COMPDYN 2013
4th ECCOMAS Thematic Conference on
Computational Methods in Structural Dynamics and Earthquake Engineering
M. Papadrakakis, V. Papadopoulos, V. Plevris (eds.)
Kos Island, Greece, 12–14 June 2013

SECURING COMMUNITY RESILIENCE BY MODERN INFRASTRUCTURE DESIGN

Thomas Pickering[1], Sarah Dunn[2], Dr Sean Wilkinson[2]

[1]School of Civil Engineering and Geosciences, Newcastle University
Newcastle University, Newcastle Upon Tyne NE1 7RU, UK
thomas.pickering@ncl.ac.uk

[2]School of Civil Engineering and Geosciences, Newcastle University
Newcastle University, Newcastle Upon Tyne NE1 7RU, UK
sarah.dunn@ncl.ac.uk, s.m.wilkinson@ncl.ac.uk

Keywords: Infrastructure, Disaster Engineering, Resilience, Fragility

Abstract: *In the National Security Strategy and Strategic Defence and Security Review, the UK Government prioritised the need to improve security and resilience against attack, damage or destruction of infrastructure critical to keeping the country running. In response to this a guide (Keeping the Country Running: Natural Hazards & Infrastructure) was produced to focus on one of these threats, natural hazards.*

The purpose of the guide is outlined as "to encourage infrastructure owners and operators, emergency responders, industry groups, regulators, and government departments to work together to improve the resilience of critical infrastructure and essential services" [1]. "To share best practice and advice to enable organisations to continuously improve their infrastructure's resilience to natural hazards." And to "supplement existing guidance and fills gaps identified during the consultation on the Strategic Framework and Policy Statement in March 2010".

The guide suggests that resilience can be secured through a combination of four main elements; namely: resistance, reliability, redundancy, and response and recovery. In this paper we demonstrate how these components all contribute to achieving resilient communities. We analyse the resilience of a simple network which is augmented and subjected to events of different magnitudes to quantify the performance of the degraded systems. In our examples, the first network has a greater resistance (which incorporates reliability) to the disruption, whilst the second network has a greater redundancy and the third network has a superior response. We demonstrate that for each disruption the three networks have different resilience and that the most resilient network changes for each level of disruption. The examples presented in this paper illustrate a methodology for designing resilient critical infrastructure networks and demonstrate how all elements of resilience must be considered to achieve communities that can resist natural hazards.

INTRODUCTION

In the National Security Strategy and Strategic Defence and Security Review the UK government prioritises the need to improve security and resilience of critical infrastructure [1]. The review identifies that natural hazards are a large risk to the UK's security interest, as a result the "Keeping the Country Running: Natural Hazards & Infrastructure" document was developed as a guide to "*encourage infrastructure owners and operators, emergency responders, industry groups, regulators, and government departments to work together to improve the resilience of critical infrastructure and essential services*" [1]. This document presents a methodology to assess the resilience of critical infrastructure to natural hazards and to test potential mitigation strategies prior to deployment.

The Cabinet Office [1] defines Resilience as, "*the ability of assets, networks and systems to anticipate, absorb, adapt to and / or rapidly recover from a disruptive event*", the guide then progresses to define four key principles which contribute to infrastructure resilience (Table 1).

Resistance	"*to prevent damage or disruption by providing the strength or protection to resist the hazard"*
Reliability	"*ensuring that the infrastructure components are inherently designed to operate under a range of conditions"*
Redundancy	"*availability of backup installations or spare capacity will enable operations to be switched or diverted to alternative parts of the network"*
Response and Recovery	"*enable a fast and effective response to and recovery from disruptive events"*

Table 1 – Captions of definitions from the "Keeping the Country Running" document

These four principles are important in achieving community resilience because unlike other forms of the built environment these systems form complex networks which provide essential services to the community. The design emphasis therefore is to provide systems capable of delivering critical services even when the design hazard is exceeded and not simply providing infrastructure components with sufficient resistance to withstand particular hazard intensities. For example the power network supplies electricity across the country and a small physical disruption to the infrastructure of this system can have a devastating effect on the service it provides and in turn the citizens who rely on it.

