Civil Engineering Special Issue
Volume 165 Issue CE6

Infrastructure resilience for high-impact low-chance risks
Blockley, Agarwal and Godfrey

ice | **proceedings**

Proceedings of the Institution of Civil Engineers
Civil Engineering Special Issue 165 November 2012 Issue CE6
Pages XX–XX http://dx.doi.org/10.1680/cien.2012.165.6.13
Paper 1100046
Received 10/10/2011 Accepted 12/07/2012
Keywords: failures/infrastructure planning/risk & probability analysis

ICE Publishing: All rights reserved

ice Institution of Civil Engineers
publishing

Infrastructure resilience for high-impact low-chance risks

1 David Blockley PhD, DSc, FREng, FICE, FIStructE
Emeritus professor and senior research fellow, Queens School of Engineering, University of Bristol, UK

2 Jitendra Agarwal MTech, PhD
Senior lecturer, Queens School of Engineering, University of Bristol, UK

3 Patrick Godfrey DEng, FREng, FICE, FEI, FCGI
Professor and systems centre director, Queens School of Engineering, University of Bristol, UK



Infrastructure resilience is the ability of an infrastructure system to withstand or recover quickly from difficult conditions, which in turn requires a detailed understanding of vulnerability and risk. But while designing for foreseeable risks is a challenge, accounting for risks which are difficult or even impossible to foresee – such as those arising from complex interdependent processes – poses a far greater challenge. This paper argues that civil engineers need a way of addressing such low-chance but potentially high-impact risks if they are to deliver truly resilient infrastructure systems. They need to cultivate a wisdom to admit what they genuinely do not know, and to develop processes to manage emerging unforeseeable consequences. A generalised vulnerability theory that can be applied to any infrastructure system is described, together with an example of how it can be applied to an urban transport network.

1. Introduction

Physicists define 'resilience' as the ability of an elastic material to absorb energy. Ecologists define it as the ability of an ecosystem to return to its original state after being disturbed, while medics refer to an ability to recover readily from illness, stress, depression or adversity. Thus a general definition of resilience is an ability to withstand or recover quickly from difficult conditions (OUP, 1998), or to adjust easily to misfortune or change.

In the UK government's critical infrastructure resilience programme (Cabinet Office, 2010), resilience is defined as, 'the ability of a system or organisation to withstand and recover from adversity'. ISO Guide 73 (ISO, 2009) defines resilience as the adaptive capacity of an organisation in a complex and changing environment.

According to the UK government, a resilient system or organisation will be able to achieve its core objectives in the face of adversity through a combination of good design, protection, effective emergency response, business continuity planning and recovery arrangements (Cabinet Office, 2010). The omission of the word 'quickly' is unfortunate, as speed of response may sometimes be critical.

2. Resilient infrastructure

Civil engineers intuitively want to create resilient infrastructure, but until recently few have attempted to articulate what resilience entails. Debates have largely been expressed in terms of 'optimisation', 'sustainability', 'robustness', 'vulnerability', 'risk', 'disaster planning' and, more recently, 'complexity' (Elliott and Deasley, 2007). It is important therefore to clarify similarities and differences between these terms.

At its simplest level optimisation is about getting the best out of a system and sustainability is a capacity to endure. A solution that is optimal or highly tuned in one context may well be vulnerable in another.

Vulnerability is a key term which, although referred to a great deal in the literature, is often defined in an unhelpful way that confuses it with risk. In this paper it is defined, based on previous research (e.g. Agarwal *et al*., 2003), as susceptibility to damage or perturbation – especially where small damage or perturbation leads to disproportionate consequences. This is more revealing and helpful in practical usage and distinguishes it from risk much more clearly.

Whereas the terms optimisation, vulnerability and robustness are normally used to refer to whole structures, it is also important to

recognise them at localised levels and in existing standard design procedures. So, for example, an I-beam optimised only for simple bending becomes vulnerable to lateral torsional buckling. A generic sense of design for resilience requires work at all levels of detail.

Sustainability logically implies resilience. In logic the inference that A logically implies B is the case except when A is true and B is false. That means that logically it can be inferred that a system is not sustainable when it is not resilient. But if it is resilient, it may or may not be sustainable because there are other factors, such as environmental management and consumption of resources, that are needed for sustainability.

In other words, resilience is necessary but not sufficient for sustainability, but sustainability is sufficient for resilience. In logic a necessary condition is one that is required – a 'must have' – and a sufficient condition is one that is adequate on its own, that is its existence leads to the occurrence of something. For examples of the importance and direct use of these logical terms in engineering, see Blockley and Robertson (1983), Blockley and Henderson (1988) and Blockley and Godfrey (2000).

