ISBN 978-1-84919-696-3
2013

The Institution of Engineering and Technology

Infrastructure Risk and Resilience: **Transportation**

INSIDE THIS SPECIAL INTEREST PUBLICATION Selected papers highlighting the current thinking regarding the resilience of Transport Networks, including the assessment of criticality, vulnerability, risk and the identification of measures to reduce the likelihood or consequences of man-made and natural events.

Published by the Institution of **Engineering and Technology**

www.**theiet**.org/infrastructure

The Institution of Engineering and Technology

IET Advantage. For the career you **really want.**

IET Advantage is a three step membership programme which offers exceptional value to early career engineers who are determined to achieve more.

As your career develops, it's reassuring to know that your IET membership will keep pace with your changing needs. IET Advantage delivers the depth of knowledge, expert support and professional tools you need to achieve your career ambitions.

Graduate Advantage is all about easing your transition from graduation to employment. Building essential knowledge, providing study tips, CV advice and job searching.

Career Advantage concentrates on your knowledge and experience. Providing you with the tools to establish yourself in your career and build the essential skills of a professional.

Professional Advantage focuses on achievement. Preparing you for professional registration as an Incorporated or Chartered Engineer (IEng/CEng).

Welcome to your Professional Home for Life®

IET **Advantage**

www.**theiet**.org/advantage

Contents

About the Transport Knowledge Transfer Network, the Register of Security Engineers and Specialists, the Institute of Risk Management and the Institution of Engineering and Technology 2

Transport Infrastructure Risk and Resilience
Introduction and Forewords 4

Infrastructure risk and resilience: a review James Peter Kimmance and Anthony John Harris 8

Europeanising Transport Security: Policy and research recommendations for improving transport infrastructure security in Europe Jakob Haardt and Samuel Rothenpieler 17

Introduction to network theory and game theory as frameworks for the analysis of critical infrastructure Urszula Kanturska and Dr Panagiotis Angeloudis 22

Synchronisation in changing response situations: a high-level exploration of the management of resources during crisis Christopher John Cullis 29

Understanding the impacts of multiple stakeholders on the future security of main English railway stations Lucy Gregson-Green, Andrew Dainty and Lee Bosher 34

Surviving catastrophic events: stimulating community resilience Alexander H. Hay 41

A new approach to risk reduction in the railway industry Eberechi Weli and Michael Todinov 47

Black Swans means business Atula Abeysekera 53

Understanding how tunnel ventilation analysis decreases risk and increases resilience Kate Hunt and Chermac Rolle 59

Do we have the skills and knowledge to adapt transport infrastructure to climate change risks? James Dunham, Andrew Heather, Kristina Kueng and David Viner 65

We would like to thank the following groups for their involvement in this publication:
- Risk Mechanics Ltd
- Transport Knowledge Transfer Network
- The Register of Security Engineers and Specialists
- The Institute of Risk Management
- Parsons Brinckerhoff Ltd
- Atkins Highways and Transportation
- PTV Transport Consult GmbH
- CPNI
- Built Environment Sector Committee
- Transport Sector Committee

We would also like to thank the Editorial Panel for their review of papers in this publication:
- James P. Kimmance, Director - *Risk Mechanics Ltd*
- Neil Ridley, BEng, CEng, MIMechE, Director - *Transport Knowledge Transfer Network*
- The Registrar, *The Register of Security Engineers and Specialists*
- Carolyn Williams, MA ACII MIRM, Head of Thought Leadership - *The Institute of Risk Management*
- Eur Ing Matthew Clarke, BEng CEng MIET MCMI, Head of Tolling, Technology and Lighting Design - *Atkins Highways and Transportation*
- Dr.-Ing. Georg Mayer, Head of Department Tunnel Equipment and Operation - *PTV Transport Consult GmbH*
- Oliver Hoare, Director - *Dysart Solutions Ltd &* Special Adviser - *Foreign and Commonwealth Office Services*
- Hugh Boyes, Technical Lead, Cyber Security - *The IET*
- Bruce McLelland, Built Environment Sector Head - *The IET*
- Michelle Sawyer, Sectors Project Co-ordinator - *The IET*

Catalysing innovation across transport to move people and goods more efficiently

The Transport Knowledge Transfer Network is supporting the development of integrated, efficient and sustainable transport systems, by bringing together independent but interrelated organisations to stimulate innovation through knowledge transfer.

Road, rail and marine sectors share common challenges where technology and expertise can be shared and developed in collaboration, across the many stakeholders. We raise awareness of these common challenges and bring together organisations to develop products and services that address these, both nationally and internationally.

We achieve this through:

- acting as a catalyst to bring organisations together around specific issues.
- deepening and broadening of cross-sector knowledge through the impartial dissemination of challenges, experience, ideas and best practice.
- drawing in solution providers from adjacent industries including electronics, sensors, ICT, aviation, etc.
- supporting industry strategies with activities including road mapping, best practice exchange and research.

Visit www.transportktn.org or email enquiries@transportktn.org for more information. Membership is Free.

RSES
Register of Security Engineers & Specialists

The Register of Security Engineers and Specialists (RSES) has been established to promote excellence in security engineering by providing a benchmark of professional quality against which its members have been independently assessed. Security engineering is defined as "the protection of the health of the population, the built environment and infrastructure against terrorism, sabotage and crime by the application of engineering and scientific principles".

The Register is open to engineers, applied scientists, health professionals and specialists who apply their knowledge to securing the built environment and infrastructure. Admittance to the Register provides the public, insurers and potential clients the assurance that the registrant has:

- achieved a recognised competence standard through a professional review process;
- accepted a code of ethics and has a commitment to Continuing Professional Development (CPD), with an emphasis on security engineering.

The RSES is sponsored by the Centre for the Protection of National Infrastructure (CPNI) and is administered and operated by the Institution of Civil Engineers (ICE). For more information visit www.rses.org.uk or www.ice.org.uk/rses.

The Institute of Risk Management (IRM) is the world's leading enterprise-wide risk management education Institute. We are independent, well-respected advocates of the risk profession, owned by practising risk professionals. IRM passionately believes in the importance of risk management and that investment in education and continuing professional development leads to more effective risk management. We provide qualifications, short courses and events at a range of levels from introductory to board level. IRM supports risk professionals by providing the skills and tools needed to put theory into practice in order to deal with the demands of a constantly changing, sophisticated and challenging business environment. We operate internationally with over 4000 members and students in more than 100 countries, drawn from a variety of risk-related disciplines and a wide range of industries in the private, third and public sectors.

The IET has recognised that the demands on the modern engineering community have changed. By prioritising five Sectors; Transport, Information and Communications, Energy, Design and Production and Built Environment, the IET has provided an access point to the multi-disciplinary knowledge, experience and content available to members and the global science, engineering and technology communities.

Both the IET Built Environment Sector and the IET Transport Sector have played pivotal roles in the delivery of this Special Interest Publication. Both Sectors aspire to be the principal point of reference for engineers and technicians on a global scale. They also recognise the importance of promoting professional qualifications and accreditation in this field.

The Sector aims are:-

- to identify emerging and key topics and activities to ensure the IET deploys its expertise for maximum impact
- deliver knowledge dissemination through collaborations and partnership with aligned industry bodies and organisations
- produce technical briefings, policy statements, codes of practice, thought leadership documents and reports
- be agile and respond to announcements rapidly to provide an informed view to practitioners, academics and the public
- work at both local and global levels with all stakeholders and industry to discuss issues and encourage best practice and innovation
- to provide up-to-date news and information for professionals and other stakeholders
- to publicise and represent the information and communication engineering profession to a wider audience

For more information, visit www.theiet.org/sectors

ISSN 2041-5923

Transport Infrastructure Risk and Resilience

Introduction and Forewords

Bruce McLelland - IET Built Environment Sector Head, The Institution of Engineering and Technology

In an increasingly integrated transport environment, failure or loss of individual components can have a significant impact on the operation of the overall network. There is an increasing reliance on a dependable and robust transport network, supporting extended supply chains, just in time delivery of high value and perishable items, gas imports and commuters to our cities. Over half the world's population now live in these cities where a functioning, integrated transport system are essential.

These systems are under constant threat from a variety of areas. As these systems integrate, there is now a real risk that a system failure will have a disproportionate impact in the system of systems. The threats are identifiable broadly as natural or environmental threats like volcanic ash on aviation, high power winds like tornadoes, tidal surges resulting flooded transport hubs and malicious attack with intent to disrupt modern transport systems.

The IET remains firmly interested in the engineering techniques and approaches to the protection of assets in terms of reliable systems design, identification of failure modes and single points of failure. Furthermore, the processes for combating malicious attack and reducing impact of human/operator error and the methodology for assessing environmental impact on assets. This publication, which is intended to be the start of a series of publications looking at the protection of a number of infrastructure categories, goes some way into looking at how these threats are being studied in the transport sector.

For more information visit www.theiet.org/infrastructure

Carolyn Williams - Head of Thought Leadrship, The Institute of Risk Management

The Institute of Risk Management (IRM) is delighted to have been given the opportunity to work with IET on the publication of this timely document on Transportation and Infrastructure Risk and Resilience.

Infrastructure and transport construction is a hugely important driver of economic development and employment: the efficient and effective delivery of bridges, tunnels, railway lines, ports, airports and other infrastructure is essential to support the supply chains and activity underpinning modern economies. Yet these are hugely complex projects displaying the full range of risks, from financial to behavioural to political to strategic and operational. There is a lot that could go wrong – but also big benefits to be gained when things go right. Managing risk effectively means that more things go right, more of the time.

We cannot always predict the future, particularly the 'black swan' events which by definition cannot be imagined until they actually materialise in front of you. Our defence against the unexpected, however, is resilience – we need strong, resilient infrastructure networks to maintain performance in the face of threats, whether these are natural hazards or manmade threats

like terrorism. The papers in this publication look at some of the ways that we are coming to understand more about resilience and how it can be achieved.

As an educational and professional institute we also would argue for the key role of the professions in producing qualified and experienced people who will communicate with each other in driving the resilience agenda forward. The project to produce this document has brought together professionals and academics from various disciplines to learn from each other and contribute towards the knowledge resources available for all. IRM and its members have been very pleased to take part.

For more information, visit www.theirm.org.uk

Neil Ridley – CEO, Transport Knowledge Transfer Network

The Transport Knowledge Transfer Network (Transport KTN) is delighted to have supported this special interest publication.

Our transport systems must be able to respond to the global forces of population growth, urbanisation, energy consumption and environmental sustainability. These forces are putting ever more pressure on the transport system and infrastructure, which must meet the growing demands and the need for 24/7 operation. To help address these issues the Transport KTN is catalysing innovation to develop integrated, efficient and sustainable transport by bringing together independent, but interrelated organisations to share knowledge and develop world's leading solutions.

The solutions to our transport needs are multiple and involve an ever-growing number of stakeholders as new technologies and business models develop. These introduce not only new opportunities, but also complexities that require careful assessment and management to ensure unintended consequences are minimised. Risk and resilience capabilities, tools and techniques are a key input to this to ensure robust, yet flexible systems where disruption is minimised and localised. This special interest publication identifies a number of applications that have global opportunities, which in turn will bring significant benefits to the UK economy through development and application of UK-based talent.

For more information visit www.transportktn.org

Register of Security Engineers and Specialists

Whatever the type of transport network, recent natural and manmade events worldwide have demonstrated the importance of considering the risk and resilience associated with the network, to ensure its continued operation. Be it severe flooding, volcanic ash, criminal acts such as cable theft, cyber-attacks on control systems or acts of terrorism, the ability of the transport infrastructure to function under such conditions will depend upon the amount of attention the operating organisations have paid to identifying the network's vulnerabilities and dependencies, and the measures it has in place to mitigate against the effects of such events. Mitigation actions may include design, crisis response and recovery issues and will undoubtedly require cooperation and coordination between public and private stakeholders.

RSES
Register of Security Engineers & Specialists

The Register of Security Engineers and Specialists (RSES) is responsible for maintaining the standards of practicing security engineers and specialists, to ensure that the highest level of advice is provided to transport infrastructure owners and operators within the United Kingdom and Internationally. The ability of Members of the Register to consider resilience and risk as a part of their planning process is fundamental to ensuring that clients receive the most appropriate advice. As such the RSES is pleased to sponsor the IET Infrastructure Risk and Resilience: Transportation special interest publication.

The broad range of papers in the publication typifies the diversity of the subject area and will hopefully encourage debate within the engineering and wider transport community and transparency about resilience for commuters and other stakeholders.

Although many of the more frequent risks associated with disruption of transport networks are caused by natural phenomena, there are lessons that can be drawn for security engineers, particularly where infrastructure vulnerabilities are highlighted. As such the RSES believes this special interest publication will provide stimulating Continuing Professional Development for both the security and mainstream engineer.

Georg Mayer - Head of Department, Tunnel Equipment and Operation, PTV Transport Consult GmbH

Reliable and efficient transport infrastructures are crucial to modern society. Therefore, a major concern of owners and operators of important transport links in Europe is to ensure their high availability.

PTV assists by offering a complete and integrated set of services covering all important problems of today's and future traffic and transport. The interdisciplinary staff of PTV deal with complex planning tasks related to all transport systems, integrating information technology (IT), communication technology and geographical information systems (GIS). PTV is active in the fields of Transport Logistics, Transport Telematics, Transport Planning, Public Transport, GeoMarketing and Infomobility, but is also engaged in Research & Development. PTV develops and supplies its PTV Vision software suite for all traffic planning activities.