The work presented in this study examines each of these principles to determine the influence each has on network resilience. This is achieved by subjecting three simple six node power networks to a simulated wind hazards and then relating post event performance to each of the four principles.

RESISTANCE, REDUNDANCY AND RESPONSE OF A SIMPLE NETWORK

So how do we incorporate all of these into our critical infrastructure networks? We do this by adapting a methodology used in earthquake engineering. Seismic design is unusual in that there is increased emphasis on scenarios where the system is overloaded. This started as a dual design approach, which is still what is used in the majority of cases, but has moved to performance based design - at least theoretically. In this approach we are trying to minimise the cost due to earthquake induced damage by integrating all of the costs resulting from all likely earthquakes during the life of a structure. This is achieved by using a hazard model to generate earthquakes which are then fed into a computer simulation that predicts building damage, the cost of which is then estimated by a damage model. One approach to this type of methodology is the discussion presented by Bruneau [2]. In the discussion Bruneau outlines the aspects involved in securing community resilience for earthquake hazards and confers a framework, which enables the assessment and evaluation of the contributions of various activities to resilience. In a similar way this study aims to evaluate the aspects of infrastructure design which contribute to resilience, however the objective of this study is to demonstrate a methodology which can assess the performance of a network at system level by evaluating resilience to hazard at a component level.

To demonstrate this methodology and how the four principles of infrastructure resilience contribute to system resilience a simple network model is analysed, where an electricity Control Network (Figure 1a) with a single generation source (node 1), supplies surrounding demand nodes (substations). To demonstrate the concepts of resistance, redundancy and response, the resistance of the network is modelled using a fragility curve (a curve which relates probability of failure for a component to an event magnitude [3]) (Figure 2), enhanced with additional links for redundancy (Figure 1c) and a simulated crisis management plan for response (which does not alter the network's physical properties) (Figure 1d). The fragility curve for each network is used to determine random failures, and the resulting network connectivity's are analysed to determine which network performs best for each hazard.

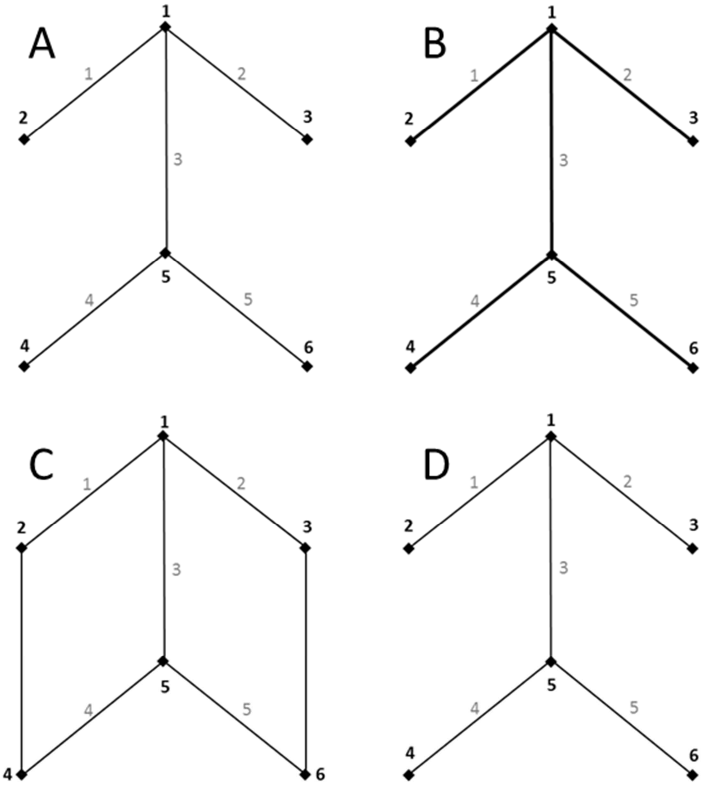

Figure 1 - Network Maps – Control (A), Resistant (B), Redundant (C), Response (D).