Vulnerability is sufficient for the occurrence of lack of robustness. Robustness is the property of being strong, healthy, hardy and able 'to take a knock'. A robust system is strongly or stoutly built – again with an implied sense of endurance. More generally robustness is the ability of a system to persist when subject to changes or perturbations and uncertain conditions.

Resilience must therefore entail or imply robustness and hence robustness is necessary but not sufficient for resilience, since the latter also includes recovery to an original state or to a state which continues to meet an acceptable level of the original purpose of the system. Vulnerability is especially critical in dealing with high-impact, low-chance risks. A system is not robust if it is vulnerable. Optimising a system without proper attention to robustness can lead to vulnerabilities through unrecognised and hence unexpected modes of behaviour.

In the simple example used above, when designers of I-beams routinely consider all known limit states – including simple bending, lateral torsional buckling and deflections – they are creating greater robustness. Optimisation, resilience, robustness and vulnerability must be clearly distinguished from risk – risk is in the future – it is the chance of an event that may cause harm and the consequences that follow.

The UK Health and Safety Executive (HSE,1992) recognises there is no such thing as zero risk – no matter how remote a risk might be, it could just turn up. Risks have to be managed to a tolerable level. This means they should not be regarded as negligible or something that might be ignored, but rather as something that needs to be kept under review and reduced still further if possible.

The British Tunnelling Society (2003), however, seems to conflate risk and robustness by defining the fundamental objective of the design process as that of achieving a robust design. It continues by stating that a robust design is one where the risk of failure or damage to the tunnel works or to a third party from all reasonably foreseeable causes, including health and safety considerations, is extremely remote during the construction and design life of the tunnel works. However, it does say that high-consequence but low-frequency events that could affect the works or a third party shall also be considered.

In summary, vulnerability entails a lack of robustness. Robustness is necessary but not sufficient for resilience, and resilience in turn is necessary but not sufficient for sustainability. The logic is illustrated in Figure 1, which shows that the state of being sustainable and not being robust is not allowed. Similarly the state of being sustainable and not being resilient is not allowed, as is being resilient and not robust. All are handled systemically by managing risks, a well-known example of which is the observational method in geotechnics (Le Masurier *et al*., 2006).

As a contribution to civil engineers' attempts to secure resilience in modern complex infrastructure systems, the purposes of this paper are to

- argue that in complex systems, civil engineers need to cultivate the wisdom to admit to knowing what they genuinely do not know
- show that civil engineers need consciously to design processes with sufficient resilience to manage unexpected consequences
- outline briefly a generalisation of structural vulnerability theory which can be applied to any infrastructure system.

Quotexxx

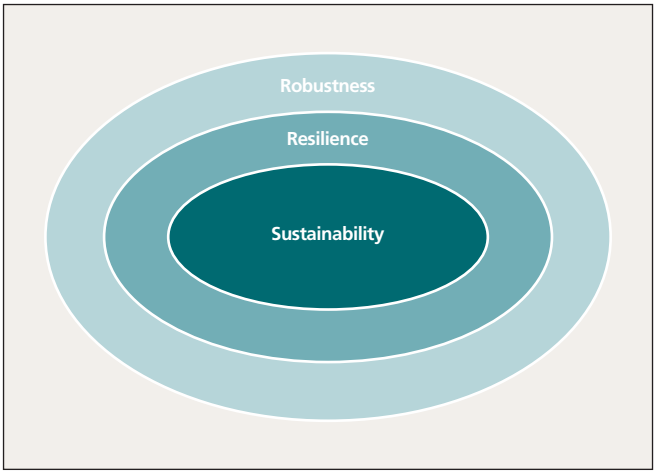

Figure 1. Sustainability implies resilience implies robustness

3. Complex systems

Complex behaviour (Elliott and Deasley, 2007) can emerge from interactions between many simpler, highly interconnected processes. There is a growing recognition of new risks through interdependencies that may not be fully understood.

For example, it is known that some (but not all) physical processes are chaotic in the sense that, while they may appear to be reasonably simple, they are inherently difficult to predict. It has been discovered that they may be very sensitive to very small differences in initial conditions and may contain points of instability where paths diverge. This is seen even in quite simple systems, like a double pendulum, as well as bigger and more complex systems like weather forecasting. This is a new kind of uncertainty that presents a new kind of risk.

Highly interconnected systems, such as electrical power supply networks, the internet, traffic highways and building structures can become vulnerable to quite small damage, cascading to disproportionately large consequences that extend beyond the boundaries of envisaged systems. Even if the chance of the initial damage is very low, the consequences can be very severe. Such systems lack resilience or robustness.