Recent projects have focused on infrastructure risk assessment, development of simulation tools for road traffic risk analyses and hazardous goods analyses; methods for cost calculation and optimisation of road bridge maintenance as well as transport master plans. PTV is also a member of several boards reviewing German road construction guidelines.

Dr. Georg Mayer is the head of the department of Tunnel Equipment and Operation. In his person, he combines year-long experience in national and international expert reports and research projects on tunnel engineering with special skills like computational fluid dynamics, quantitative risk assessment and digital video analysis. He has produced a great number of reports on planning and testing tunnel equipment and tunnel operation technology, in particular on tunnel ventilation systems.

He is also an internationally acknowledged expert on safety and security assessment by means of quantitative risk analysis (QRA), the elaboration of safety and security concepts as well as the development and application of numerical models for fire dynamics (CFD) and fire and evacuation simulation.

PTV is proud to be able to add to a higher awareness of the Infrastructure Risk & Resilience topic, to contribute to find solutions for safety and security problems and eventually to help achieving better standards.

For more information, visit www.ptvgroup.com

Matthew Clarke - Head of Tolling, Technology and Lighting Design, Atkins Highways and Transportation

Economic and environmental pressures are forcing infrastructure providers to make better use of existing assets. This means that there is an increasing dependency on operational efficiency, which in turn places technology at the heart of infrastructure system performance.

This can be seen, for example, in Interurban highways, where the hard-shoulder is starting to be used as a running lane. The benefits of using the hard-shoulder are clear; additional capacity is available without disruptive and expensive widening. The challenge of using the hard-shoulder is safety performance, which is dependent on compliance with speed limits and other instructions, early detection of problems and rapid incident resolution. This means that operational processes, agencies, equipment, systems and highway infrastructure need to be co-ordinated in an integrated operation. Resilience of each of these elements is essential to provide motorists with the service that they expect and that the country needs.

There are additional constraints imposed by hard-shoulder usage. In particular, access is more restricted for maintenance staff to stop safely to perform inspections, repairs, cleaning or other preventive maintenance. Technology needs to have higher reliability and availability performance with less frequent and more limited access.

Technology is improving to meet these challenges. In-vehicle navigation technology enhances highway traffic and travel information provision, highway display technology has migrated to LEDs, modular construction helps spares management, lightweight equipment speeds up replacement and intelligent equipment monitoring identifies faults early. These

developments are combined with maintenance contract service level agreements and sophisticated engineering planning to meet the needs of the network.

It is clear that there is a link between technology resilience and network performance and this dependency is likely to grow. This will be driven by increased integration between the infrastructure and user's technology and additional demands from future economic growth and sustainability and safety performance.

For more information visit www.atkinsglobal.com

ISSN 2041-5923

Infrastructure risk and resilience: a review

James Peter Kimmance[1] *Anthony John Harris*[2]

[1]*Risk Mechanics Ltd, UK*
[2]*Parsons Brinckerhoff Ltd, UK*

Abstract: Critical infrastructures important to society are at risk from natural hazards and man-made events, ranging from climate change to terrorism. The awareness of the potential consequences in socio-economic terms of losing the functionality and availability of this infrastructure has grown in the past two decades. The result has been considerable research effort into understanding our infrastructure systems, how they are interconnected and the levels of risk that exist from the variety of hazards they face. A significant number of infrastructure related risk and resilience policies, plans and supporting methods of analysis and assessment have been produced. This paper reviews current thinking regarding risk and resilience of infrastructure, and in particular that of transportation systems. The aim is to illustrate the key concepts, identify developments and signpost sources of suitable information.

Keywords: Critical infrastructure, risk, resilience, interdependency, climate change, terrorism, transport

1 Introduction

Typically there are likely to be a number of systems that encompass identified critical infrastructures (CI) in any nation, region or business district. There is an increased awareness that infrastructure systems may be vulnerable to a range of hazards. Furthermore it is recognised that many of the CIs may be interconnected to the extent that they are interdependent at various levels and that an adverse event on one CI may cascade into secondary or tertiary effects and consequences on other CIs, such that the resulting cumulative consequences may have far broader repercussions than may have been anticipated when considering the original event in isolation. In such cases there may be no clearly identified measures to preclude, mitigate or adequately respond in order to facilitate an efficient recovery, thereby compounding the potential for adverse consequences. Such interdependencies of infrastructure systems are becoming increasingly complex and challenging with the increased use of telecommunication and information networks to support and even control many CI functions. Energy, transportation, water and finance are key examples of the use of information and communications technology (ICT) to reduce business costs, promote better service levels, support efficiency and sustainability, and as a result increasing the reliance on system interdependency.

Reflecting this awareness of society's vulnerability to the many hazards that infrastructure systems are exposed to, the concepts of risk and resilience within the context of CI and its protection have been increasingly researched and documented. The terms and the technical methods associated with them can sometimes be ambiguous with a lack of consistency and common terminology being a handicap to understanding and defining interdependencies between systems. These inconsistencies are influenced by factors ranging from the original objectives or discipline (e.g. security risk or natural hazard studies), the type of infrastructure/industry sector being considered, as well as national differences including economic characteristics and scale (e.g. regional, national or local).

This review does not try to be exhaustive but selectively identifies and introduces some key topics and terms that are important to understanding resilience of infrastructure in a fairly broad, general sphere but with a particular emphasis on transportation.

1.1 Critical infrastructure

The origin of the term CI has been attributed to President Bill Clinton in the mid 1990s, and formally adopted in the Homeland Security Act 2002 [1]. In summary these

infrastructures were considered to be physical assets, people and information/communication (cyber) systems necessary for national, state and urban security, economic stability and public safety. Initially 15 infrastructure sectors were identified, including; information technology; telecommunications; transportation systems; energy; banking and finance. This was developed further with Homeland Security Presidential Directives [2] and National Infrastructure Protection Plans [3], providing the strategy and guidelines for determining criticality and appropriate forms of protection for facilities and infrastructure objects. The Australian Government [4] and UK Government Cabinet Office [5, 6] have developed similar CI strategies and infrastructure sector specific plans with the goals of protecting systems and increasing their resilience. Common to each of these national guides is their applicability to 'All Hazards' i.e. natural, as well as man-made and malicious disruptions to our infrastructure. As such they have drawn extensively upon the approaches adopted in assessing the effects of natural hazards at community and regional scales [7, 8].

It should be noted that the concept of 'criticality' can also be applied to individual elements or objects within a system, i.e. criticality in much of the literature on the subject is very much scale and scope related.

1.2 Resilience

Resilience has, in a relatively short time scale, become a widely used term, with a variety of domain specific definitions. Resilience within the area of materials science [9] can be related to elasticity in terms of the maximum energy that can be absorbed without creating permanent distortion. Similarly in terms of systems, resilience can be seen as having the ability to resist, absorb, recover from or adapt to adverse changes. Common to both these descriptions is the concept of a force or 'event' causing change or disruption. As such it has therefore found increasing use within the context of CI resilience where the event may be

1. Sudden natural events such as hurricanes or earthquakes

2. Sudden man-made accidents or deliberate terrorist actions

3. Gradual change to the operating environment, brought about by climate or demographic/usage change.

Within the broader context of resilience, a broad spectrum of research has been ongoing for some time in terms of natural hazards and community resilience [10], interconnected local systems [11], and ecosystems [12]. Some of the work on the natural environment has provided particularly valuable insights into how complex systems, through their adaptability, transformability [13] and interactions at various scales develop inherent resilience. What is apparent from this research however is that any analyses, particularly those pertaining to risk originating from natural and man-made hazards, need to recognise the interplay and connections between infrastructure (both physical and cyber), human (social), natural and economic systems. It is also apparent that the term resilience is a ubiquitous one which conceptually enables the capture and assessment of issues encompassing a broad range of subject areas that are increasingly considered important by society (i.e. safety, health, security, environment and sustainability [14]), and as such its use is likely to continue to expand. Its ubiquitous nature may be illustrated in terms of sustainability and climate change, a major strategic and operational consideration for today's societies. A resilient infrastructure may be considered as one in which the physical systems and assets have a degree of robustness and are therefore capable of surviving and performing well under conditions of change, while avoiding excessively conservative design. In doing so the needs for redesign, maintenance, refurbishment, re-construction or demolition during the intended lifecycle of the infrastructure may be reduced, thereby contributing to improved sustainability.

Returning to an 'all hazards' CI perspective, that covers natural and man-made hazards as well as terrorist attacks, the RAMPCAP^{Plus} approach describes resilience as 'the capability to function during an event or to recover function rapidly after an event, including provision of a substitute function or asset provided after an attack or natural event' [15]. Additional suggestions are made that 'indicators of resilience could be reductions in the duration and severity of service denial and or economic loses'. Fig. 1 (after [16]) illustrates this concept in terms of a system operating at its designed level of functionality (100%), until an event occurs that exploits a vulnerability to disrupt and reduce its functionality by some amount (the consequence) for some period until recovery in full functionality is achieved.

1.3 Multi-hazard infrastructure risk assessment

The concept of resilience illustrated above includes aspects of threat (or likelihood) of a disruptive event, vulnerability to such an event and the associated consequences, all terms associated with the many branches of risk management. A number of approaches to assessing infrastructure risk with the intention of identifying mitigation measures and developing resilience have been developed. These can often be very infrastructure specific and qualitative, using judgements based upon pre-set matrices and factored 'score card' systems for assets types and scenarios found within that specific infrastructure sector [17].

Other more quantitative approaches have been developed, and these generally fall into two or three categories. Those intended for a variety of hazards and applicable across a broad range of infrastructures and facilities [15], or those for specific hazard types and targeted at specific types of infrastructure such as oil and gas [18], or those developed

for specific infrastructures such as the Sandia suite of risk assessment methodologies [19] (including dams, water utilities, energy, chemical plants, power transmission, prisons etc).

The majority of the quantitative approaches are based upon the basic relation common to many risk assessments:

Risk = Likelihood * Consequence, which can be further decomposed into the form

Risk = Threat * Vulnerability * Consequence

In RAMCAP Plus this basic quantitative approach is contained within seven core stages: (1) asset characterisation; (2) threat characterisation; (3) consequence analysis; (4) vulnerability analysis; (5) threat assessment; (6) risk/resilience assessment; (7) risk/resilience management.

In order for these risk based methods to be most effectively applied and provide assessments from which priorities and resources can be managed to reduce risk and increase resilience, it is necessary to have reliable information/intelligence regarding threats, vulnerabilities and consequences.

A significant problem exists in estimating the likelihood/threat, especially in relation to terrorist attacks, where the terrorist in order to succeed needs to do something 'unexpected' in order to circumvent established security measures. In these situations 'past' levels and types of activity may not apply. There are useful databases available [20], but as these are backward looking and do not necessarily capture trends or paradigm shift in approach or technology that may occur in the future, so their use in predicting likelihood/threat levels for future scenarios needs to be approached carefully.

As a result a variety of approaches have been developed. One category that may be termed 'evidence based analysis or assessment' uses data sources such as those above in what are typically statistical approaches. Although the use of such apparently detailed quantitative approaches can provide confidence (often un-warranted), a simplistic method often adopted is the use of score card systems summing various contributions to threat/vulnerability [17, 21] (e.g. ease of access to target, symbolic value, expertise etc) which can be used to determine a threat level, with the advantage that they are easy to apply. Alternatively techniques such as event tree analysis, widely used in safety and reliability analysis, may be used as an approach to threat analysis. In this approach all the actions and conditions necessary for a malicious entity to launch an attack are identified, sequentially structured and probabilities allocated to the likely success of each step.

In all these cases the threat/likelihood estimates are relatively subjective and therefore limited in terms of reliability and can hence fall short of the needs of risk managers using traditional risk models to prioritise decisions and resources.

This problem can also extend to natural hazards where, although historical data on frequencies and magnitudes are available and 'predictive' models based upon understanding mechanics have been developed, there can still be significant uncertainty due to the following:

- monitored major events may be infrequent, and therefore the data set is sparse and any underlying cycles are unidentified, or
- the observed cycles and predictive models are undergoing change. A prime case being that of climate change generating a 'new' environment with increased uncertainty regarding frequencies and intensities.

In circumstances where evidence based approaches are found lacking (particularly relevant to terrorism), one approach is to adopt a conditional threat risk scenario (often setting the threat level at unity) so that relative consequences, possible mitigation costs and the possible benefit from those mitigations can be directly compared. However, in adopting this approach, a major limitation is introduced in that, the results cannot be used to contrast the risk levels applicable to non-similar infrastructure systems and assets.

Other approaches that allow a more inventive approach to developing potential event chains include threat scenario development, reverse stress testing, and the more structured game theory – although still accommodating imaginative input. The advantage of game theory is that it enables the dynamic nature of threat and vulnerability, combined with consequences and terrorist intent/opportunities to be modelled. Combined with other analysis methods (e.g. networks etc) game theory provides a mechanism by which the terrorist intent or goals are identified but the targets and methods are not, and may vary both in time and space. After simulation of many 'games' the types of attack and likelihoods of delivering the likely outcomes can be arrived at [22].

