leaving both those directly and indirectly impacted vulnerable to the ramifications of many possible failures. The debate between these theories centers on system accidents: those accidents involving "the unanticipated interaction of multiple failures" and "damage to subsystems or systems as a whole, stopping the intended output or affecting it to the extent that it must be halted promptly" (Perrow, 1999, p. 70). Both HRO and NAT recognize the inevitability of lower level failures, such as a malfunctioning part

[1] This paper examines, primarily, the impacts on society when transmission systems are affected. Transmission systems are those that transfer power over large geographic distances at a high voltage strength from power generation facilities to community substations, referred to in North America as "interconnects." Upon reaching a community, power is run through distribution lines from the substation to residences and properties. As such, distribution grids are largely independent of one another, but heavily reliant on the transmission system. While a distribution failure is localized, a transmission failure can, in contrast, affect a number of distribution zones.

or unit, as well as the use of management techniques or technological advances to mitigate these failures appropriately; it is in the prevention of unknown risks where they fundamentally differ in nature.

High Reliability Organization Theory

The central tenant of HRO can be summarized as: “safe operations are possible […] if appropriate organizational design and management techniques are followed” (Sagan, 1993, p. 13). Those subscribing to this point of view emphasize the influence of management and experts in the control of an organization (Hopkins, 2007). It is believed that the tools available to decision-makers can be used to address any vulnerability that may arise and therefore mitigate risks to a manageable size. Tools available to the HRO practitioner include effective management processes such as: decentralized decision-making, an increased emphasis on safety, the embrace of redundancy and uniformity, and continuous training, and learning from previous experiences (Sagan, 1993). In this way, HRO theorists stress the importance of learning from failures more so than successes (Hopkins, 2007). As such, HRO theorists emphasize the importance of anticipatory and resilience mechanisms in managing highly-complex and tightly-coupled organizations (Sagan, 1993; Hopkins, 2007).

If a systems accident were to occur in a complex organization, HRO theorists would argue that effective management oversights were not in place. Thus, HRO theorists are highly optimistic as they believe in the human ability to manage complex organizations and the externalities to those systems (Sagan, 1993); in fact, they believe that “formal organizations can create rules, structures and processes to regulate risky decision-making” within an organization (Vaughan, 1996, p. 415). HRO emphasizes the importance of the collective capacity of individuals within an organization—an organization can compensate for individual weaknesses, therefore, allowing the organizational whole to become “more rational and effective than [the] individuals” that comprise it (Sagan, 1993, p. 16).

Normal Accidents Theory

In contrast to HRO theory, Normal Accidents theory describes the inevitability of system accidents that are inherent to highly-complex and tightly-coupled organizations. While HRO theorists assume that the elimination of risk is achievable through rational decision-making, NAT theorists believe that these systems are too complex to comprehend fully. The “theory of bounded rationality” states that limits on rational decision-making are an inherent quality of complex systems (Perrow, 1999, p. 316), resulting in decisions that are less-than-optimal solutions, known as “satisficing”. NA theorists argue that the level of uncertainty, which leads to satisficing and is exacerbated by satisficing behaviours, increases the risk of system accidents. This approach diminishes the role of management and expert opinion as it serves to highlight the vulnerability of human constructions, such as highly-complex organizations, despite the best intentions of those individuals within the organization (Sagan, 1993). NAT

theorists argue that an integral role of management is assessing the tolerance for system accidents; if the risks associated with inevitable failure are unacceptable, the system should be abandoned (Perrow, 1999).

Because they acknowledge that "we cannot know everything about these complex and hazardous technologies" within organizations, NAT theorists believe that system accidents are "normal and inevitable" (Leveson, et al., 2009, p. 229). New system accidents will occur regardless of how much an organization learns from its previous mistakes. In contrast to the optimism expressed in HRO theory, NAT is inherently pessimistic (Sagan, 1993) or, depending on one's point of view, *realistic* as it acknowledges the impossibility of "failure-free operations" (LaPorte & Consolini, 1991, p. 42).

Examining these two theories of organizational failure helps to highlight organizational management of risk and is useful for managers to understand particular vulnerabilities in modern tightly-coupled and complex organizations. This is especially true of CEI in North America where international borders are crossed and the necessary technology is vulnerable to both human and natural threats, which can, at times, be unpredictable. As a result, organizations become more internally complex and flexible in their organizational structure in order to adapt a vast array of possible contingencies (La Porte, 2006). An examination into electrical system failures is, therefore, especially important due to the electrical grid's interdependence with other critical infrastructure sectors. As the case study demonstrates, other critical infrastructures such as health and transportation depend on the efficient and consistent operations of CEI, and as such, are greatly impacted when energy or electrical infrastructures are damaged. Furthermore, CEI "is of paramount importance to the economy," and therefore, its protection is crucial in order to limit "the threat of cascading failures" (Shore, 2008, p. 2; Watts, 2003, p. 565). The remainder of this paper outlines the case of a large-scale power outage in North America's Eastern Interconnect electrical grid within the context of HRO and NAT. This is done to inform recommendations for public managers in controlling CEI within this grid.