Civil engineers have to recognise that they cannot predict the total behaviour of a complex infrastructure system from the performance of its interdependent parts – they have to expect the unexpected with unintended consequences. An ongoing example is currently occurring in Christchurch, New Zealand where some of the repairs from the earthquake in early 2011 are on hold because people cannot get insurance for new building, unless they are shifting from a damaged house where they were existing customers for an insurance company. Contractors are finding it difficult to insure buildings as they are building them; this is an unexpected and unintended outcome (D. Elms, personal communication, 2011).

4. Resilience engineering

Resilience engineering is a term proposed by Hollnagel *et al.* (2006) to capture a way of thinking about safety which enhances the ability at all levels of organisations to be robust yet flexible, and to use resources proactively to manage processes to success. They argue that too many people have regarded safety as something a system has (a property) rather than something a system does (a performance).

Resilience engineering therefore abandons the search for safety as a property – such as adherence to standards, calculations of reliability, event trees and counts of human error – and instead sees resilience as a form of control. In other words the system properties are necessary but not sufficient for safety.

The approach is entirely consistent with methods based on systems thinking proposed by Blockley and Godfrey (2000) as a way of 'rethinking construction' after the Egan Report, and with work on human and social factors in man-made disasters by Turner and Pidgeon (1998). By this thinking resilience is an outcome of a process that emerges from the interactions between its sub-processes. So, just as linear elastic strain energy is an outcome, expressed as a property of a material that emerges from the interactions between its molecules, so the resilience of an infrastructure project emerges from the interactions between its well-engineered sub-processes.

A central aspect of vulnerability – and hence robustness, resilience and sustainability – of technical and socio-technical systems is how to ensure that 'surprises' are managed, especially those that have high impact but are of low chance or probability. Incompleteness in risks can be divided into those that are knowable and foreseeable – 'known knowns' – and those which are difficult or even impossible to know and foresee – 'known unknowns' and 'unknown unknowns' (Blockley, 2009).

The focus is on clearly identifying, characterising and managing complex interdependent processes to success by explicitly tracking and managing risk and uncertainty. It is important to stress that these processes are not rigid, inflexible procedures, as implemented in some quality assurance systems. Rather the intention is to create a process model, accessible by an intranet to all involved, which facilitates a rigorous clarity, adaptability and resilience on

- what is being done and on what timescale, particularly for contingency planning
- who is responsible and how are they accountable
- what success means and how it can be reached

together with a constant monitoring of progress to manage unforeseen unintended outcomes.

Infrastructure systems such as transport, energy, waste, water supply, flood control and information contain complex interdependencies. Experts are naturally and understandably reluctant to consider risks that fall outside the range of their professional scope and expertise. Hence, especially in a commercial context, they can be reluctant to admit when they are operating outside their comfort zone. This can lead to situations where experts reject potential evidence simply because it falls outside their current understanding.

The reason why teams are so important is that they can bring a wider range of skills and expertise than can individuals. But even good teams may be unwilling to give credence to complex and very improbable risks. If a situation is considered too complicated then there is a danger that organisations may not react at all. Civil engineers need to cultivate the wisdom to admit to what they genuinely do not know (Government Office for Science, 2012) so that they can then devise processes that monitor performance with contingency plans to make systems resilient and sustainable, even when subject to unforeseen and unintended demands.

5. Avoiding surprises

As stated earlier, one measure of unintended consequences is the number of 'surprises' experienced, particularly surprises that arise from a lack of knowledge or the inability to perceive the consequences of what is known.

In any situation where civil engineers may admit they genuinely do not know something, then they must have robust methods for managing that situation. So, for example, they will need to create processes that develop and consider possible scenarios that have potentially serious consequences, even if they are very unlikely to happen.

Processes are needed to consider how to ensure systems are not brittle, and degrade in a way that, at the very least, allows some control of the safety of people. Processes are also needed that build awareness among users of infrastructure systems and in particular for contingency and disaster planning.

In short, a resilient organisation should expect unintended emergent behaviour for novel complex systems and design the

systems accordingly (Elliot and Deasley, 2007). It is not the purpose of this paper to identify all of these kinds of processes, since that process is itself considerable, but Figure 2 provides an outline overview of the processes for repair and recovery.

Grundy (2011) has outlined six useful steps to disaster risk reduction.

- Know the hazards and risks.
- Identify weaknesses.
- Retrofit for resilience against all hazards.
- Plan emergency response procedures.
- Educate the community to understand and implement the procedures.
- Rehearse emergency responses regularly.