Methodologies using game theory, probably combined with structured network or systems analysis and contained within a risk management framework to facilitate demonstrable governance and decision making support, seems to provide one of the more promising ways forward.

At this point it is normal for most modern discussions on risk due to unforeseen or complex events that result in major consequences to draw upon the 'Black Swans' concept proposed by Taleb [23]. Fukishima and the M1 motorway fires [24, 25] could be cited as examples of this outlook. Although much in agreement with Taleb's observations, it is suggested that his work actually provides a timely

reminder of the limitations of conventional risk management approaches. This enables us to recognise and place boundaries on the use of conventional risk assessment methodologies, including those involving networks and game theory and develop better informed decision making tools [26]. It is suggested that research in this area may provide future benefits to the study of resilience.

1.4 Relating risk and resilience

The discussion above in part highlights another potential confusion in this subject area – that is the apparent interchange and overlap between risk and resilience relating to infrastructure. Examining the development of the various national infrastructure protection documents identified in Section 1.1 above, could partly provide an explanation of this. As the available literature has been reviewed and re-issued over the past decade there has been a shift in emphasis:

- Initially risk assessment was seen as the means by which threats and vulnerabilities to infrastructure could be managed by the identification of suitable protection measures, thereby increasing resilience. The weakness in this type of approach (as discussed in 1.3 above) is that it uses historical data from similar, previous events to prioritise and then develop protection strategies. In the case of extreme weather events resulting from changing trends in climate, or deliberately planned, malicious acts such historical perspectives are of limited or even no use.

- Subsequently resilience has been seen as distinct from risk management, but part of an integrated cycle with risk management. Generally resilience is seen as being responsible for dealing with uncertainty inherent in risk assessments which means that risk may not be prevented by the identified protection methods and a method of dealing with this 'residual' risk is required. This change in perspective seems to have occurred from about 2009 onwards [27], and seems to be the most common approach. It also means that the types of multi-hazard method discussed in section 1.3, which risk practitioners are familiar with, remains valid.

- More recently it has been argued that the complexity and interdependency of infrastructure systems, coupled with imperfect information on the threats and vulnerabilities to which they are exposed renders 'risk assessment' based approaches of limited value, if not invalid [28]. In this case it is suggested [27] that the approach adopted should be purely resilience based, and that resilience may actually be supported by internal redundancy, adaptability and the concepts of a system having multiple states of equilibrium, that in this case would have 'acceptable' levels of performance. This type of approach isn't supported by the majority of national guides to the assessment and protection of CI, and is really one in which research for suitable assessment tools should be considered work in progress.

1.5 Interdependency

Irrespective of whether infrastructure systems operate at national, regional or more local community and business scales, they tend to mirror each other to the extent that they are individually complex and comprise a collection of internally interacting components, as well as external linkages to other systems. These linkages or interconnections can bring about synergies improving efficiency and service levels with associated economic and societal benefits.

This interactivity, with systems becoming 'systems of systems' that are connected at multiple nodes through a wide variety of mechanisms can also bring about the risk of disruptive events cascading through these interfaces with the consequences effectively 'amplified'.

Unfortunately, although there are a number of techniques for modelling the behaviour of individual infrastructures [29] in order to identify vulnerabilities or consequences to scenarios, there are very few proven or mature methods available to model interaction of networks and cascading failures. Those that do exist or are under development seem to be based around stochastic modelling of interactions, or generic cascading epidemiological modelling. They tend to be useful at a high level and/or are massively complex demanding major computational effort to model real world small to moderate scale systems.

However the existing single infrastructure and interface models do enable us to develop a better understanding of CIs, and how they 'might' react to various disruptions and scenarios. The understanding gained may best be combined with more topological/mapping based approaches to allow examination of the possible interactions between infrastructures. One of the first such comprehensive approaches was for the US Critical National Infrastructure [30] that demonstrated complexity with often previously unconsidered uni- or bi-directional dependencies. Numerous examples of various scales exist. One is a very illustrative perspective of a specific infrastructure sector, health care in Germany [31], in which more than 13 infrastructure interdependencies of varying significance were identified. A useful graphical tool termed the US CI Interdependency wheel [32] has been developed and used to identify Canadian and US CI at the national level. The approach cleverly uses two overlaid wheels, one with mapped relations between 9 CIs. As the top wheel is rotated to select the 'initial impacted' CI other windows in the wheel details the 3 most likely downstream cascades in an 8 to 36 hour window, post the initial CI impact. It also provides the upstream/or inbound dependencies of the impacted CI, that will be important in restoring or re-establishing the initially impacted CI. It is interesting to note that the differences between nations meant that the wheels had to be re-constructed for each national location. This needs to be considered for each change in region and

scale – but the approach provides a very good structured basis for identifying interdependencies.

The examples above illustrate a consistent theme in such studies, which is that interdependencies are generally extremely numerous and highly complex and that there are sufficient, significant regional variations that necessitate that mapping of interdependencies cannot simply be transferred between regions and infrastructure sectors.

The European Commission under its Seventh Framework Programme (FP7) has an ongoing project called DOMINO [33] that aims to develop a model that will quantify the modes of propagation and consequences of failures, in order to predict casualties, economic loss and damage to public confidence. It is intended that the methodology will be transferable to any country and any infrastructure sector.

A recent UK Government publication [34] regarding infrastructure preparedness for climate change discusses systematic interdependencies and identifies five key sectors (energy, ICT, transport, waste and water) as being significantly interdependent, the greatest dependency being on energy and ICT infrastructures. Interestingly transport is identified as having all five sectors dependent on it through a reliance on providing transportation for the workforce.

It is apparent in this literature review that most studies on CI interdependency concentrate on 'hard' physical or cyber systems [29], with far less attention given to 'softer' aspects such as people, culture and organisation. With the emergence of risks such as pandemic viruses and biological terrorism [35], coupled with observations that up to 85% of CI resources reside in the private sector [36] where there are potentially shortfalls in catastrophic continuity and emergency planning, it has become apparent that operations may be compromised by a shortage of key staff. This area needs to be addressed, if possible in an integrated manner, in any study of resilience

It is therefore also possible to argue that the transportation of the people necessary to keep systems operational (more so than materials) may play an even bigger role in infrastructure resilience, even for largely automated systems.

2 Transport systems

2.1 Susceptibility to disruption

Transportation systems including airports, ports, highways, waterways, rail and mass transit systems are clearly CIs, with many cross sector interdependencies. Comprising a complex mix of fixed and moving assets transport systems are designed for ease of access and efficiency. Most open to access, by necessity of the role they play, are highways, rail and mass transit systems. This openness, and in the case of rail and mass transit systems the funnelling of large numbers of people within relatively small areas has made them prime terrorist targets. Attacks on such targets can cause large scale casualties, bring entire systems and cities to a halt, damage passenger and community confidence, and cause significant commercial damage. Data regarding attacks with explosives against transport systems between 1995 and 2011 [20] indicates that there have been more than 1717 incidents, of which 247 attacks have occurred within Europe. The majority of these have been on rail/subway mass transit systems, with the trend since 2004 for successful incidents to incur increased casualty rates, amid an overall trend of increased attacks against transport [37]. Table 1 illustrates some notable attacks on rail transit systems following one of the first major incidents which involved a chemical attack on the Tokyo subway in 1995, which killed 8 and injured 4700 people.

These data suggest there is a clear susceptibility and attractiveness of mass transit systems to terrorism, a conclusion supported by others [38].

They are also susceptible to natural disasters and climate changes, as seen from Hurricane Sandy's impact on New York [39], where with overall costs lying in the region of $30–50 Bn, the costs of repairing the transport system, including a flooded subway system normally carrying 8.5 M passengers per day, estimated as lying between $5–10 Bn. To this extreme example we can add a background of Europe and the UK experiencing extreme weather events, such as flooding, that causes disruption to transport networks for hours, days or months (2009, Cumbria flooding and bridge collapse).

2.2 European transport perspective

Within the European Union there are 65,000 km of designated motorways, 212,000 km of railways, and 42,000 of waterways, all of which have fixed assets that are to a varying extent, vulnerable to a range of disruptive events. They also often come in close proximity to each other or interact at nodes, where a failure of one may cascade on to other transport systems, or other CIs such as energy or water. An unintended example of just how such interfaces and interdependencies can cascade was provided in 2006, when an intentional isolation of a 380 kV power cable overlying the River Ems in Germany was carried out to allow a ship to pass safely underneath. This destabilised the electricity grid causing a failure affecting 10 M people over several hours.

Other examples of disruption and loss of life due to catastrophic accidents on European transport systems are numerous. Fires are a particular concern: 1987 Kings Cross Station Fire killing 38 people; 1996, 2006, 2008 and 2012 Channel Tunnel fires, of which the 1996 and 2008 were the worst; 1999 Mont-Blanc tunnel fire killing 39 people; 2001 Gotthard tunnel fire killing 11 people, 2004 Wiehltal Bridge incurring no deaths but significant disruption for 3 years.

With a demonstrable background of man-made accidents and deliberate acts of terrorism causing disruption to

Table 1 Notable attacks on rail mass transit systems

Date	Location	Attack	Asset	Casualties Dead, (Injured)
03/1995	Tokyo	Chemical	Subway	8, (4700)
07/1995	Paris	Bomb	Subway	7, (87)
08/1995	Paris	Bomb	Rail	7, (60)
06/1996	Moscow	Bomb	Subway	4, (12)
12/1996	Paris	Bomb	Subway	4, (86)
11/2000	Dusseldorf	Bomb	Subway	0, (9)
03/2001	Manila	Bomb	Rail Station	9, (60)
02/2004	Moscow	Bomb	Subway	40, (100)
03/2004	Madrid	Bomb(s)	Train(s)	191, (1800)
08/2004	Moscow	Bomb	Subway	10, (48)
07/2005	London	Bomb(s)	Train(s)	39, (1000)
07/2006	Mumbai	Bomb	Train	150, (439)
02/2007	Delhi	Bomb	Train	68, (111)
03/2010	Moscow	Bomb	Train	38, (25)

transport infrastructure, the European Commission has funded many studies into the subject area. One report [40] reviewing the potential threats to public transport emphasises that physical elements of the systems are difficult to protect, and that assets like bridges and tunnels are often very exposed.

Most recent studies have been funded under the 7th EC Framework Programme: Security systems integration, interconnectivity and interoperability, and specifically under ICT-SEC-2007-1.0-01: *Risk assessment and contingency planning for interconnected transport or energy networks*.

One such funded study, recently completed (at the end of 2012) is the Security of Road Transport Networks (SeRoN) project [41], focused on the economically important European roads network. Examining the impacts of possible man-made attacks on the transport network, in particular the impacts on the regional and supra-regional scale, the aim was to develop a methodology to identify and analyse critical road transport networks, or parts thereof and undertake a risk assessment, using this to prioritise protection measures, and evaluate their effectiveness in terms of risk reduction and cost. The initial part of the study involved the review of existing literature on the vulnerability and risk to surface transportation tunnels and bridges from terrorism. Several documents were found to be most useful with respect to bridge and tunnel security risk and mitigation strategies [42–44]. Papers considering the vulnerability and structural

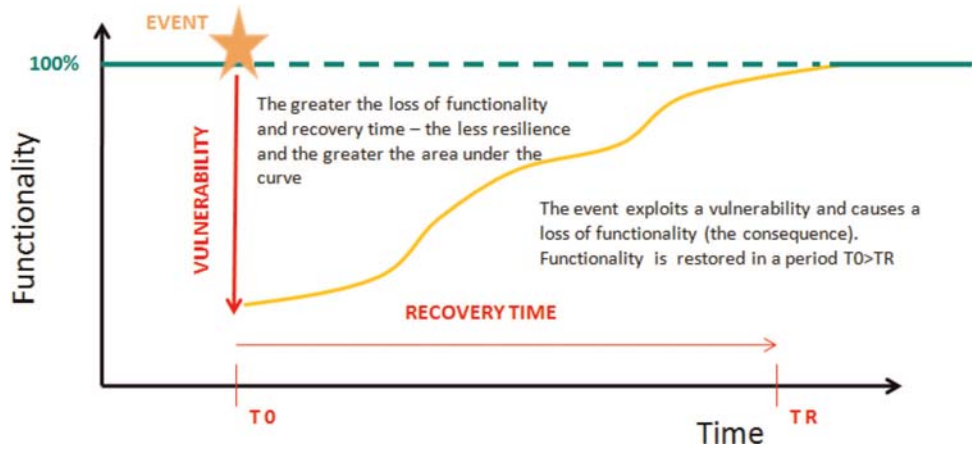


Figure 1 *Idealised concept of resilience (after Kimmance [16])*

performance of bridges and assessment of bridges subjected to explosions were of use in supporting the development of scenarios and impact models [45–47]. Using this information the resulting methodology adopted a combination of larger network and smaller object asset inventory and characterisation. This was followed by specific asset (bridge and tunnel) threat, vulnerability and consequence assessments. Initially conducted at a high level (filtering), and refined to include the comprehensive analysis of assets meeting selection criteria. Risk assessments and mitigation measure evaluation, and cost benefit decisions could then be made within a structured framework. The methodology has wider applications which maybe be further developed.