The networks are subjected to hypothetical windstorm events which vary in magnitude; however for demonstration purposes the intensity on each element within each network is considered equal (i.e. the hazard that each element is exposed to is identical.) This technique reflects the properties of a desired system in which each element with the same physical properties has the same fragility. In a real system however variations may exist in some characteristics, which could affect this (for example, lack of maintenance at one of the substations, or a transmission tower being located in a coastal environment resulting in increased corrosion) but for now we will ignore this.

Resistance is represented by fragility curves [3, 4, 5], where the probability of failure of the population of elements is defined as a function of hazard intensity, in this case wind speed (Figure 2). The Resistance Network has greater strength (a result of the network being constructed with stronger materials for example), and therefore its components have a correspondingly smaller probability of failure. The fragility of the Redundant and Response Networks are identical to the Control Network, the resilience of the Redundant Network originates from additional network links, and the Response Network from a better crisis management plan, which enables repair of damaged links to be made more quickly.

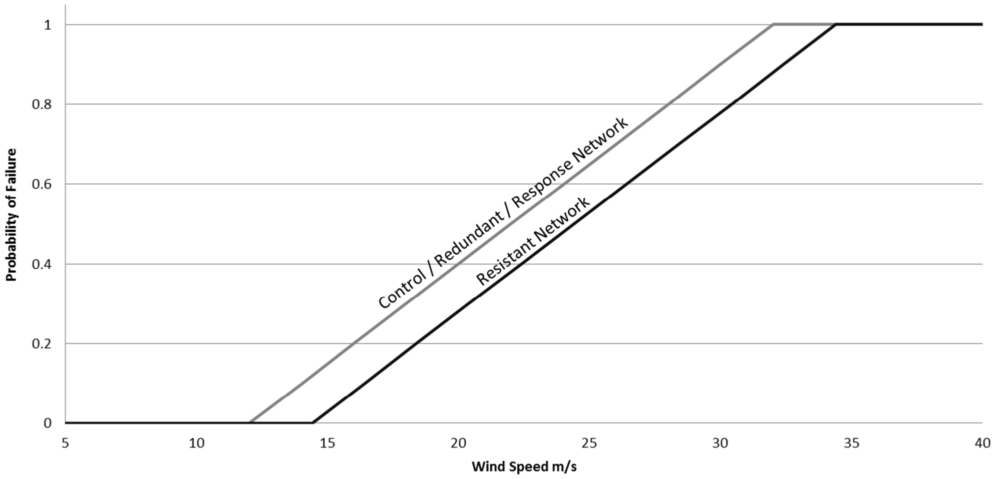

Figure 2 - Network resistances are depicted as conceptual fragility curves. As the event magnitude increases, the probability of failure increases linearly, until it equals 1 (where complete failure of the network occurs).

$$P(F_i|v)\ \epsilon_i = 1,2,3 \qquad (1)$$

$$P(F_i|v)\ \epsilon_i = 4 \qquad (2)$$

By introducing additional links into the Control Network we create resilience through redundancy. Therefore, in the event of failure, the network has an increased chance of staying connected (i.e. each of the substations maintain a connection to the supply), even if it may be at a reduced efficiency. Figure 1 Network C shows the augmentation introduced to the Control Network to create this redundancy.

To determine which network is more resilient, the process adopted has been to conduct a Monte Carlo simulation where events of a given magnitude are used to generate failure probabilities for each component in the various networks and then to assess the performance of the degraded networks. The results of many simulations are then averaged and compared to determine their relative resilience. Three intensity scales have been investigated; low magnitude, medium magnitude and high magnitude.

Low magnitude event

The first scenario considered is a low magnitude event at 14ms^{-1}, which results in a probability of failure of 10% for each link in the Control Network (as well as the Redundant and Response Networks), and correspondingly a 0% of failure on the Resistant Network.

In this simulation the result of 100 trials of the Monte Carlo simulation, the Control Network sustained 48 node disconnections out of a possible total of 500; similarly the Redundant Network sustained 11 out of 500 disconnections. In the case of the Resistant Network however, the increased strength of the elements results in no links failing (Table 2), as the Response Network is identical to the Control Network, the result for the Control Network is representative of both networks.