These processes are clearly particularly important in seismic zones. For example, retrofitting for resilience must consider checking not only for robust form but also for robust management processes that sense and adapt to respond to threats.

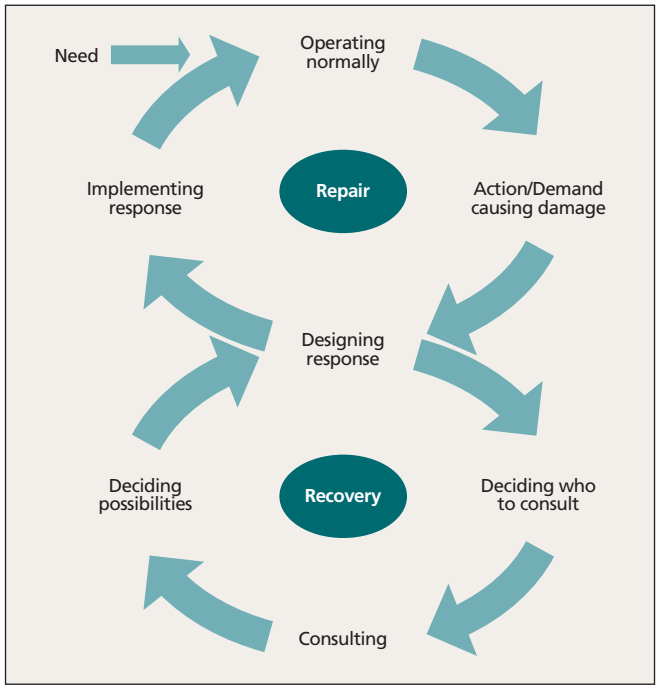

Figure 2. Outline design processes for repair and recovery

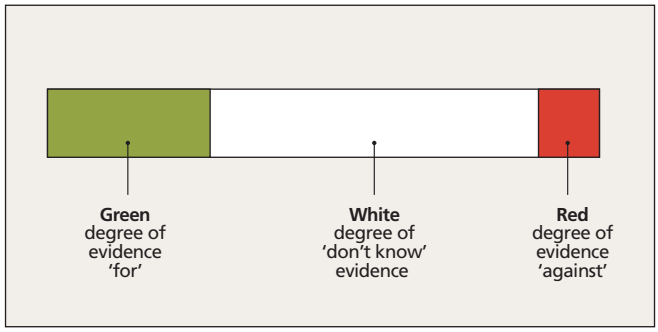

Figure 3. Italian flag – evidence of dependability for a purpose

'Italian flags' (Figure 3, Blockley and Godfrey (2000)) have been proposed and used to elicit degrees of evidence and to control processes in which evidence is significantly incomplete. Note that the flag is not to be confused with a traffic light – it is a representation of a logical theory of interval probability that includes levels of incompleteness. The green part of the flag indicates the level of positive evidential support for the dependability of a proposition, the red part indicates the level of negative evidential support against the dependability of a proposition and the white part indicates the lack of evidential support for or against the dependability of a proposition, that is the level of incompleteness or 'do not know'.

Italian flags can be used entirely informally or formally to support decision making at various levels in a process hierarchy, as in Figures 4 and 5, where significant differences of understanding are illustrated. In Figure 5 the dam owner has not appreciated the incompleteness of the geotechnical engineer's interpretation of the evidence available or the real worries of the operator. The flags are one way in which these different perspectives are highlighted so that they may be communicated and addressed.

6. Cascading failure – a systems approach to vulnerability

Low-chance risks with extremely high consequences are a particularly difficult source of surprises. Eurocode 1, part 1-7 (BSI, 2008) recognises the need to assess actions arising from accidental human activity, including impact and collisions from wheeled vehicles, ships, derailed trains and helicopters on roofs, as well as gas explosions in buildings.

For nuclear power stations, the UK Health and Safety Executive (HSE,1992) calls for robustness through redundancy and back-up by way of independent components or design diversity, especially in software. It requires a rule of conservatism that pays attention to the quality of a nuclear plant, including management systems, and operational procedures. HSE (2001) also calls for the use of the precautionary principle so that where there are threats of serious or irreversible environmental damage, lack of full scientific certainty shall not be used as a reason for postponing cost-effective measures to prevent degradation. This rules out lack of scientific certainty as a reason for not taking preventive action.

Despite such initiatives, the potential for cascading failures from small damage resulting in disproportionate consequences is not well understood. Assumptions of independence that are often made where data are sparse may be seriously misleading. Damage may come from unknown sources and any inherent weaknesses in the form of the system need to be explored at the design stage.