Case Study: The 1998 Ice Storm

The January 1998 Ice Storm, which occurred in the northeastern portion of Canada and the United States, illustrates the impossibility of "failure-free operations" (LaPorte & Consolini, 1991, p. 42). Electrical grid failure throughout Ontario, the Maritime provinces, the New England states, and particularly Québec, was provoked by a natural disaster of previously unseen financial and physical severity, representing nearly $1.44 billion in insured losses (Lecomte, 1998). The damage inflicted on the electrical grid (both the Eastern and Québec Interconnects), caused by the icy precipitation, resulted in a number of energy infrastructure failures; approximately 1 000 high-tension wire pylons, 35 000 wooden utility poles, and 120 000 kilometres of electrical lines (transmission and distribution level) were destroyed as a result of the storm (Lecomte, 1998). This damage left approximately five million Canadians

(16% of the Canadian population) and nearly 550 000 Americans without electricity, representing approximately five-and-a-half million affected citizens in total (Lecomte, 1998). Furthermore, Canada's economic output declined by 0.7 percent in January 1998 in part due to the fact that Canadians were "impeded or prevented from getting to work" (Lecomte, 1998, p. 14). Additionally, 30 Canadian deaths were associated with the impacts of the storm (Aubin, 2003). These economic and health impacts demonstrate North America's dependency on electricity, the electrical system's vulnerability to hazards, and the lack of holistic planning in protecting the grid from large-scale failures (Lecomte, 1998).

Natural disasters that are followed by industrial failures are not uncommon—other examples include the disasters associated with Hurricane Katrina and the tsunami in Fukushima, Japan. These cases represent a series of failures to protect infrastructure (i.e. power lines, levees, nuclear power facilities) before a natural disaster. While HRO theorists would suggest that such failures are the result of insufficient planning, and therefore, could have been prevented, NAT theorists would argue that these failures are the result of the complex interdependencies and tight-coupling inherent to electricity systems. In the case of the 1998 Ice Storm, vast geographic spread and interdependence, a lack of governmental coordination, and poor reactionary procedures (Lecomte, 1998) limited the electrical grid's management decision-making. Since appropriate information-sharing between decision-makers was not in place (Lecomte, 1998), decisions made regarding the protection of the grid were bounded or satisficing in nature, and thus, exposed the grid to risk before the increased pressures on the system due to the ice storm.

At the same time, however, infrastructure failures such as the 1998 Ice Storm demonstrate the general principles of Normal Accident Theory: failures are inevitable, and as such, demonstrate human and infrastructure vulnerability. In essence, NAT stresses *possibility* over *probability*: it emphasizes that the mere potential for an event or hazard to occur is enough to conclude that it will, eventually, happen (Clarke, 2005). Specifically, this perspective suggests that "it can be downright dangerous to neglect possibilities in favour of probabilities" (Clarke, 2005, p. 41). Such is the pessimistic nature of NAT—electricity blackouts are perceived as normal and inevitable in tightly-coupled and complex systems such as the Eastern Interconnect. NAT acknowledges this vulnerability and in a fatalist twist, accepts this fate: we accept the fact that we are not in control of the systems we create.

Lessons Learned

Potential failure in CEI is an example of a systemic risk because it is "embedded in the larger contexts of societal processes," and it requires "a more holistic approach to risk management" (Renn et al, 2011, p. 234). The Ice Storm of 1998 would fall into the uncertain subset of systemic risk because of its magnitude and severity—the lack of data would have made it difficult to assess its probability. It is due to the increasingly systemic nature of risk exposure in CEI that it has become of utmost importance in the protection of critical infrastructures.

Consequently, handling systemic risk depends on what classification the risk is (i.e. uncertain, ambiguous, simple, or complex). For uncertain risks, such as the 1998 Ice Storm, consultation with agency staff, experts, and industry stakeholders provides a more holistic view of the particular risk domain. This ongoing dialogue allows the grid's management body to focus on institutional resilience in order to ensure the "reversibility of critical decisions" (Renn et al., 2011, p. 1). In this way, the solutions proposed by HRO theorists can prove effective in the management of electrical grids.