	Control Network	Resistant Network	Redundant Network
Total nodes analysed	500	500	500
Number of isolated nodes	68	0	11
Percentage of failed nodes	13.6%	0%	2.2%
Degraded performance ratio	-	0	0.16

Table 2 – Summary of 100 trials comparing the control, resistant and redundant networks for a low magnitude event

The key value from Table 2 is the degraded performance ratio; this indicates the comparative difference in the number of disconnections between a network and the Control Network. For this low magnitude event it can therefore be seen that the degraded performance of the Redundant Network compared to the Control Network is 0.16, (i.e. an 84% decrease in the number of isolated nodes). For the Resistant Network this value is 0, this indicates that for the low magnitude scenario it is the most resilient as the closer the degraded performance is to zero the better the network has performed in relation to the Control Network.

Consequently for low magnitude events, Table 2 indicates that the Resistant Network is the most resilient as there are no repair costs associated with replacing any failed links (i.e. the least number of failures), nor is there any associated cost with service losses. Both the Control and the Response networks have the greatest number of node disconnections; however the Control Network is the least resilient as the Response Network will be repaired more quickly and this is demonstrated in greater detail in the next example.

Medium magnitude event

In the second event, the magnitude is increased to 20ms^{-1}. Figure 2 now indicates corresponding failure probabilities of 40% and 28% for the Control and Resistant Network elements respectively. The simulation is repeated and new performance ratios are obtained. The results of the simulation are displayed in Table 3.

	Control Network	Resistant Network	Redundant Network
Total nodes analysed	500	500	500
Number of isolated nodes	224	157	126
Percentage of failed nodes	44.8%	31.4%	25.2%
Degraded performance ratio		0.70	0.56

Table 3 – Summary of 100 trials comparing the control network to the resistant network for a medium magnitude event

What can be seen from **Error! Reference source not found.** is that for the medium magnitude event the degraded performance ratios are 0.7 and 0.56 for the Resistant and Redundant Networks respectively, which indicates that the Redundant Network has outperformed the Resistant Network by 6%. For the medium magnitude event it can therefore be concluded that Redundant Network is the most resilient, as it results in less disruption to consumers.

Medium magnitude event - Response

Keeping the Country Running, outlines response as "*the effectiveness of this element is determined by the thoroughness of efforts to plan, prepare and exercise in advance of events*"[1], because of this, resilience cannot be quantified through the methods previously investigated. Instead, resilience is obtained through planning and event management; by incorporating these additional preparations network restoration time after a failure is reduced. To demonstrate this response planning each of the networks is first subjected to a medium magnitude event, and the restoration of the network is then plotted as available capacity against time (Figure 3). In the example shown by Figure 3, response planning allows the reconstruction of failed links to begin in 50% of the time it takes the other networks; only one link per time step can be restored in this model, regardless of network type.

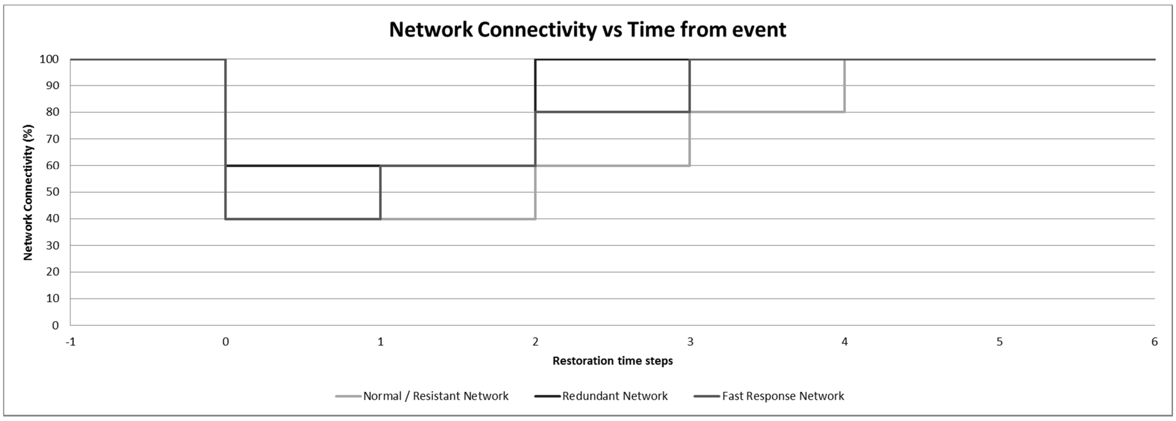

Figure 3 - Graphical representation or restoration time for each network after an event