Vulnerability theory (Agarwal *et al*, 2003; England *et al*, 2008) is a systems approach to the problem which has been applied to structures and is now being generalised to apply to all engineering systems. There is space here only to present an outline of the theory, in which the form of a system is organised into layers of clusters in a hierarchical process model. The model is then examined for weak points to identify vulnerable scenarios on which risk calculations are based.

Vulnerability may arise because the form of the system has certain characteristics. Form and function are closely related in that an appropriate form is required to achieve a particular function. If the form is damaged then the function will also be

affected. Disproportionate consequences derive from a form that is inappropriate because it 'unzips' or cascades when subjected to one or more specific demands, which may not have been anticipated, in an unacceptable way. Hence vulnerability is examined by concentrating on the way in which the form of a system is affected by any arbitrary damage. Then the results can be combined with the analysis of response to different specific demands.

A system is considered as a set of interacting process objects defined in layers and arranged and connected together in an appropriate form for the purposes of that system (Blockley, 2010; Blockley and Godfrey, 2000; Woodcock and Godfrey, 2010). The process objects interact with each other in order to deliver success or to fulfil a role in a higher level process. They may themselves result from lower level processes. The nature of objects may differ substantially from one system to another. For example, beams and columns are process objects in a structure and pipes and valves are process objects in a water supply network.

Such systems can be represented as a graph model using nodes and links. The links are the channels of communication between nodes. In most systems there is one channel per link, for example electrical current or the flow of a fluid such as water. However, there can be more channels along a link, for example up to six degrees of freedom in a structure. Associated with each link is a parameter describing a quality of the form of the link. This parameter depends upon various components in a system and their relationships, for example in mechanical and electrical systems – see Shearer *et al*. (1967).

Relationships are expressed in terms of across- and through-variables. The across-variables balance around the circuit and the through-variables balance across any section through the circuit. Table 1 summarises some of the variables for different systems including structures, water supply and traffic networks.

Vulnerability analysis provides a measure of the relative size of the consequences of damage to the effort of producing that damage no matter the chance of it happening – a vulnerability index. The assessment of likelihood of a failure scenario combined with the

Quotexxx

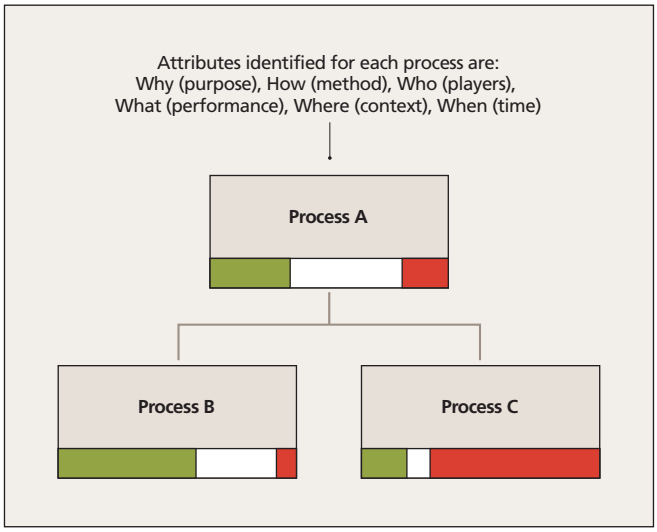

Figure 4. Italian flag for some simple processes – evidence for process C indicates it is very likely to fail, while the owner of process A believes it will succeed. If A is dependent on C, the two process owners need to sort out the reasons for their differing perceptions