3 Summary

This paper has introduced the topic of infrastructure resilience, and provided a high level review of recent research and developments which should enable interested readers to conduct their own more detailed reviews and research into the subject area. It has highlighted that threats to our CIs resulting from climate change, accidents and terrorism are real, and that transportation systems are very much on the frontline with the potential to incur major consequences in terms of lives lost, economic damage and reduced public confidence. In order to manage the risks and improve resilience it has been observed that risk-based frameworks, built around a variety of simulation or analysis models (e.g. network analysis, blast and structural dynamics, game theory) are feasible, based upon current practices and modelling tools.

4 References

[1] Department of Homeland Security. Homeland Security Act (2002). http://www.dhs.gov/homeland-security-act-2002

[2] Homeland Security Presidential Directive. HSPD-7:Critical Infrastructure Identification, Prioritisation, and Protection. 2003. http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy04/m-04-15.pdf

[3] Department of Homeland Security. National Infrastructure Protection Plan: Partnering to Enhance Protection and Resiliency (2009). http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf

[4] Australian Government. Critical Infrastructure Resilience Strategy. Attorney General, Commonwealth of Australia. http://www.tisn.gov.au/Documents/Australian+Government+s+Critical+Infrastructure+Resilience+Strategy.pdf

[5] CABINET OFFICE: 'Keeping the Country Running: Natural Hazards and Infrastructure' (Cabinet Office, London, 2011), https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/61342/natural-hazards-infrastructure.pdf

[6] CABINET OFFICE: 'A Summary of Sector Resilience Plans' (Cabinet Office, London), https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/62312/Summary-2012-Sector-Resilience-Plans.pdf

[7] FEMA: 'Multi-Hazard Identification and Risk Assessment: The cornerstone of the national mitigation strategy' (Federal Emergency Management Agency, Washington, 1997), http://www.fema.gov/library/viewRecord.do?id=2214

[8] LINDELL M.K., PRATER C.S.: 'Assessing Community Impacts of Natural Disasters', *Natural Hazards Review*, 2003, **4**, (94), pp. 176–185

[9] CAMPBELL F.C.: 'Elements of Metallurgy and Engineering Alloys' (ASM International, 2008), p. 672

[10] BRUNEAU M., CHANG S.E., EGUCHI R.T., LEE G.C., WALLACE W.A.: 'A Framework to Quantitatively Assess and Enhance the Seismic Resilience of Communities', *Earthquake Spectra*, 2003, **19**, (4), pp. 733–752

[11] TURNER B.L., KASPERSON R.E., MATSON P.A., MCCARTHY J.J., CORELL R.W., CHRISTENSEN L., ECKLEY N., KASPERSON J.X., LEURS A., MARTELLO M.L., POLSKY C., PULSIPHER A., SCHILLER A.: 'A framework for sustainability science', *Proceedings National Academy Sciences*, 2003, **100**, (4), pp. 8074–8079

[12] WALKER B., HOLLING C.S., CARPENTER S.R., KINZIG A.: 'Resilience, adaptability and transformability in social-ecological systems', *Ecology and Society*, 2004, **9**, (2), p. 5

[13] FOLKE C., CARPENTER S.R., WALKER B., SCHEFFER M., CHAPIN T., ROCKSTROM J.: 'Resilience thinking: Integrating resilience, adaptability and transformability', *Ecology and Society*, 2010, **15**, (4), p. 20

[14] COAFFEE J.: 'Risk, resilience, and environmentally sustainable cities', *Energy Policy*, 2008, **36**, (12), pp. 4633–4638

[15] RAMCAP PLUS – ALL HAZARDS RISK AND RESILIENCE: 'Prioritising Critical Infrastructures Using the RAMCAP Plus Approach' (American Society of Mechanical Engineers Innovative Technologies Institute (ASME – ITI, 2009), p. 155

[16] KIMMANCE J.P.: 'Introduction: Infrastructure Risk & Resilience'. In IET/SeRoN Conference on Infrastructure Risk and Resilience, 2012London, http://tv.theiet.org/technology/transport/15077.cfm

[17] SCIENCE APPLICATIONS INTERNATIONAL CORPORATION (SAIC): 'A guide to Highway Vulnerability Assessment for Critical

Asset Identification and Protection' (AASHTO, USA, 2002), p. 47

[18] AMERICAN PETROLEUM INSTITUTE AND NATIONAL PETROCHEMICAL & REFINERS ASSOCIATION: 'Security Vulnerability Assessment Methodology for the Petroleum and Petrochemical Industries' (API Publishing, Washington, 2004), p. 155

[19] Sandia. Sandia National Laboratories Security Risk Assessment Methodologies: Overview. http://www.sandia.gov/ram/

[20] Global Terrorism Database. http://www.start.umd.edu/gtd/

[21] BEITEL G.A., GERTMAN D.I., PLUM M.M.: 'Balanced Scorecard method for predicting the probability of a terrorist attack'. Fourth International Conference on Computer Simulation in Risk Analysis and Hazard Mitigation. Risk Analysis IV, Southampton, 2004, vol. 10

[22] KANTURSKA U., ANGELODIS P.: 'Complex networks & game theory as frameworks for the analysis of critical infrastructure'. In IET/SeRoN Conference on Infrastructure Risk and Resilience, London, 2012, http://tv.theiet.org/technology/transport/15081.cfm

[23] TALEB N.: 'The Black Swan, The Impact of the Highly Improbable' (Penguin Books, London, 2008), p. 44

[24] TETT G.: 'Black swans, but no need to flap' (Financial Times.Com Magazine, 2011)

[25] Association for Project Management. Risk doctor defends M1 closure decision. 2011. http://www.apm.org.uk/news/risk-doctor-defends-m1-closure-decision

[26] HATFIELD M.: 'Game Theory in Management' (Gower, Surrey, 2012), p. 197

[27] Centre for Security Studies. Resilience and Risk Management in Critical Infrastructure Protection Policy: Exploring the Relationship and Comparing its Use. Focal Report 7: SKI. CSS, ETH Zurich, 2011, p. 19

[28] FISCHBACHER-SMITH D., FISCHBACHER-SMITH M.: 'The changing nature of risk and risk management: the challenge of borders, uncertainty and resilience', *Risk Management*, 2009, **11**, (1), pp. 1–12

[29] Adelard LLP. Infrastructure interdependency analysis: Introductory research review. (2009), p. 35. http://www.csr.city.ac.uk/projects/cetifs/d422v10_review.pdf

[30] HELLER M.: 'Life-cycle infrastructure risk management: R&D needs' (Roundtable on Risk Management Strategies in an Uncertain World, New York, 2002), http://www.ldeo.columbia.edu/chrr/documents/meetings/roundtable/pdf/notes/heller_miriam_note.pdf

[31] RIEGEL C.: Risk Assessment and Critical Infrastructure Protection in Health Care Facilities: Reducing Social Vulnerability. Paper for the Summer Academy 'Megacities: Social vulnerability and resilience building' hosted by United Nations University - Institute for Environment and Human Security (UNU-EHS) and Munich Re Foundation 2007. http://www.ehs.unu.edu/file/get/3796

[32] MACAULAY T.: US Critical Infrastructure Interdependency Wheel (CIIW) Executive Summary, 2009. http://tysonmacaulay.com/CIIW%20US%20Overview%20-%20July%205%202009.pdf

[33] European Commission. DOMINO Project. http://www.dominoproject.eu/

[34] GOVERNMENT H.M.: 'Climate Resistant Infrastructure: Preparing for a Changing Climate' (The Stationary Office, Norwich, 2010), p. 71

[35] RAIMBAULT C., BARR A.: 'Emerging Risks: A strategic Risk Management Guide' (Gower, 2012), p. 241

[36] FEMA. 2011 Pandemic Influenza Guide for Critical Infrastructure and Key Resources, http://www.ready.gov/document/pandemic-influenza-guide-critical-infrastructure-and-key-resources

[37] European Organisation For Security (EOS). A Global European Approach for Mass Surface Transportation Security & Resilience. 2009. http://www.eos-eu.com/files/Documents/WhitePapers/surface_transport.pdf

[38] GROSSMANN P.: WP120: Threat Analysis, Vulnerability Study and Risk Evaluation. Deliverable D121: Historical Background – Analysis of Security Related Incidents. TRIPS project within the EU research programme 'The enhancement of the European industrial potential in the field of Security Research'. (2006), p. 63

[39] DONAHUE P.: 'Repairing the New York subway system after Hurricane Sandy may be the MTA's biggest task yet', *New York Daily News*, 2012, http://www.nydailynews.com/new-york/hurricane-sandy-mta-biggest-task-article-1.1195365#ixzz2QX5TUVTT

[40] PUBLIC PASSENGER TRANSPORT CLUSTER: 'Study PT 1: Impact Assessment on Rail and urban passenger transport security at the European Level regarding terrorist threats in railways and urban passenger transport' EU-6th Framework Programme (FP6), 2007, p. 65

[41] SeRoN Project. Security of Road Transport Networks. Framework Programme 7 (FP7 - ICT- SEC-2007). (2009–2012). http://www.seron-project.eu/

[42] Transportation Research Board. Making Transportation Tunnels Safe and Secure. NCHRP Report 525 (Vol. 12), pp. 168, (2006). http://onlinepubs.trb.org/onlinepubs/nchrp/nchrp_rpt_525v12.pdf

[43] DOLNIK A.: 'The Terrorist Threat to Singapore's Land Transportation Infrastructure: A Preliminary Enquiry' (Institute of Defence and Strategic Studies, Singapore, 2006), p. 25

[44] THE BLUE RIBBON PANEL ON BRIDGE AND TUNNEL SECURITY: 'Recommendations for Bridge and Tunnel Security' (FHWA, 2003), p. 64

[45] LEUNG M., LAMBERT J.H., MOSENTHAL A.: 'A Risk-Based Approach to Setting Priorities in Protecting Bridges Against Terrorist Attacks', *Risk Analysis*, 2004, **24**, (4), pp. 963–984

[46] RAY J.C.: 'Risk-based prioritization of terrorist threat mitigation measures on bridges', *Journal of Bridge Engineering*, 2007, **12**, pp. 140–146

[47] WINGET D., MARCHAND K., WILLIAMSON E.: 'Analysis and design of critical bridges subjected to blast loads', *Journal of Structural Engineering*, 2005, **131**, (8), pp. 1243–1253

ISSN 2041-5923

Europeanising Transport Security: Policy and research recommendations for improving transport infrastructure security in Europe

Jakob Haardt Samuel Rothenpieler

Federal Highway Research Institute, Brüderstraße 53, 51427 Bergisch Gladbach 02204-43858, Germany
E-mail: haardtj@bast.de; rothenpieler@bast.de

Abstract: Although the EU has implemented some legislation on the security of transport infrastructure in Europe (i.e. EPCIP Directive 2008/114/), the security of transport networks up to date remains a national prerogative. While research has been conducted on a European scale, operative measures are implemented only on the national level. This paper argues for an Europeanisation of transport security, focussing on practicable recommendations for achieving this goal. Additionally, the divergence between a nationally shaped risk perception and the cross-boundary nature of security threats is discussed and possible strategies to overcome this problem are outlined. Furthermore, the paper aims at fostering the debate between (transport) security stakeholders in the EU Member States and presenting incentives and arguments for a shift from a national to a European security rationale.

Keywords: Transport, security, research, Europeanisation, recommendations, risks, threats

1 Introduction

A functioning and robust transport system is of vital importance to Europe's economy and society. It facilitates market competitiveness and decreases the overall costs of economic and social activities. According to recent European Union (EU) figures [1], in 2009, total goods transport of the EU27 has amounted to 3.632 billion tonne kilometres (tkm) of intra-European transport. For passenger transport, transport activities have amounted to 6.305 billion passenger kilometres (pkm).

Addressing the overall importance of transport security, the European Commission (EC) recently published a Commission Staff Working Document on Transport Security [2] to identify 'what can be done at the EU level to improve transport security'.

Taking up the suggestions of the EC working paper, this article develops practicable recommendations for improving transport security both from a policy and research background. In particular, it focuses on the security of transport infrastructure which plays a key role within the overall transport network of the EU.

The paper starts with a short introduction on the main threats to the transport system. Based on the identified threats, the paper develops an understanding for the main obstructions towards a more secure transport system of the EU both from a policy and a research point of view. Finally, practicable recommendations are given on how to overcome still existing gaps.

2 Threats to transport and transport infrastructure

Threats to the transport system and its infrastructure are versatile. Common distinctions differentiate between man-made and natural hazards. Man-made hazards include terrorist attacks or criminal acts as well as unintentional events such as accidents. Natural hazards relate to natural phenomena such as earthquakes, extreme weather events, flooding or storms, as well as the gradual effects of climate change such as increasing temperature or precipitation.

While the likelihood of terrorist attacks in Europe remains relatively low, natural hazards do have an inevitably higher significance for the transport system today and (even more so) in the future [3]. In particular, threats which are a consequence of climate change-induced extreme weather events concern infrastructure owners and operators as well as policy makers to the same degree [4].

It has been estimated that extreme weather conditions cost the EU's transport system at least €15 billion per annum [5]. Particularly, the maintenance and operation costs of transport infrastructure are significantly influenced by extreme weather events such as storms, severe winters (cold, ice, snow) and floods. Whereas, for example, the impact of floods on the road network is estimated to cost around 650 million € every year [6], the resulting indirect consequences of extreme weather events on users and the increasing insurance costs further increase this amount. Man-made as well as natural hazards not only affect the transport infrastructure (availability of international transport routes, repair works after adverse climate events, increase of maintenance cycles) but also the safety of the users of the different transport modes. For instance, it is estimated that roughly 10% of all road accidents, 5% of rail, and 10% of inland waterways accidents in Europe can be attributed to extreme weather conditions [7].