This case highlights the extent to which risk and failure are tolerated in the energy industry. In a system fraught with vulnerabilities, the lack of protection of the electrical grid appears contradictory (Amin, 2004). CEI is important in today's complex and tightly-coupled society; as part of the "golden triangle" of critical infrastructure (Power Switch, 2005, p. 4),[2] other critical infrastructures are excessively reliant on electrical systems. According to this principle, CEI should have a low tolerance for risk, and subsequently, for failure. Furthermore, the nature of uncertain risks associated with energy infrastructure along with its reliance on expert-opinion requires CEI to have a low tolerance for risk (Hopkins, 2007; Renn 2011). However, this examination has demonstrated that minimal efforts have been taken to protect North America's energy infrastructure.

This case did prompt, to some extent, organizational learning. As a result of earlier blackouts and the 1998 Ice Storm, Hydro Québec spent approximately $3 billion upgrading its power grid. The system was modified to be self-sufficient, and therefore, protected from the complexities introduced by interconnected systems that may have been overworked (Catalan & Robert, 2010). The actions of Hydro Québec demonstrate that by focusing on reducing "unnecessary complexity" (lessening coupling) as opposed to creating redundancies, organizations or systems can increase reliability without compromising efficiency (Leveson et al., 2009). The lessons learned from the ice storm were a key factor in Québec's ability to remain unaffected by the Northeastern Blackout in 2003, and as a result, the province was able to divert 1 000 MW of electricity to affected areas (Aubin, 2003). In order to effectively manage CEI in the future, grid management must acknowledge the benefit that comes from learning from failures and strive toward the correction of errors that lead to these failures. Again, such an approach acknowledges the tenants of HRO theorists.

This case of organizational learning represents the tendency of complex and tightly-coupled systems to revert from a decentralized, individualist approach to a more centralized and hierarchical approach when failures occur (Chang et al., 2007). This is demonstrated in Ontario and the United States— jurisdictions that have taken steps toward setting standards to

[2] The "golden triangle" refers to the importance of telecommunications, banking, and energy systems on modern day societies. If one of these infrastructures were to fail, other critical infrastructures, such as health (hospital systems), transportation systems, and public safety systems, would be directly impacted due to their reliance on the "golden triangle" of critical infrastructure as part of their daily operations.

ensure the continued maintenance of, and investment in, CEI in response to the 2003 Blackout. A privatized energy sector with many stakeholders, such as the one present in Ontario in 1998, poses certain challenges to regulation efforts, namely the motivation to put infrastructure investment before profit (LaPorte & Consolini, 1991, p. 32). Furthermore, the public "still expect[s] governments to step in and maintain the reliability of service provision;" therefore, motivation for the private-sector to invest in infrastructure is hindered by the fact that governments are, ultimately, is held responsible when infrastructure fails (de Bruijne and van Eeten, March 2007). Efforts to stabilize the sector have proven unsuccessful thus far:

> Whether measured in terms of city-sized blackouts or smaller events, the statistics show that reliability has not improved. Indeed if the data show any trends in the past few years, it is toward lower reliability (Apt, Lave, & Morgan, 2009, p. 8).

In the case of Québec, however, where a crown corporation Hydro Québec, managed the electrical grid, investment in infrastructure was not ignored in favour of profit. Further, Ontario's actions in response to the 2003 Blackout demonstrate the broader trend of moving toward centralization in managing electrical grids. This movement reinforces the NAT assertion that these systems, due to their complex nature, must be standardized. Such standardization will encourage organizational resiliency, communication, and cooperation when systems inevitably fail.

Another way to manage electrical systems while operating under the NAT assumption that failures are inevitable is to use scenario-based planning tools (Van der Heijden, 2005). Planning tools, like scenario analysis, are used to 'predict the unpredictable'. Such devices allow planners and managers to consider possibilities instead of probabilities, and to effectively consider all options (Clarke, 2005). Such tools enable organizations "to respond quickly to events in a way that would have been impossible without the mental preparation of the scenario analysis" (Van der Heijden, 2005, p. 7).

Conclusion

The consequences of critical energy infrastructure failures are immense. The nature of its tight-coupling with other critical infrastructure sectors highlights the importance of protecting electrical lines, substations, and generators. By articulating the central arguments of HRO and NAT, this paper has demonstrated the importance of standard setting and behaviour modification in ensuring that critical energy infrastructure within the Eastern Interconnect is adequately protected (LaPorte & Consolini, 1991; Apt, Lave, & Morgan, 2009). The extent to which CEI is protected from systemic and uncertain risks within North America, however, does not reflect the level of protection that should be in place. While acknowledging the inherent exposure of CEI to risk, and therefore failure, this paper points to several methods in which tightly-coupled and highly complex systems such as power grids can avoid or minimize the impacts of system accidents. Overall, these approaches reflect the prevalence of Normal

Accident Theory in the critical infrastructure realm—decision-makers in a privatized electrical sector are likely to invest more in to planning for failures and organizational resilience rather than predict, invest, and control as discussed in High Reliability Organizational theory in response to the failures that are bound to happen in tightly-coupled and complex electrical grids.

