Modelling the Role of Software in the Propagation of Failures Across National Critical Infrastructures

Chris. W. Johnson

Department of Computing Science, University of Glasgow, Scotland, UK, Johnson@dcs.gla.ac.uk

http://www.dcs.gla.ac.uk/~johnson

Previous terrorist attacks, system failures and natural disasters have revealed the problems that many States face in preparing for national civil contingencies. The diversity of critical infrastructures and the interconnections between different systems makes it difficult for planners to 'think of everything'. For example, the loss of power distribution networks can disrupt rail and road transportation systems. Knock-on effects can also be felt across telecommunications infrastructures as the uninterruptible power supplies (UPS') that protect mobile phone base stations fail over time. Domestic water supplies are affected when pumping and treatment centres lose power.

It is difficult to under-estimate the safety implications of these interdependencies. For example, Pironi, Spinucci and Paganelli describe how the Italian blackout of 2003 affected patients that relied on home parenteral nutrition systems [1]. These individuals used electronic pumps for the overnight infusion of nutritional solutions. The loss of power disrupted their treatment. Different devices responded in different ways as some began to generate alarms while others reverted to battery power. Patients responded in different ways as they became worried about whether or not their systems had sufficient power to complete their treatment for that night. The blackout lasted several days across many areas of Italy. This created further problems as stores of parenteral solution had to be stored in freezers. Other patients were placed at risk when the loss of power began to affect water treatment centres. It became difficult to guarantee that there was no microbiological or toxic contamination in the water supplies for dialysis patients.

One area of increasing concern is the dependencies that are created by the use of digital communications systems to connect key areas of our national critical infrastructure. For example, the separation of responsibility for maintaining electricity distribution systems and for generating or marketing power has created a situation where software systems are increasingly used to monitor and respond to changing demands across the network. Infrastructure operators rely on digital communications systems to balance the complex interactions between supply and demand as market pressures encourage large scale power transfers between low cost generators and remote end users. Failures in the digital communications systems can propagate to the distribution networks and vice versa. Many commercial and government agencies have recognised these vulnerabilities and have responded, for example, by placing reliability requirements on the networks and software that support critical infrastructures. However, there are strong commercial pressures for more and more systems to use the public Internet. At the same time, Hurricane Katrina and the UK floods of 2007 have illustrated that it may be inappropriate to place high-levels of confidence in bespoke networks.

Forensic techniques can help to identify patterns of failure across digital communications systems. For example, a number of studies have been conducted into the impact of the 2003 US-Canada blackout on Internet traffic. Abnormal Border Gateway Protocol (BGP) events indicate that 3,175 networks lost connectivity. Most of these were in the New York City area [2]. However, we are a long way from being able to conduct more predictive forms of analysis at a regional level. In particular, there are no agreed means of modelling the effects of any future power system failures on national computational infrastructures. This, in turn, makes it impossible to anticipate the secondary impact of the loss of Internet connectivity on the increasing numbers of critical systems that rely upon these networks for the exchange of operational information.

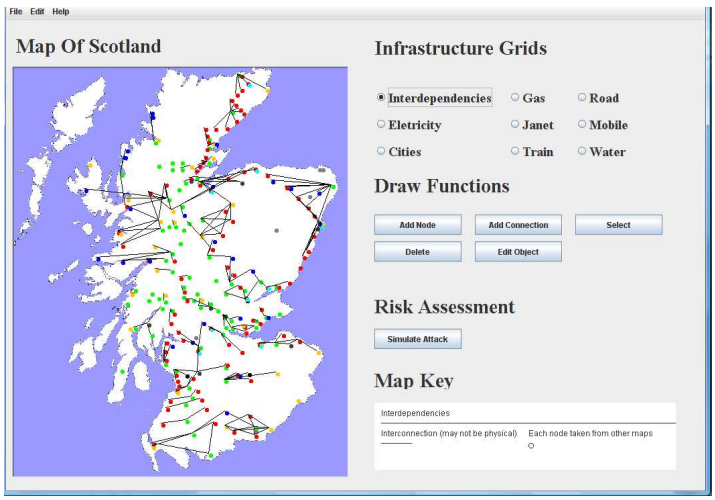

Figure 1: Infrastructure Dependencies GIS (ID-GIS)

It will take many years before we can the knock-on effects that would arise if we were to lose significant sections of our digital communications and power distribution networks. Figure 1 illustrates the interface to a Geographical Information System that exploits Bayesian techniques to generate failure scenarios across national critical infrastructures [3, 4]. This approach provides an alternate to the detailed causal modelling of infrastructure interdependencies that are created by the increasing integration of digital communications networks to support everything from food distribution to the monitoring of large volume gas transmission. Expert judgement can be used to assess the dependent probability of a system failing given that problems have been observed in another infrastructure. Where possible, these estimates can steadily be refined with more accurate probability distributions based on partial causal models or from data obtained during previous contingencies. Further information about these techniques can be obtained from the author and on the web site indicated above.

[1] L. Pironi, G. Spinucci and F. Paganelli, Effects of the September 28 2003 blackout in Italy in patients on home parenteral nutrition (HPN), Clinical Nutrition, (23)1:133, February 2004.

[2] J. Li, D. Dou, Z. Wu, S. Kim and V. Agarwal, An Internet Routing Forensics Framework for Discovering Rules of Abnormal BGP Events**,** ACM SIGCOMM Computer Communication Review, (35)5:55-66, 2005.

[3] C.W. Johnson and K. McLean, Tools for Local Critical Infrastructure Protection: Computational Support for Identifying Safety and Security Interdependencies between Local Critical infrastructures. To appear in the Third IET Systems Safety Conference, Birmingham, UK, 2008.
Preprint available from: http://www.dcs.gla.ac.uk/~johnson/papers/IET_2008/Local_Critical_Infrastructure_Final.pdf

[4] C.W. Johnson and R. Williams, Computational Support for Identifying Safety and Security Interdependencies between National Critical Infrastructures. To appear in the Third IET Systems Safety Conference, Birmingham, UK, 2008. Preprint available from:
http://www.dcs.gla.ac.uk/~johnson/papers/IET_2008/National_Critical_Infrastructure_Final.pdf