Addressing the internal and external dimension of EU security policy, the EU Security Strategy [8] of 2003 defines the threats to security in Europe as per se being of trans-boundary nature. This turn in global security policy also has practical relevance for specific fields of security policy and research within Europe such as the transport sector.

3 Deficits and obstructions towards a more secure transport system

Contemporarily, most methodologies for the assessment of threats to the security of transport systems and structures focus on one specific mode of transport. Challenges arise when interconnected or intermodal transport networks are considered. The EC Working Paper identifies particular difficulties with growing intermodal transport hubs 'where the cross-modal nature of operations' requires that the level of security is consistent throughout the hub [9]. For improving the security not only between the Member States but also between the respective modes, it states that 'the absence of common approaches or standards throughout the EU leads to weaknesses, inconvenience or additional cost'. Therefore, the improvement of transport security has to start with the lowest common denominator that is increasing the resilience of underdeveloped modes to support the resilience of the overall transport network. Additionally, common methodologies for assessing security risks for all modes have to be developed and put into practice across Europe. Effectively, transport systems in Europe are much more integrated and interconnected than in the past and this integration is likely to increase in the future. The levels of security, however, are neither equal for different modes nor among EU Member States.

Security is considered to be a policy field where the traditional concept of sovereignty is still predominant. The protection of the national society and its citizens is a discipline that requires a clear sociopolitical identity on behalf of the organisation being responsible. Transport security, however, is not 'hard security' (where sovereign rights have to be transferred) but 'soft security' (meaning that security remains a national prerogative) affecting all EU states to the same degree.

Problems arise from the fact that, traditionally, security is still largely a national prerogative and nations are highly reluctant to transfer competencies to European bodies. The idea of an interconnected European economic space and the still increasing interconnection of transport routes and corridors (TEN-T corridors) across all modes of transport, however, make national approaches obsolete. National initiatives cannot address the nature of European transport anymore. While transport security research has become a major focus of the European Research Framework Programs such as FP7 and Horizon 2020, there is still an evident lack of operative implementation of security solutions.

The European transport system, including its physical transport infrastructure, accordingly has to be seen as the backbone of Europe's highly integrated economy. If a particular transit route (TEN-T) in a certain region is affected by a security-relevant event, this may have dramatic economic and social consequences for other EU Member States as well. Hence, moving the security to Europe helps each EU Member State to address the hazards and threats to their infrastructure and even cope with the impacts of an event. While the EPCIP directive[1] responded to this aspect already in 2008, the EC may only set the framework for integrated action among European Member States while allowing for some flexibility in the actual implementation.

4 Policy and Research Guidelines

As the EC identified in its Commission Staff Working Document on Transport Security, 'the absence of common approaches or standards throughout the EU leads to weaknesses, inconvenience or additional cost' [10]. The focus is predominantly on the issue of land transport since this is the field where most of the intra-EU transport freight (up to 63%) [11] is transferred and only few security regulations on EU level exist.

[1]EPCIP stands for European Programme on Critical Infrastructure Protection. For more information go to http://europa.eu/legislation_summaries/justice_freedom_security/fight_against_terrorism/l33260_en.htm, last visited on 17/01/13

Addressing the research and policy gaps of transport security, the following policy and research recommendations reflect the findings of the EC Document and come up with research ideas and recommendations that should be taken up in order to improve transport and transport infrastructure security throughout the EU:

4.1 Develop common and European-wide applicable risk maps

Due to the fact that particular threats are not always as relevant for one country as they are for another, transport policy officials should encourage the development of European-wide risk maps. Risk maps developed on the basis of a common methodology allow for closing the gap between perceived risks or threats which are predominantly shaped by subjective perception and actual risks. Each country or rather its officials have particular threat perceptions depending on individual or group specific framings of how frightening the environment 'is perceived' and how risk averse a national community is (including the political parties, the media and the society). For the interconnected TEN-T network, however, it is of vital importance to identify so called 'hot spots' which are more threatened than other areas. These 'hot spot areas' should be defined as those regions that are particularly threatened by a specific threat, for instance rising sea water level (natural hazard), and have major relevance for the overall European economy. Possible investment into protection measures should start in these 'hot spot areas' where it is agreed that these are more threatened than others.

The usage of geographic information systems (GIS) is well known in the field of civil protection [12] where multiple data sets are merged into a visualised risk map. This patterned data can be used to reveal critical areas for the transport sector by collecting and merging statistical data from hazards, their occurrence, frequency or spatial distribution. For natural hazards regionalised climate projections can already today be used for substantial risk mapping [13].

4.2 Develop a common procedure to identify vulnerable transport infrastructure

Although the above described risk maps would help identifying and visualising prevalent threats to the transport system, a procedure is still needed to also identify vulnerable infrastructure assets within the transport network, such as tunnels, bridges, seaports, airports, embankments etc. Such procedure should allow for a threat-specific evaluation of critical infrastructure assets. The SeRoN project[2], for example, which was funded by the 7th EC Framework Programme, already developed a methodology for identifying critical road infrastructure and assessing suitable protection measures with regard to man-made hazards. The project was initiated in response to the EPCIP directive and developed a methodology how the EU Member States, in particular owners and operators of infrastructure assets, could deal with the identification of critical road infrastructure on a European level. However, the results of this project still need to be integrated into an intermodal context to allow for a holistic comparison between transport modes and other relevant threats to the transport system.

The need for a standardised tool is obvious, although there are still practical obstructions and also justified concerns about standardisation issues. Nevertheless, the aim should be a procedure that allows identifying and protecting European critical transport infrastructure across transport modes and with respect to different hazard types. A compilation of threats to the transport sector in a comprehensive hazard catalogue would be a needed prerequisite for the development of a common procedure to identify critical transport infrastructure.

Although such a common method could be used by every country on its own, the implementation of it should also be encouraged by European bodies. A wide application of this method in many European countries could help identifying relevant vulnerable infrastructure on a European level. This would put pressure on those countries where the level of security is comparably low to that in others and would prevent those states from becoming the 'entry point'[3] to the transport system towards different kinds of threats.

4.3 Develop more practicable solutions in form of handbooks and manuals

To bring the research results into practice, there is a growing demand for ready-for-practice handbooks and manuals that can be used by owners and operators of vulnerable transport infrastructure. These handbooks and manuals should achieve both a better understanding of threats to the transport system and its infrastructure throughout Europe and a better understanding of the available methodologies to identify and protect vulnerable transport infrastructure.

Handbooks and manuals should indicate what the main threats to the transport system are and should encompass a procedure for selecting appropriate and infrastructure-specific protection measures to be applied.

4.4 Integrate security aspects in transport infrastructure planning to improve the resilience of the TEN-T network

Apart from improvements in the actual state of the TEN-T network, the future planning and building of transport infrastructure needs to address security aspects as well. New

[2]For further information on the SeRoN project, please go to www.seron-project.eu.

[3]This term has been used by the EC for describing the different levels of security throughout EU Member States. When the interconnected European Single Market is to be understood as an economic system, the disruption of transport in one country may also affect other countries.

infrastructure projects should dedicate a considerable amount of effort into investigating the redundancy of infrastructure assets within the TEN-T network as well as include robustness issues also in the design phase of infrastructure assets. This procedure has already proven effective in the U.S. where the Federal Emergency Management Agency published a series for design guidance to improve security and provide inbuilt security standards to mitigate consequences of potential terrorist attacks [14].

On the basis of the above mentioned risk maps and the identified critical 'hot spot' areas (critical nodes and interchanges) infrastructure planning should pre-investigate the potential loss of infrastructure assets and possibilities for de-routing. The merging of these dimensions should consider the network and object criticality of transport infrastructure. Cost-effective protection measures should be implemented already in the design phase of TEN-T infrastructure projects in order to improve the robustness of transport infrastructure from the very beginning.

For identified critical 'hot spot areas' also emergency and contingency plans need to be developed that indicate substantial de-routing possibilities and emergency services operations for the most critical transport links. Furthermore, these plans should contain possible mitigation measures for likely security scenarios.

4.5 Standardise transport security regulations

As a prerequisite for the identification and protection of critical infrastructure and infrastructure assets, planning common security standards is required. Some of these regulations already exist today in the field of safety, such as the EU Tunnel Directive from 2004[4] or the Road Infrastructure Safety Management Directive from 2008[5]. To only identify critical nodes and assets is ineffective if design standards and possible protection measures are not harmonised to a comparable degree. In particular, this is valid for the EU enlargement process. Accession candidates need to ratify a certain acquis communautaire when it comes to security standards for transport policy and infrastructure security.

5 Conclusion & Outlook

For the EC, 'effective transport systems' are 'essential to Europe's prosperity, having significant impacts on economic growth, territorial cohesion, social development and the environment' [15]. Facilitating transport and exchange processes, transport infrastructure play a key role within the overall transport network of the EU providing access to employment, essential services such as health care and education, providing businesses with links to their supply chains and markets and ensuring social cohesion. Single infrastructure objects of specific transport modes, such as bridges and tunnels for the road and rail network or ports and watergates for the inland waterways network, have a crucial role in the interconnection of vital transport routes of the EU. With this in mind, it becomes obvious that the diversification of threats towards these infrastructures as well as their trans-boundary nature make a coherent European security approach necessary.

The present paper discusses the contemporary deficits regarding these issues and introduces a number of policy and research guidelines which could foster and further develop a single approach to the security of transport networks. These include:

(1) The Development of common and European-wide applicable risk maps;

(2) The Development of a common procedure to identify critical intermodal transport infrastructure;

(3) The Development of more practicable solutions in form of handbooks and manuals;

(4) The Integration of security aspects in transport infrastructure planning in order to improve the resilience of the TEN-T network;

(5) The Standardisation of transport security regulations.

Although further discussion and research on this matter is highly needed, the identified recommendations may serve as a starting point for promoting a European security perception within the public as well as academia and the political realm.

6 References

[1] European Commission (2012). EU Transport in figures, Statistical Pocketbook 2012, Luxembourg: Publications Office of the European Union, 2012, p. 19, in: http://ec.europa.eu/transport/facts-fundings/statistics/doc/2012/pocketbook2012.pdf

[2] European Commission (2012). Commission Staff Working Document on Transport Security, Brussels, 31.5.2012, SWD(2012) 143 final, in: http://ec.europa.eu/transport/themes/security/doc/2012-05-31-swd-transport-security.pdf

[3] INTERGOVERNMENTAL PANEL ON CLIMATE CHANGE: in FIELD C.B., BARROS V., STOCKER T.F., QIN D., DOKKEN D.J., EBI K.L., MASTRANDREA M.D., MACH K.J., PLATTNER G.-K., ALLEN S.K., TIGNOR M., MIDGLEY P.M. (EDS.) (Cambridge University Press, Cambridge, 2012)

[4]For more information please go to http://europa.eu/legislation_summaries/transport/road_transport/l24146_en.htm, last visited on 17/01/13

[5]Please go to http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:319:0059:0067:EN:PDF, last visited on 31/01/13

[4] WORLD ECONOMIC FORUM: 'Building Resilience in Supply Chains', *Industry Agenda*, 2013, p. 9

[5] MARKO NOKKALA, PEKKA LEVIÄKANGAS, KALLE OIVA (EDS.) (2012). The costs of extreme weather for the European transport system, EWENT project D4, Esbo: JULKAISIJA – UTGIVARE – PUBLISHER, p. 4, in: http://www.vtt.fi/inf/pdf/technology/2012/T36.pdf

[6] MARKO NOKKALA, PEKKA LEVIÄKANGAS, KALLE OIVA (EDS.) (2012). The costs of extreme weather for the European transport system, EWENT project D4, Esbo: JULKAISIJA – UTGIVARE – PUBLISHER, p. 26

[7] MARKO NOKKALA, PEKKA LEVIÄKANGAS, KALLE OIVA (EDS.) (2012). The costs of extreme weather for the European transport system, EWENT project D4, Esbo: JULKAISIJA – UTGIVARE – PUBLISHER, p. 42

[8] European Commission (2003). A Secure Europe in a Better World. European Security Strategy, Brussels, in: http://www.consilium.europa.eu/uedocs/cmsUpload/78367.pdf

[9] European Commission (2012). Commission Staff Working Document on Transport Security, Brussels, 31.5.2012, SWD(2012) 143 final, p. 3, in: http://ec.europa.eu/transport/themes/security/doc/2012-05-31-swd-transport-security.pdf

[10] European Commission (2012). Commission Staff Working Document on Transport Security, Brussels, 31.5.2012, SWD(2012) 143 final, p. 4, in: http://ec.europa.eu/transport/themes/security/doc/2012-05-31-swd-transport-security.pdf

[11] European Commission (2012). EU Transport in figures, Statistical Pocketbook 2012, Luxembourg: Publications Office of the European Union, 2012, p. 19, in: http://ec.europa.eu/transport/facts-fundings/statistics/doc/2012/pocketbook2012.pdf

[12] http://www.enpi-info.eu/mainmed.php?id=21173&id_type=1

[13] AUERBACH, MARKUS/HERRMANN, CARINA, KRIEGER, BEATA (2011): Anpassung der Straßenverkehrsinfrastruktur an den Klimawandel; in Federal Ministry of Transport, Building and Urban Development (2011): KLIWAS. Auswirkungen des Klimawandels auf Wasserstraßen und Schifffahrt in Deutschland; in: http://www.bmvbs.de/cae/servlet/contentblob/84044/publicationFile/57861/kliwas-ergebnis-zweite-konferenz.pdf, p. 54, last visited on 31/01/13

[14] Federal Emergency Management Agency (FEMA) (2003): Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings; Report 426; in: http://www.fema.gov/library/viewRecord.do;jsessionid=D5A6D1397996DE7E1FB80F10D43F1F5F.WorkerPublic2?action=back&id=1559, last visited on 31/1/13

[15] European Commission (2012). Commission Staff Working Document on Transport Security, Brussels, 31.5.2012, SWD(2012) 143 final, p. 2, in: http://ec.europa.eu/transport/themes/security/doc/2012-05-31-swd-transport-security.pdf

ISSN 2041-5923

Introduction to network theory and game theory as frameworks for the analysis of critical infrastructure

Urszula Kanturska Dr Panagiotis Angeloudis

Imperial College London,
E-mail: urszula.kanturska05@imperial.ac.uk; p.angeloudis@imperial.ac.uk

Abstract: This paper provides an accessible introduction to the application of basic concepts from network theory and game theory to identify critical elements of networks. Simple examples are used to illustrate the application of these methods in the analysis of transport networks and to discuss the interpretation of the results.