References

Amin, M. (2004). North American electricity infrastructure: System security, quality, reliability, avaliability, and efficiency challenges and their societal impacts. National Science Foundation (Ed.). *National Science Foundation (NSF) report on "Continuing Crises in National Transmission Infrastructure: Impacts and Options for Modernization* (Chapter 2). Retrieved from http://central.tli.umn.edu/amin/NSF_Chapter2.pdf

Apt, J., Lave, L. B., & Morgan, M. G. (2009). Can the U.S. have reliable electricity (working paper CEIC-06-02). *Carnegie Mellon Electricty Industry Center*.

Aubin, B. (2003, August 25). Memories of a long, cold electricity outage. *Maclean's Magazine*. 26.

Catalan, C., & Robert, B. (2010). *Evaluation of organizational resilence: Application in Quebec*. Montreal, QU: Ecole Polytechnique du Montreal.

Chang, S. E., McDaniels, T. L., Mikawoz, J., & Peterson, K. (2007). Infrastrucuture failure interdependencies in extreme events: Power outage consequences in the 1998 Ice Storm. Natural Hazards, 41(2), 337-358. http://dx.doi.org/10.1007/s11069-006-9039-4

Clarke, L. (2005) *Worst cases: Terror and catastrophe in the popular imagination*. Chicago, IL: University of Chicago Press.

de Bruijne, M., & van, Eeeten, M. (2007). Systems that should have failed: Critical infrastructure protection in an institutionally fragmented environment. *Journal of Contingencies and Crisis Management, 15*(1), 18-29. http://dx.doi.org/10.1111/j.1468-5973.2007.00501.x

Hopkins, A. (2007 January). *The problem of defining high reliability organizations* (Working Paper 51). National Research Centre for Occupational Health and Safety Regulation. Retrieved from http://ohs.anu.edu.au/publications/pdf/wp%2051%20-%20Hopkins.pdf

LaPorte, T.R., & Consolini, P. (1991). Working in practice but not in theory: Theoretical challenges of "high reliability organizations". *Journal of Public Administration Research and Theory, 1*(1), 19-48.

La Porte, T. (2006). Seeds of disaster, roots of response: How private action can reduce public vulnerability. Eds. Philip E. Auerswald*. In Organizational Strategies for Complex System Resilience, Reliability, and Adaptation*. pp. 135-154.

Lecomte, E.L., Pang, A.W., & Russell, J. W. (1998 December). *Ice storm '98*. Institute for Catastrophic Loss Reduction Research Paper Series. No. 1. pp. 1-37.

Leveson, N., Dulac, N., Marais, K. & Carroll, J. (2009). *Approach to safety in complex systems moving beyond normal accidents and high reliability organizations: A systems approach to safety in complex systems*. European Group for Organizational Studies: Sage Publications. pp. 227-249.

Perrow, C. (1999). *Normal Accidents: Living with High Risk Technologies*. 2nd ed. Princeton, NJ: Princeton University Press.

Power Switch . (2005, April 27). *Oil and food, infrastrcuture and interdepenencies*. Retrieved from http://www.powerswitch.org.uk

Renn, O., Klinke, A., & Asselt, M. (2011). Coping with complexity, uncertainty and ambiguity in risk governance: A synthesis. *Ambio, 40*(2), 231-246. http://dx.doi.org/10.1007/s13280-010-0134-0 PMid:21446401

Sagan, S.D. (1993). *The limits of safety: Organizations, accidents, and nuclear weapons*. Princeton, NJ: Princeton University Press.

Shore, J.M. (2008, March). *The legal imperative to protect critical energy infrastructure*. Critical Energy Infrastructure Protection Policy Research Series. Ottawa, ON: The Canadian Centre of Intelligence and Security Studies.

Van der Heijden, K. (2005). *Scenarios: The art of strategic conversation*. 2nd ed. Chichester, UK: Wiley.

Vaughan, D. (1996). *The Challenger launch decision: Risky technology, culture, and deviance at NASA*. Chicago, IL: University of Chicago Press.

Watts, D. (2003, October). *Security and vulnerability in electric power systems*. 35th North American Power Symposium. In Rolla, Missouri: University of Missouri. 559-566.