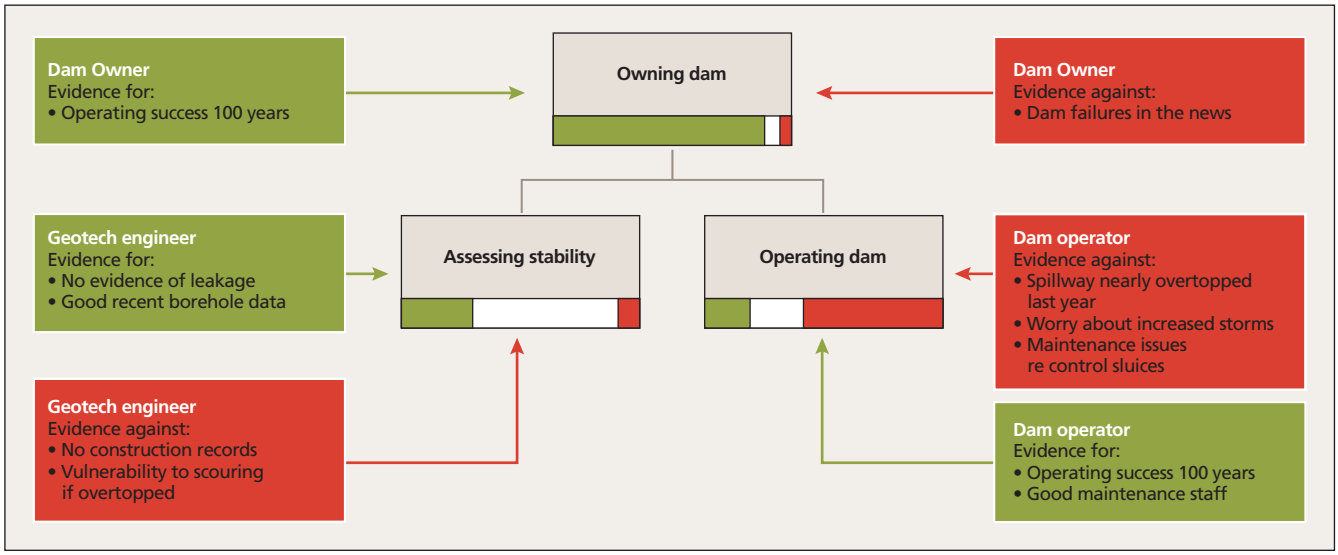

Figure 5. Italian flags showing conflicting evidence for the safety of a dam – they can stimulate identification of known unknowns through dialogue

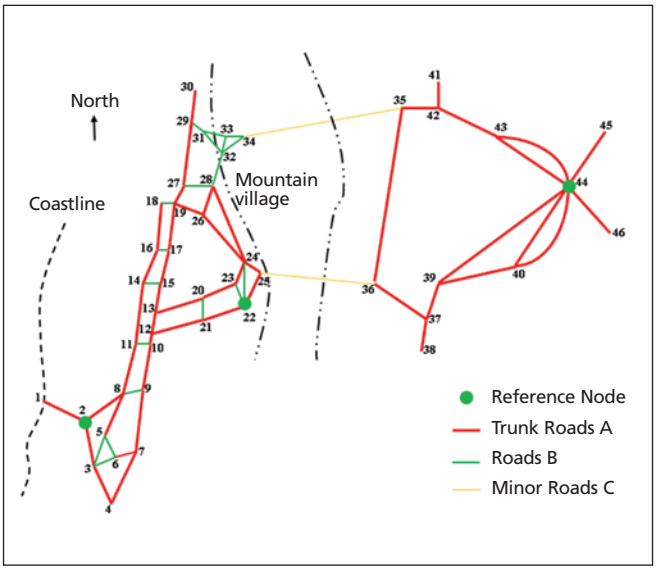

Figure 6. An example of a transport network in a coastal city

vulnerability index gives a measure of risk to the form of the system. Clearly, this risk may be part of a wider risk assessment and managed within that wider system.

7. Application to a transport network

A road network is vulnerable if a failure in one or more links causes 'knock-on' disproportionate delays to journey times. As indicated earlier, traffic potential – that is the need to travel – drives flows of traffic along links with known transmittance in a directed graph (Figure 6). A vulnerability analysis has to relate to delays between chosen reference nodes, for example population centres 2, 22 and 44 in Figure 6.

Transmittance depends on capacity speed, length and orientation (Liu *et al*., 2012) and is used to calculate a property of a cluster of nodes and links called 'well-formedness' (Agarwal *et al*., 2003). Well-formedness is a measure of the quality of interconnected loops of nodes within any chosen cluster so that the higher the number of connected nodes with higher transmittance links, the higher the well-formedness.

Attribute	Electrical circuits	Structures	Traffic	Water pipes	Organisations
Across variable (potential)	Voltage, V	Velocity, x	Need, v	Pressure difference, h	Driver of need and purpose
Through variable (flow)	Current, I	Force, F	Flow, f	Flow, Q	Flow of change
Dissipative component, R	Resistance $V = RI$	Damping $F = cx$	Resistance to movement	Resistance to flow	Dissipation of energy/conflict
Across storage component, C (accumulation)	Capacitance $I = C\frac{dV}{dt}$	Mass (inertia) $F = mx$	Parking	Internal reservoir	Message passing time/inertia
Through storage component, L (delay)	Inductance $V = L\frac{dI}{dt}$	Flexibility (inverse of stiffness) $F = kx$	Length of link	Length of link	Response time/delay
Weighting parameter describing form of a link, w	Impedance	Stiffness	Transmittance (ease of flow)	Transmittance (ease of flow)	Impedance

Table 1. Parameters governing the form of different systems (e.g. see Shearer et al. (1967))