Keywords: game theory, network theory, complex networks, critical infrastructure

1 Introduction

The term 'critical infrastructure' commonly refers to sectors of the economy, public services or facilities that underpin the functioning of a state (e.g. telecommunications, healthcare, banking, water supply, electricity, transportation). Yet, 'critical infrastructure' can also refer to individual components of systems (e.g. a bridge, a pumping station), as is the case in this paper. Critical components are those elements of infrastructure systems whose functioning is essential for proper system-wide operation, or in other words, whose loss would cause most detriment to a system.

While somewhat imperfect operation is acceptable, infrastructure owners and operators are keen to invest in ensuring that some minimal level of service is retained in the majority of reasonably expected scenarios.

This definition indicates that concepts of resilience and criticality always need to be rigorously interpreted with clear reference to:

- what performance measure is adopted to express 'system functioning' or 'proper operation'; and
- what disruption scenarios or undesirable impacts are considered.

For example, performance criteria may range from compound probabilistic conditions (e.g. 'spare capacity of at least 20% on at least 95% routes for at least 50% of time') to simple measures (e.g. 'travel speed above 40 mph' or 'London and Sheffield remain connected'). Likewise, undesirable impacts vary in terms of severity (e.g. 'slippery bridge surface', 'lane closure', 'bridge collapse') and intention (e.g. 'planned engineering works', 'random accident' or 'targeted attack').

Here we introduce important insights from network theory into how network configurations affect resilience against random and targeted disruptions, and then introduce some basic concepts of game theory which illustrate that the risk related to undesirable events can be controlled even if their probabilities are unknown.

2 Network theory in practice

Network theory is a branch of science concerned with studying properties of networks, hence it is well suited for the analysis of transport infrastructure. The topology of a network, i.e. spatial configuration of links and nodes, has a major impact on a network's resilience, which we intuitively expect, but cannot express or measure without formal analysis. How do we know which of the metro systems shown in Fig. 1 exhibits best resilience?

In network theory, the following measures form the basis of topological analysis:

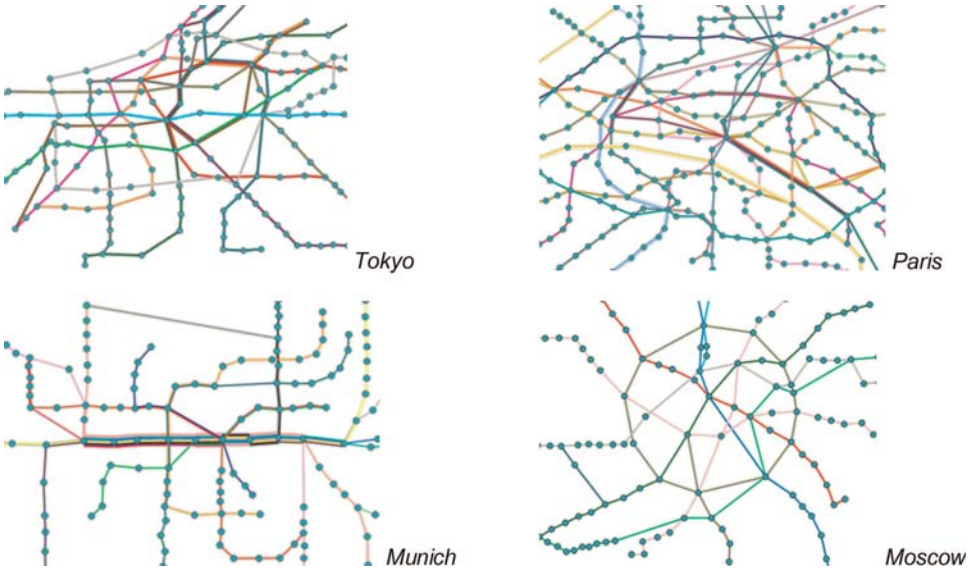


Figure 1 *Example of different topologies of world metro systems*

- Shortest paths – distance between any two nodes in the network, examined for all pairs of nodes in the network;

- Node degrees – number of direct connections each node has to other nodes, examined for each node in the network;

- Size of the node group – number of nodes that are connected to each other directly or indirectly.

These measures make it possible to determine which general class a network falls into. Most real-world transport networks are neither entirely 'random', such as the network in Fig. 2a, nor 'regular', such as the network in Fig. 2b. Instead, they combine properties of both, and belong to a class of 'complex' networks (Fig. 2c). Among complex networks we can distinguish two key sub-types:

- 'small-world' networks (Fig. 2d) with an interconnected structure, in which most nodes have a similar node degree and the most connected node in the network typically links directly to at most 10% of all nodes (e.g. highway networks); and

- 'scale-free' networks (Fig. 2e) that are dominated by a few highly connected nodes (e.g. airport hubs) while other nodes have only one or two direct connections.

Both types of complex networks are associated with certain advantages and disadvantages in terms of resilience. Typically this is tested by removing network nodes and checking how this affects the remaining connectivity: resilience against random incident is modelled by removing nodes at random; resilience against attack by removing nodes in the order of importance.

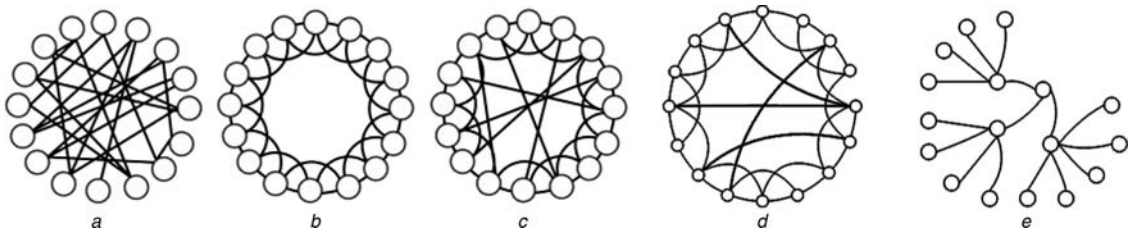


Figure 2 *Key network types: a – random, b – regular, c – complex, d – complex small-world, e – complex scale-free*

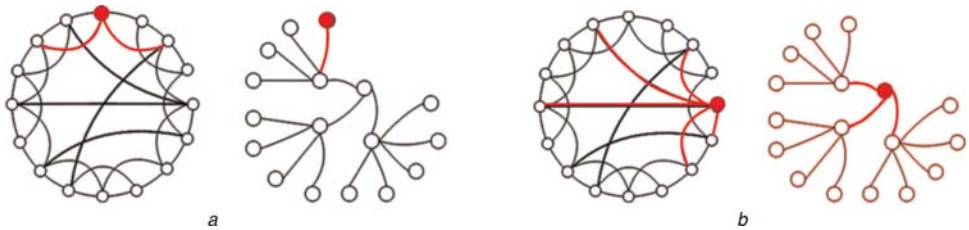


Figure 3 *a – random error in small-world and scale-free networks; b – targeted attack in small-world and scale-free networks*

An example of connectivity loss due to node removal is shown in Fig. 3 in red and highlights that due to major hubs being easy to identify, scale-free networks are very weak against targeted attacks (Fig. 3b), though they tend to be more resilient against random errors (Fig. 3a) than small-world networks [1].

In modelling targeted attacks, node degree has traditionally been used as a proxy for node importance, i.e. nodes attached to most links would be removed first. An improved approach was proposed in [2] where node importance is measured by the number of shortest paths that pass through a node, considering paths between all pairs of nodes in the network. This method was applied to analyse 150 metro systems around the world.

The results indicate that metro networks tend to be robust against random failures, but vulnerable against intentional attacks, whereby dramatic loss of connectivity occurs when some 3% of nodes (approximately 5 to 10 nodes) are removed from the system. Fig. 4 illustrates this for networks shown previously in Fig. 1. While the densely interconnected Paris network shows good resilience against a random error (red line) as well as against an attack (blue line), the Munich network suffers significant loss of connectivity after the removal of just one node, as all routes share a common central stretch.

3 Game theory comes into play

Game theory is a study of situations of uncertainty in which the outcome depends on decisions made by everyone involved. Players know each other's decision options and can estimate payoffs associated with each possible combination of decisions. Payoffs represent desirability (utility) of particular outcomes. Because players do not know which decision the other one will ultimately make, they behave strategically to maximise their own payoffs. Adopting a strategy means that in making choices they take into account what they expect the other player's preferences and rational choices might be.

Table 1 Payoffs associated with the example game against nature

Action ↓ State →	Will rain	Won't rain
Take	1	−1
Not take	−2	0

3.1 Games against nature

First consider a special case, where only one player behaves strategically and selects options based on payoffs, while the other one is not strategic, but selects decision options at random. This is known as a 'game against nature'. For example, in deciding whether to take an umbrella or not we consider four possible outcomes: I take it and it will rain; I take it but it won't rain; I don't take it but it will rain; and I don't take it and it won't rain. The payoffs associated with each outcome are traditionally represented in a table, such as Table 1, and depend on how a person values particular outcomes, e.g. inconvenience of carrying the umbrella versus discomfort of getting wet.

What is the optimal decision when uncertainty is intrinsically associated with nature's state? Such situations are formally a remit of 'decision theory' [3] and require adopting a decision principle, for example:

- *Subjectivity* – attach the best-guess subjective probabilities (e.g. 20% 'Will rain', 80% 'Won't rain') to each state and select the action with the highest expected payoff: for 'Take' expected payoff is $0.2 \cdot 1 + 0.8 \cdot (-1) = -0.6$; for

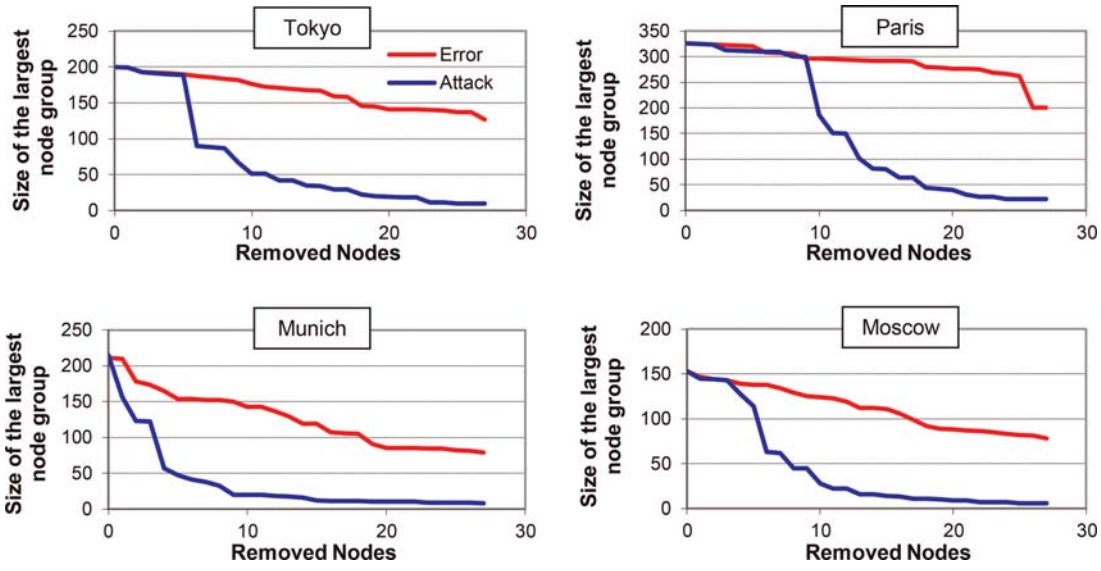


Figure 4 *Change in the size of the largest node group remaining connected for random and targeted failures in metro networks*

Table 2 Payoff table in rock– paper–scissors game

Column player → Row player ↓	Paper	Scissors	Stone
Paper	(0,0)	(−1,1)	(1, −1)
Scissors	(1, −1)	(0,0)	(−1,1)
Stone	(−1,1)	(1, −1)	(0,0)

Table 3 Simplified payoff table in rock–paper–scissors game

Column player → Row player ↓	Paper	Scissors	Stone
Paper	0	−1	1
Scissors	1	0	−1
Stone	−1	1	0

'Not take' it is $0.2 \cdot (-2) + 0.8 \cdot 0 = 0.4$, so the best action is 'Not take'.