Figure 3 displays the effect of a medium magnitude event on each of the network types. The event has disrupted links 1, 2 and 5 on all networks. This reduces the functioning capacity of the Control Network group to 40% (2 connected nodes) and 60% on the Redundant Network (3 connected nodes). Progressively one time step allows the Response Network to have its first link repaired increasing its connectivity to 60%, a result of the better event planning. At the second time step the Response Network increases to 80% connectivity, the Control and Resistant Network increase to 60% connectivity (first repair); however the Redundant Network reconnects all nodes to the network, a result of the additional links which did not fail. This makes the Redundant Network the most resilient as the other networks at the end of the second time step each have one node disconnected. In time step 3 the Response Network is restored, and in time step four the Control and Resistant Networks are restored.

Large magnitude event

In this event, a large magnitude of wind speed (36ms^{-1}) is chosen, this wind speed results in failure of all the links in all the networks. The advanced planning associated with the Response Network returns it to full capacity in the shortest time making it the most resilient, (Figure 4) resulting in fewer overall losses. The Control, Resistant and Redundant Networks are returned to operating capacity in the same amount of time after the Response Network (note the redundant network has the same resilience as it will be initially repaired in a form that is identical to the other networks. Subsequent to this it will continue to be restored to its original configuration and there would be an extra cost associated with this. The Resistant and Redundant Networks are the least resilient for a high magnitude event because of the additional cost associated with the stronger elements and additional links (transmission lines) in each respective network.

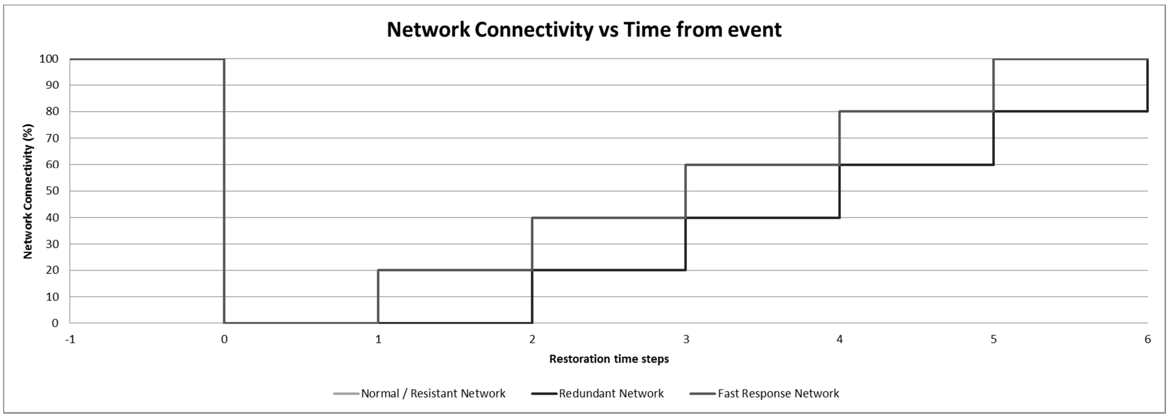

Figure 4 - Large magnitude event network restoration

RELIABILITY OF NETWORKS

"The Reliability component is concerned with ensuring that the infrastructure components are inherently designed to operate under a range of conditions and hence mitigate damage or loss from an event. The tendency of a reliability strategy is to focus only on the events within the specified range, and not events that exceed the range. This can lead to insufficient awareness or preparation for events outside of the range, and hence significant wider and prolonged impacts can occur. Reliability cannot therefore be guaranteed, but deterioration can sometimes be managed at a tolerable level until full services can be restored after the event" [1]

Put simply this definition of reliability is concerned with both the infrastructure having sufficient resistance for events that can be considered reasonable design events but also to have some capacity after exposed to events greater than this.