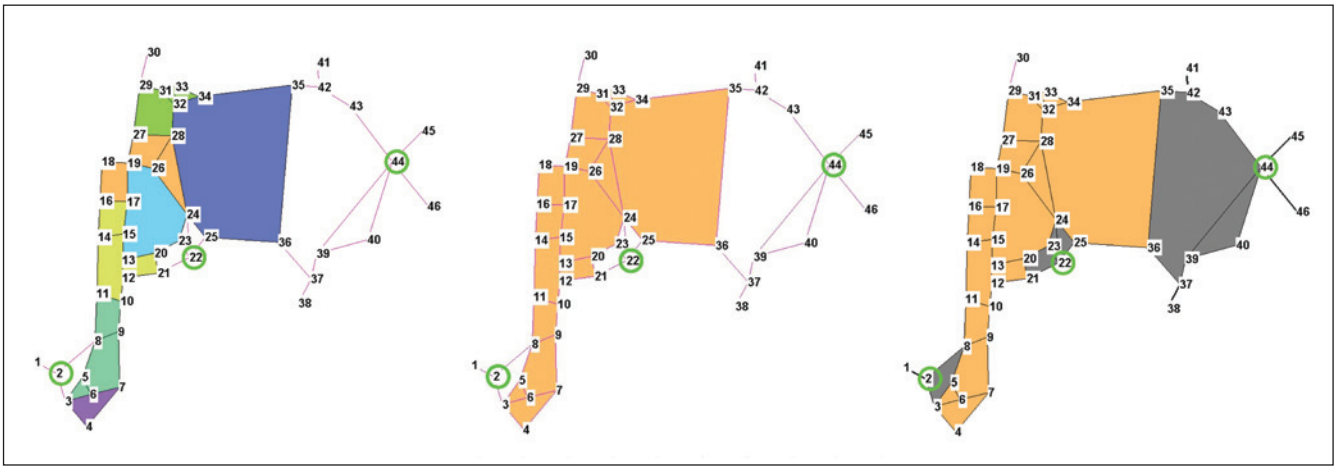

Figure 7. A clustering sequence of the results from a vulnerability analysis of transport delays between population centres 2, 22 and 44 in Figure 6

Well-formedness is effectively an indicator of robust form through the number of good-capacity alternative routes for traffic to flow. For simplicity the network of Figure 6 has only three categories of transmittance – A, B and C roads. The hierarchical layers of the systems are created by a clustering process. This starts from the seed loop not linked directly to a reference node and having the highest well-formedness. This seed is grown into a bigger cluster by attaching neighbouring loops if the well-formedness increases. When there is no increase in the well-formedness, a new cluster is seeded.

When all seeds are grown and well-formedness cannot increase further (Figure 7(a)) then the clusters are themselves clustered into one single cluster (Figure 7(b)). Finally the links to the reference clusters are clustered (Figure 7(c)). The process produces a natural hierarchy of interconnected clusters. This hierarchy is then systematically searched for various damage scenarios that separate well-formed clusters at all levels in the hierarchy.

For example and simply for the purposes of illustration, it is straightforward to see in Figure 7 that if links 25–36 and 34–35 are cut then reference node 44 is completely separated from the others. Likewise by cutting links 8–11 and 9–10 then reference node 2 is completely separated. There are other less obvious scenarios which can be prioritised and used when deciding maintenance strategies for the network.

8. Conclusions

Complex infrastructure systems may contain new risks through interdependencies that may not be fully understood. Civil engineers have to recognise that they cannot predict the total behaviour of a complex system from the performance of its interdependent parts – they have to expect and devise ways of dealing with unexpected and unintended consequences.

Resilience is considered as the ability of a system to withstand or recover quickly from difficult conditions. It is not a simple property like a safety factor or probability of failure; rather it emerges from the interactions between sub-processes. A system is vulnerable if it is susceptible to damage or perturbation, especially where small damage or perturbation leads or cascades to disproportionate consequences.

Vulnerability is sufficient for a lack of robustness. However, robustness is necessary but not sufficient for resilience and resilience in turn is necessary but not sufficient for sustainability. All are handled by systemically managing risks.

Resilience engineering has been used previously to capture a new way of thinking which does not regard safety as something a system has (a property) rather than something a system does (a performance). The approach is entirely consistent with methods based on systems thinking previously proposed by the authors.

One measure of unintended consequences is the number of 'surprises' experienced. Optimising a particular property of an infrastructure system can increase its vulnerability and reduce its resilience. Vulnerability theory is a systems approach to this problem which has been applied to structures and is now being generalised to apply to all engineering systems.