- *Ignorance* – assume that both states are equally likely (i.e. 50% 'Will rain', 50% 'Won't rain'), and select an action with the highest expected payoff: for 'Take' expected payoff is $0.5 \cdot 1 + 0.5 \cdot (-1) = 0$; for 'Not take' it is $0.5 \cdot (-2) + 0.5 \cdot 0 = -1$, so the best action is 'Take'.

- *Pessimism* – select the action with the best payoff in the worst case state: 'Will rain' is the worst state as it is associated with the worst payoff in the whole table; for this state the action with the best payoff is 'Take'.

- *Optimism* – select the action with the best possible payoff: the best payoff in the whole table requires action 'Take'.

- *Regret* – choose the action with the smallest worst-case regret. First calculate for each state of nature how much each payoff differs from the largest payoff for that state of nature: For state 'Will rain': regret if 'Take' is $1-1=0$, regret if 'Not take' is $1-(-2)=3$; For state 'Won't rain': regret if 'Take' is $0-(-1)=1$, regret if 'Not take' is $0-0=0$. Then compare the worst-case regret for 'Take' and for 'Not take' (0 and 3, respectively), to see that the action minimising regret is 'Take'.

3.2 Games of conflict

So far, we considered a game when only one player behaves strategically. Yet, in traditional games we deal with two players who value the outcomes differently, favour different outcomes and adopt strategies to maximise own payoffs. In an extreme case when players have completely opposite interests and want to achieve opposite outcomes we have a 'zero-sum game'. As the name indicates, the positive payoff to one player equals the negative payoff to the other, because gain for one player is always at the expense of another.

For example, in a game of 'paper–scissors–stone' the payoffs to both players are shown in Table 2. In zero-sum games this traditional notation is often simplified by only showing payoffs to the row player, as in Table 3. In this case, the opposite interests of the players require an implicit assumption that the payoffs will be maximised by the row player and minimised by the column player.

What is the optimal decision in this case? John von Neumann established and proved the Minimax Theorem, which states that for every two-person zero-sum game, such as this one, there always exists a mixed strategy for each player such that the expected payoff for one player is the same as the expected cost for the other, and that expected payoff C, known as the 'value of the game', can be determined as

$$\max_{p}\left(\min_{q}\sum_{i,j} p_i c_{ij} q_j\right) = \min_{q}\left(\max_{p}\sum_{i,j} p_i c_{ij} q_j\right) = C$$

where cij denotes payoff related to the combination of decision i of the first player and j of the second player, taken respectively with probabilities pi by the first player and qj by the second player.

The minimax strategy is a Nash equilibrium, meaning that players have no incentive to change their strategy, as it offers the best possible expected payoffs for both. In other words, the optimal strategy for each player is to minimise the maximum payoff possible for the other player, which is equivalent to minimising own maximum loss. The optimal strategy guarantees that the actual payoff will be no worse than that indicated by the value of the game.

If a player's optimal strategy can be defined by a single action i such that $pi = 1$, as it was the case for the decision principles in games against nature, the strategy is called 'pure'. However, in traditional (non-cooperative) games a solution in pure strategies is only obtained when pure minmax strategy of the first player leads to the same outcome as pure maxmin strategy of the other player. For example, in a game shown in Table 4 the value of the game equals to a single payoff, highlighted with shading.

How is this solution identified? The row player is trying to minimise the opponent's maximum payoff, while maximising his own minimum gain. He first checks what the minimum gain is for options 1 and 2 (payoffs of 0 and 3, respectively) and selects the option which maximises this value (Option 2). The column player does the opposite, i.e. he first checks what the maximum loss is for options A and B (payoffs of 7 and 3, respectively) and selects the option which minimises this value (Option B). As Option 2 and Option B lead to the same outcome, they indicate the solution of the game.

Table 4 Example of a zero-sum game with pure-strategy solution

Row player ↓ Column player →	Option A	Option B	MIN ↓	
Option 1	7	0	0	
Option 2	4	**3**	3	← MAX
MAX →	7	3		
		↑ MIN		

More often than not, the optimal strategy is 'mixed', meaning that the players alternate between several pure strategies, according to pre-determined optimal frequencies pi and qj. In the example shown in Table 5 no pure-strategy solution exist, because pure minmax strategy of the row player leads to a different outcome than the pure maxmin strategy of the column player.

How to find a solution in this case? We will make use of the fact that the Nash equilibrium for a two-player, zero–sum game can be found by solving a related linear program

$$\text{Max}\{\text{Min}\{p_1 \cdot (1 \cdot q_A + 3 \cdot q_B) + p_2 \cdot (2 \cdot q_A + 0 \cdot q_B)\}\}$$

subject to

$$p_1 + p_2 = 1$$
$$0 \leq + p_i \leq 1$$

Using a standard linear programming solver we can find that the optimal strategy for the first player is $p_1 = 0.5$ and $p_2 = 0.5$, and for the second player $q_A = 0.75$ and $q_B = 0.25$, with the corresponding value of the game of 1.5.

Applying the same process to our earlier example of 'paper–scissors–stone' we would find that the value of the game is zero, while the optimal mixed strategy for both players is to choose each option at random with equal frequencies of 0.33.

Table 5 Example of a zero-sum game with mixed-strategy solution

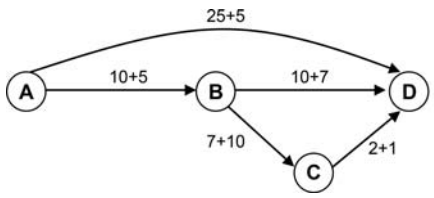
Row player ↓ Column player →	Option A	Option B
Option 1	1	3
Option 2	2	0

3.3 Simple transport game

Instead of modelling failure of network nodes, as in Section 2, here we consider an example of a transport network where links are affected, and can occur in two states: normal or failed. We therefore associate two values with each link: cost in a normal state and a cost increase in case of a failure. For example, in a small network connecting origin A with destination D, shown in Fig. 5, if link AB was affected, the normal travel time of 10 min would increase by 5 min.

Our first player is a traveller who wishes to choose a route from origin to destination that minimises his travel cost, given that that a failure may occur. Through the game-theoretic approach we can model both a situation of random failure (as a game of traveller against nature), as well as targeted attack (as a game against an imaginary evil entity). We further assume that this second player has four decision options, each equivalent to an attack on a single link, resulting in the payoffs shown in Figure 5, expressed as travel times on each route conditional upon which link has failed. Unlike in previous examples, here the row player (traveller) is a payoff-minimising (rather than maximising) player. Note that the presented approach is also suitable for more sophisticated attack options, as long as we are able to associate them with appropriate payoffs.

3.3.1 Random failure: Which route should the traveller choose if expecting a random failure? Applying the decision principles for games against nature, we can see that an optimist should select route A-B-C-D, because in most favourable circumstances, it would have lowest cost among all, equal to 19. A pessimist should go for route A-B-D, because comparing the worst-case travel time for each route, i.e. 30, 27 and 29, this one offers the least bad one. The reader can apply other decision principles to see which route will result as the best choice.



Failure → Traveller ↓	Link AD	Link AB	Link BD	Link BC	Link CD
Route A-D	30	25	25	25	25
Route A-B-D	20	25	27	20	20
Route A-B-C-D	19	24	19	29	20

Figure 5 *Example transport network with three alternative routes and the corresponding payoff table*

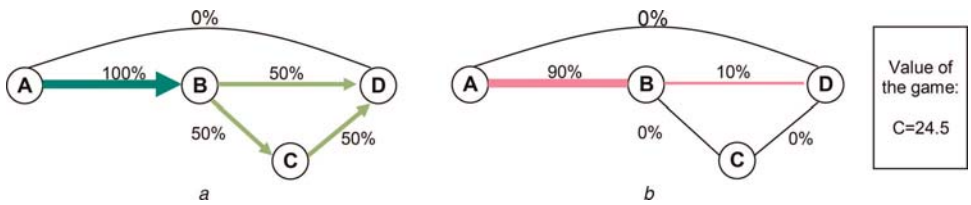


Figure 6 *Solution to the game: a – optimal routing strategy; and b – optimal attack strategy indicating critical links*

3.3.2 Targeted attack: Let us now consider the less trivial case, namely targeted attack. The traveller's game is now against an imaginary evil entity that tries to inflict maximum disruption and, unlike nature, is intelligently responding to his expectation of traveller's action.

Looking at the payoff table in Fig. 5 we first notice that for all three route options, targeting link CD would give the attacker the same or worse payoff than attacking link BC – we therefore say that strategy CD is 'dominated' by BC, hence we can exclude it from further consideration. Using a linear programming solver we then find the solution of the game, as shown in Fig. 6.

We can see that at equilibrium, the optimal strategy for the traveller is to use routes A-B-D and A-B-C-D with equal frequencies and never use route A-D. The optimal attack strategy is to target link AB nine times as often as link BD and never attack other links.

How to interpret these results? The solution identifies the worst case link attack probabilities, on the assumption that that these are what the traveller is reacting to. The value of the game at the equilibrium solution indicates the cost that the traveller can pessimistically expect. His routing strategy guarantees that no matter what the attacker's choices might be, the experienced cost will be no higher than this value. Link-use probabilities indicate the safest path choice frequency, which is highly relevant for situations such as repetitive shipments. The optimal strategy for the traveller generally involves using more than one path.

Similarly, the optimal attack strategy has disruption probabilities split between several links, which is a way to ensure that a certain loss (equal to the value of the game) can be expected to be caused, irrespective of the path selected by the traveller. Therefore the value of the game can be treated as a measure of overall network vulnerability (the higher the value the higher the cost associated with the worst-case disruption).

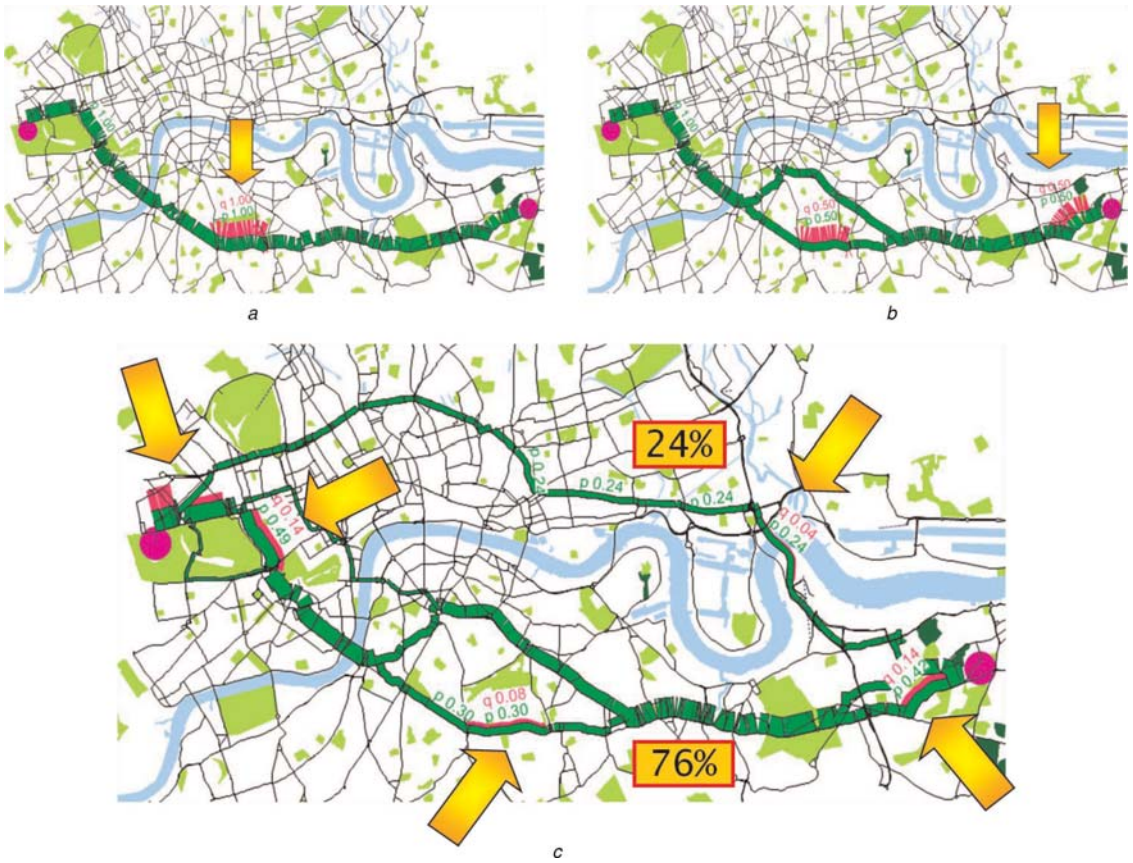


Figure 7 *a – traveller's first move and first attacked link; b – second iteration; c – equilibrium solution*

Finally, it must be noted that link failure probabilities by no means denote the links that are most likely to fail. Instead, they indicate the links that are most attractive to the attacker, hence are critical for the network under consideration.