One interpretation of reliability is therefore; for the expected range of events, components are designed to be strong enough they operate efficiently during normal conditions, which is the resistance procedure already analysed. For events that are not designed for, i.e. events which cause loads above the design threshold; reliability idealises some operational capacity to remain after a failure occurs, which can be interpreted as a form of redundancy. This can be imagined using a transmission line. The line operates within tolerances until it is subjected to an event greater than the design strength of the system and its components, which for example causes the failure of a conductor, hence failure of one circuit of the transmission line. The line can then be considered failed, however the tower may support a second circuit which remains operational and hence the line in the network still holds some capacity after the failure event, unlike the redundancy study investigated earlier where a failure was complete interruption of the line. It can also be considered that additional power capacity may also exist in the second circuit if it was not operating at its maximum when the event occurred (redundancy in the cables). During a higher magnitude event the tower may experience a collapse failure, in this case complete failure would be observed. True redundancy is therefore a combination of the number of circuits in a line, the amount of power flow in these circuits as a percentage of their peak power flow, and the number of lines which can supply power from site A to site B.

Reliability is then formed from the resistance of these components, some amount of spare capacity and the redundancy of the system that these components create.

In regards to deterioration effects, which are highlighted in the definition for reliability [1], a traditional approach can be used. Deterioration can be considered at component and system levels. In the previously examined cases, component resistance has been described through use of a fragility curve. When we consider deterioration in component resistance, this fragility curve shifts leftwards along the magnitude axis, a result which could for example be caused by corrosion. The result of this is that probability of failure increases for lower magnitude events; maintenance closely returns the fragility curve to its initial position (Figure 5).

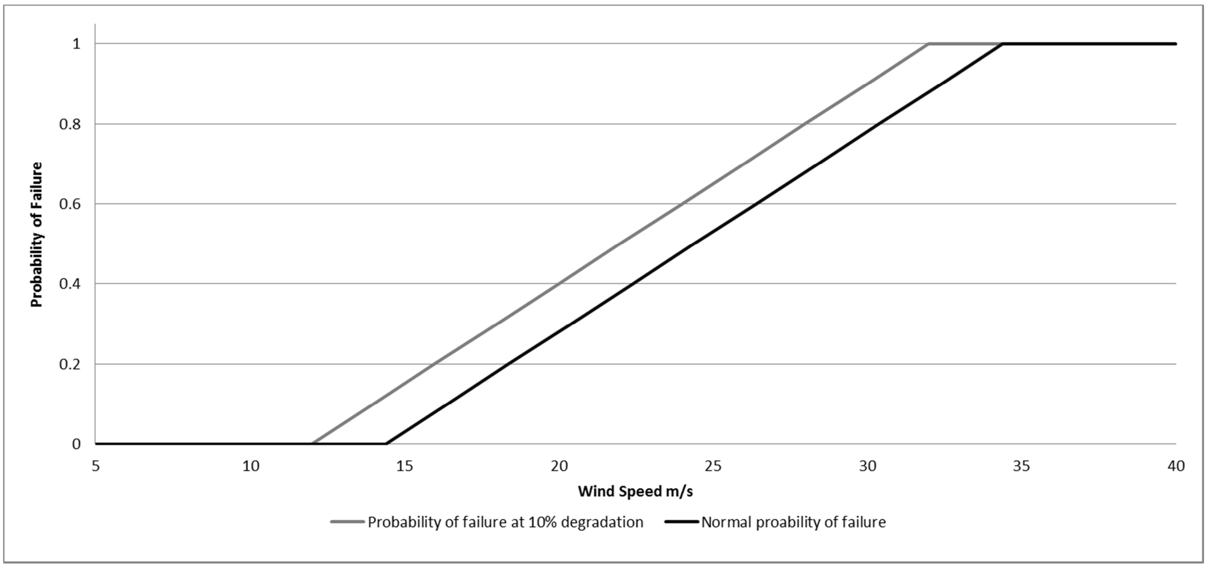

Figure 5 – Probability of failure comparison showing the normal curve and the deteriorated curves

System level deterioration is determined through simulations such as those previously presented. It can be determined that the longer a component is left without a maintenance check and repairs if necessary, the more likely it is that the component in question would have an increased vulnerability; leading to a potential reduction in system reliability which could be quantified by ascribing costs to repair components and costs of system level disruption.