References

Agarwal J, Blockley DI and Woodman NJ (2003) Vulnerability of structural systems. *Structural Safety* **25(?)**: 263–286. <AQ2>

Blockley DI (2009) Uncertainty – prediction or control? *International Journal of Engineering Under Uncertainty: Hazards, Assessment and Mitigation* **1(?)**: 1–2. <AQ3>

Blockley DI (2010) The importance of being process. *Journal of Civil Engineering and Environmental Systems* **27(3)**: 189–199.

Blockley DI and Godfrey PS (2000) *Doing it Differently.* Thomas Telford, London, UK.

Blockley DI and Henderson JR (1988) Knowledge base for risk and cost benefit analysis of limestone mines in the West Midlands. *Proceedings of the Institution of Civil Engineers, Part 1* **84**, June: 539–564.

Blockley DI and Robertson CI (1983) An analysis of the characteristics of a good civil engineer. *Proceedings of the Institution of Civil Engineers, Part 2* **75**, March: 77–94.

British Tunnelling Society (2003) *The Joint Code of Practice for Risk Management of Tunnel Works in the UK*. Institution of Civil Engineers, London, UK, see http://www.britishtunnelling.org.uk/downloads/jcop.pdf (accessed 02/03/2012).

BSI (2008) BS EN 1991-1-7:2008: Eurocode 1: General actions – accidental actions. BSI, London, UK.

Cabinet Office (2010) *Sector Resilience Plan for Critical Infrastructure.* Cabinet Office, London, UK, Crown copyright, see http://www.cabinetoffice.gov.uk/sites/default/files/resources/sector-resilience-plan.pdf (accessed 18/03/2012).

Elliott C and Deasley P (eds) (2007) *Creating Systems that Work: Principles of Engineering Systems for 21st Century*. Royal Academy of Engineering, London, UK, Report, see http://www.raeng.org.uk/education/vps/pdf/RAE_Systems_Report.pdf (accessed 18/03/2012).

England J, Agarwal J and Blockley DI (2008) The vulnerability of structures to unforeseen events. *Computers and Structures* **86(?)**: 1042–1051. <AQ4>

Government Office for Science (2012) *Blackett Review of High Impact Low Probability Risks*. Government Office for Science, London, UK, Crown copyright, see http://www.bis.gov.uk/assets/bispartners/goscience/docs/b/12-519-blackett-review-high-impact-low-probability-risks (accessed 11/03/2012).

Grundy P (2011) *Disaster Risk Reduction: The Engineer's Role*. IEAust, Engineers Australia, Barton, ACT, Australia. <AQ5>

Hollnagel E, Woods D and Leveson N (2006) *Resilience Engineering*. Ashgate Publishing, UK.

HSE (Health and Safety Executive) (1992) *The Tolerability of Risk from Nuclear Power Stations.* Health and Safety Division, HMSO, London, UK, see http://www.hse.gov.uk/nuclear/tolerability.pdf and http://www.hse.gov.uk/nuclear/keythemes.htm (accessed 02/03/2012).

HSE (2001) *Reducing Risks, Protecting People.* Health and Safety Division, HMSO, London, UK, see http://www.hse.gov.uk/risk/theory/r2p2.pdf (accessed 02/03/2012).

ISO (2009) *Risk Management – Vocabulary*, 1st edn. BSI, London, UK, Guide 73:2009.

Le Masurier J, Blockley DI and Muir Wood D (2006) An observational model for managing risk. *Proceedings of the Institution of Civil Engineers – Civil Engineering* **159(?)**: 35–40. <AQ6>

Liu M, Agarwal J & Blockley DI (2012) *Vulnerability Analysis of Highway Networks* (in preparation). <AQ7>

OUP (Oxford University Press) (1998) *New Oxford Dictionary of English.* OUP, Oxford, UK.<AQ8>

Shearer JL, Murphy AT and Richardson HH (1967) *Introduction to System Dynamics*. Addison-Wesley. <AQ9>

Turner BA and Pidgeon NF (1998) *Man Made Disasters*, 2nd edn. Butterworth-Heinemann, Oxford, UK.

Woodcock H and Godfrey PS (2010) *What is Systems Thinking?* International Council on Systems Engineering (INCOSE), Somerset, UK, INCOSE Z Guide 7, see http://www.incoseonline.org.uk/Documents/zGuides/Z7_Systems_Thinking_WEB.pdf (accessed 02/03/2012).

What do you think?

If you would like to comment on this paper, please email up to 200 words to the editor at journals@ice.org.uk.

If you would like to write a paper of 2000 to 3500 words about your own experience in this or any related area of civil engineering, the editor will be happy to provide any help or advice you need.