CONCLUDING REMARKS

This paper outlines a methodology for assessing resilience of infrastructure networks that is consistent with The Keeping the Country Running: Natural Hazards & Infrastructure document. It demonstrates the method by analysing three simple networks that have different levels of resistance, redundancy and response. In our first event the networks suffer a relatively small magnitude event that only causes minor damage to the Control, Redundant and Response Networks, and no damage to the Resistant Network. By the time all networks are repaired and the total costs are calculated it can be seen that the Resistant Network has the least cost associated with it (as it suffers no damage). Running the event again but this time with a greater magnitude and therefore greater intensities at the component level, more widespread damage occurs. Here the greater resilience of the Redundant Network allows all components to keep functioning (all be it at a reduced rate) and therefore end up incurring the lowest cost due to disruption, whereas failure of the individual components of the Control, Resistant and Response Networks result in a greater loss of service. Finally a high magnitude event results in total network outage and so the time to recover is the most important factor in reducing the cost due to losses, resulting in the Response Network having the greatest resilience even though it loses the ability to provide service the easiest.

Providing robustness (in the form of resistance) to individual components of a network may not always be the cheapest solution as a similar result can be obtained by increasing the redundancy of the network, as this provides an alternative route to supply services and therefore capacity may still be present when a link is severed. This has been shown by the networks presented, as the degraded performance ratio (relative number of link failures compared to the Control Network) decreases from the Resistant Network (0.7) to the Redundant Network (0.56) (Table 3) based on maintaining connections.

These examples could be considered as measures of reliability in the context in which the definition is written by the Cabinet office (although cost due to service disruption and repairs to components should be included). It has been determined that reliability is simply the combination of resistance for event magnitudes (load conditions) which are forecasted for in the design of the system under consideration, and redundancy for events which are beyond the scope of the design. In conclusion the components of infrastructure networks (for example electricity transmission towers) are designed with particular resistances. Whereas the failure of individual components is important, it is the provision of services that they enable that is the major design consideration. Maximising the resilience of this service to the widest range of hazards requires consideration of the resistance, robustness and reliability of the individual components as well as ensuring the network has sufficient redundancy so that the redistributed services can still reach the intended recipients.

For utility owners to adopt this methodology for real Infrastructure networks, development of fragility curves and recovery curves are required. Reliable forms of fragility curves are not presently available; however the RESNET project [6] is attempting to produce them for the UK electricity transmission network. Recovery curves may exist for relatively small disruptions, but these are not in a form that can be readily used in a risk assessment as they are usually the uncorrelated repair records of utility owners and in the case of large scale disruption are likely to be absent.

Reference

[1] UK Cabinet Office, *Keeping the Country Running: Natural Hazards and Infrastructure*. UK Cabinet Office, 2011.

[2] Bruneau, M., Chang, S.E., Eguchi, R.T., Lee, G.C., O’Rourke, T.D., Reinhorn, A.M., Shinozuka, M., Tierney, K., Wallace, W.A. and Winterfeldt, D. *A Framework to Quantitatively Assess and Enhance the Seismic Resilience of Communities,* Earthquake Spectra, Volume 19, No. 4, pages 733–752, Earthquake Engineering Research Institute, 2003.

[3] Zentner, I., Nadjarian, A., Humbert, N. and Viallet, E. *Numerical Calculation of Fragility Curves for Probabilistic Seismic Risk Assessment,* The 14th World Conference on Earthquake Engineering, 2008

[4] Applied Technology Council, *Seismic Performance Assesment of Buildings Volume 1 – Methodology, ATC-58-1 75% Draft*, Applied Technology Council, 2011.

[5] Ahmed, A., Arthur, C. and Edwards, M. *Collapse and pull – down analysis of high voltage electricity transmission towers subjected to cyclonic wind*. IOP Conference Series: Materials Science and Engineering **10**: 012004. 2010

[6] RESNET – Resilient Electricity Networks for Great Britain. 2012.
http://www.tyndall.manchester.ac.uk/projects/resnet/index.html