3.4 More advanced transport games

While the problem pictured in Fig. 6 may be solved very efficiently using a standard linear program solver, it requires identifying all possible route options which in large dense networks is simply not practical. How can a game-theoretic approach be applied to large networks?

The fact that at equilibrium both players have no incentive to move to a different strategy implies that if players initially adopted sub-optimal strategies and repetitively played the same game, they would learn from outcomes of their choices, and eventually arrived at the optimal strategy. For example, if we played 'paper– scissors–stone' a sufficient number of times we would eventually learn that the optimal approach is to select each option at random a third of the time.

The equilibrium solution in a transport game can also be found using an iterative process of repetitive game playing, represented by an algorithm developed in [4]. The game starts with a traveller choosing the least-cost path through an undamaged network. In the next step, the attacker observes the path choices made by the traveller so far and chooses to fail a link, which will cause the greatest increase to the expected trip cost. Then it is traveller's turn again. He observes the link failures caused by the attacker so far, and identifies the least-cost path through (at this stage) failed network. Then it is time for attacker response … and so on. 'So far' indicates that both players keep the history of each other's previous choices through the Method of Successive Averages. The calculation is performed by a Python code interfaced with standard commercial traffic assignment software VISUM used for the path search (for details see [5]).

The sequence of the traveller's and attacker's choices, as well as resulting equilibrium solution, are illustrated in Fig. 7. The traveller's path choices are indicated as green bars, and attacker's targets as pink bars, highlighted with arrows. At the equilibrium solution we observe that the links of highest criticality are those which do not have easy alternatives, for example links in the immediate vicinity of the origin and destination, or river crossings.

Given that not all links are equally attractive to the attacker, it is natural to ask: if we could protect the critical links, where should we focus our limited defence budget? In [5] the presented model is extended by introducing a third player – the defender, whose strategy is to choose one link to protect. Unsurprisingly, defence reduces the value of the game (hence the expected loss) and leads to more homogenous distribution of risk – even though more links are typically identified as critical, fewer are extremely critical.

3.5 Further reading

The presented introduction to the application of game theory for the analysis of critical infrastructure should enable interested readers to reach to academic papers cited in here where mathematical formulations and algorithms can be found. Game theory has also been applied in the transportation context to model other aspects such as traffic assignment or introduction of motorway tolls. A useful review is available in [6]. Finally, applications in security analysis are presented in [7].

4 Summary

This paper introduced basic concepts from network theory and game theory and showed how they can be used to identify critical network components. We demonstrated that both frameworks can provide important insights into the resilience and vulnerability of transport networks by focusing on network connectivity aspects. We argued that when input data is limited, replacing unknown probabilities of undesirable events with worst-case probabilities resulting from a minimax approach is the most rational strategy that can help in planning catastrophe-preventing countermeasures.

5 References

[1] GUTFRAIND A.: 'Optimizing network topology for cascade resilience', Handbook of Optimization in Complex Networks, eds. My T. Thai, Panos M. Pardalos, Volume 58 (Springer 2012) pp. 37–59

[2] ANGELOUDIS P., FISK D.: 'Large subway systems as complex networks'. Physica A: Statistical Mechanics and its Applications, 2006, 367, pp. 553–558

[3] NORTH D.W.: 'A tutorial introduction to decision theory', *IEEE Transactions on Systems Science and Cybernetics*, 1968, **4**, (3), pp. 200–210

[4] BELL M.G.H.: 'A game theory approach to measuring the performance reliability of transport networks', Transportation Research B, 2000, 34, pp. 533–546

[5] BELL M.G.H., KANTURSKA U., SCHMÖ CKER J.D., FONZONE A.: 'Attacker–defender models and road network vulnerability', Philosophical Transactions of the Royal Society A, 2008, 366, pp. 1893–1906

[6] HOLLANDER Y., PRASHKER J.N.: 'The applicability of noncooperative game theory in transport analysis', *Transportation*, 2006, **33**, (5), pp. 481–496

[7] BIER V.M., AZAIEZ M.N.: 'Game theoretic risk analysis of security threats', 128 (Springer, 2008)

ISSN 2041-5923

Synchronisation in changing response situations: a high-level exploration of the management of resources during crisis

Christopher John Cullis

Frazer-Nash Consultancy Ltd, UK
E-mail: securityresilience@fnc.co.uk

Abstract: The Cabinet Office definition of Resilience is the, '...ability of the community, services, area or infrastructure to detect, prevent, and if necessary to withstand, handle and recover from disruptive challenges'.

In any large enterprise, response to an emergency will inevitably involve a planned reaction by several different elements of that enterprise and by other agencies outside the enterprise. In the rail industry, for example, response to an extreme weather incident could easily involve more than a dozen different organisational actors.

The plans that are invoked when an event occurs are usually detailed and complex. Most large organisations spend significant time and effort in developing these plans and in training for when they are needed. Multi-agency training and exercising are vital tools in ensuring that plans are co-ordinated.

However, it is almost impossible to develop plans with perfect coherence. There is strong evidence from a variety of domains to suggest that crucial dependencies between the various plans relevant to emergency response only come to light when an incident occurs.

This article explores the difficulty of identifying, mapping and managing critical dependencies between planned responses through the scenario of a multi-agency response to an extreme weather event with emphasis on the rail sector, and examines how dependency management can help to optimise the response.

Case study

The case study focuses on a fictitious extreme weather event, its impact on a busy transportation node that includes several elements of critical national infrastructure, and the complications encountered during the response. The power station is of key regional importance; the M12 is a motorway; all the rail are electrified; the airport is a small, but busy 'package holiday' node (Figure 1).

It is the first weekend of the October half term week. Another wet English summer has been followed by several weeks of exceptionally high rainfall. River levels are already high and the ground is sodden. Any rainfall now is likely to generate sudden rises in water levels.

There was a violent westerly gale yesterday that cleared the leaves from the trees and caused considerable damage to woodlands. However, on the Saturday morning, the motorway and trains are crowded with families heading for their half-term holiday destinations. The wind has dropped, but it starts to rain heavily around mid-morning and run-off from the waterlogged land causes the river and streams to rise rapidly. The water is full of detritus from the storm damage.

It is mid-morning. Train services are running as usual. The motorway is very crowded and movement is slow, due to the weather and a number of accidents requiring emergency services. The airport is busy but functioning well. The Environmental Agency had issued an Amber warning for the region, but quickly issues a Red warning as the rain sets in.

As the morning progresses, the heavy rain starts to cause flash-flooding. The river rises rapidly, and starts to flood

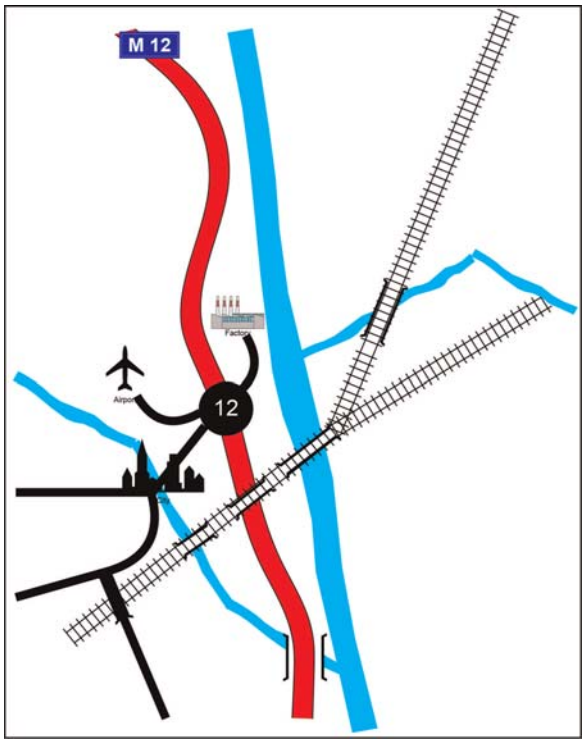


Figure 1 *Situation before the storm*

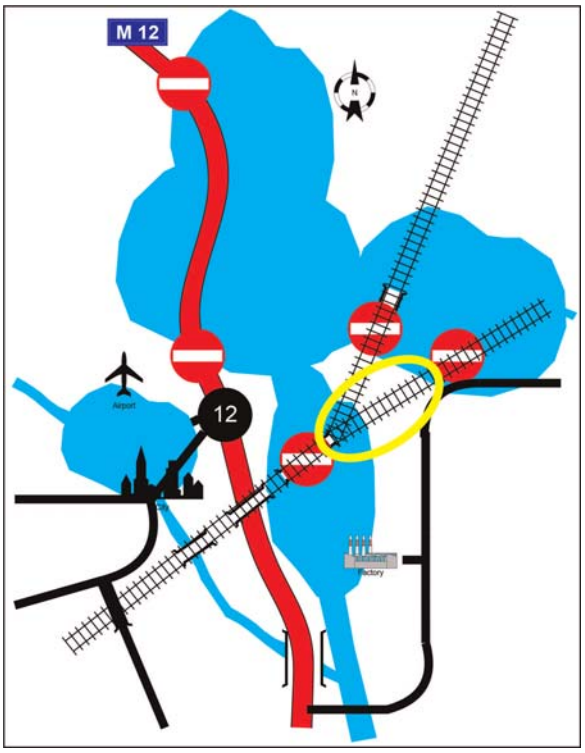


Figure 2 *Flooded incident map*

the surrounding countryside. A low section of railway line to the east of the river is flooded, behind a westbound train. Due to the sudden rise in the river towards the top of the rail/river bridge piers, the bridge ahead of the train needs a technical inspection before the train can proceed. Debris in the river begins to impact the bridges. The Rail agency deploys a Technical Response Team to assess the situation and they have to close the bridge, thus stranding the train with 500 passengers. In the meanwhile, traffic on the motorway has halted and gridlocked both ways for a 2 mile stretch north of the town's junction. This jam involves some 4000 vehicles, and around 10,000 people. The river now begins to flood across the fields, towards the motorway, and of great concern, it threatens the power station. The airport is watching with increasing concern. The situation now looks something like that shown in Figure 2.

Is this an unrealistic doomsday scenario? Not really. We have seen a shift in the UK climate in the last 6 years. 2012 saw record breaking amounts of rainfall. The months of April and June were both individually the wettest since records began in 1910. The period from April to June also saw unprecedented accumulations of rainfall for the UK. The England and Wales precipitation series shows the wettest April to June since 1766 [1]. June to July 2007 was the worst flooding in 60 years on the back of the wettest May to July since records began in 1766; June to August 2008 was one of the top 10 wettest summers since records began in 1914 for the country. November 2009 was the wettest November since records began in 1914 and there was severe flooding in northern UK, with daily rainfall of more than 200 mm in one location [2].

Flooding tends to be a regional, rather than local, issue and affects a range of different regional and national agencies and organisations; it quickly absorbs emergency services' capability and tests cross-cutting control structures, decision making, resource allocation, and so on. And it need not be weather-related: a well-targeted terrorist event and events like the East Midlands Airport crash on the M1, or a fire in the Eurotunnel, would also test planning assumptions and stress-test dependencies.

However, we are going to focus, in a very generic manner, on the small area of the stranded train, and use some simple models to show how wider events impact on the plans and response for this small event, within the emerging regional crisis.

All the agencies and other organisations have planned their response to a number of likely scenarios, based on a view of what the likely threat is, and scaled and resourced it against the output of a cost/risk/benefit analysis. These plans may have been discussed in the Local Resilience Forum, and coordination and common operating practices possibly facilitated by the National Resilience Extranet. However, planning has tended to be a little stove-piped and there has been no real investment in time to get to know counterparts and likely other players, and their thinking.

Not only is it the case that even the most detailed planning can rarely predict how events will actually unfold, but the event has also been on a greater scale than foreseen.

Figure 3 is a very simplified illustration of planning by a single agency that could be generated from a model. The agency has assessed that it will probably need no more than 3 responding units for this sector of the region and has factored this into its resource allocation. To do this, it has examined a range of likely tasks, response times against distance and then mapped this to examine resource availability. It has hopefully examined its likely need for the resources it does not own (e.g. routes, power, communications, other agencies, etc.) and will not have identified any concern here.

As the situation deteriorates and the various agencies begin to respond to an increasing number of incidents, the agency begins to have to adjust the plan. The agencies it depends on for this response have planned independently on slightly different assumptions, and are not available at the time they are needed (see the ellipse below). This is addressed under the coordination of the Police (Silver Command at this stage) as it occurs, but the need for this imposes further delay. The dependency now needs further time to respond and this begins to affect not only the teams involved, but others across the matrix of agencies. Resource need is greater than was anticipated, and although a level of provision that was anticipated as sufficient was planned in, the agency is now stretched (Figure 4).

Now look at the very simplified full picture for this small part of the response. Over at the airport, that sited its generators from a uniquely 'safety' viewpoint, without considering 'resilience', auxiliary power has now been lost as they flood. Priority therefore switches to sustaining the power station from which power has been significantly disrupted by partial flooding.

The road to the incident is now prioritised for traffic to that task. It is also barely trafficable, imposing further delay. As all the agencies spend more time on task, they become more stretched, response time becomes less and less predictable and resources delayed on task begin to run

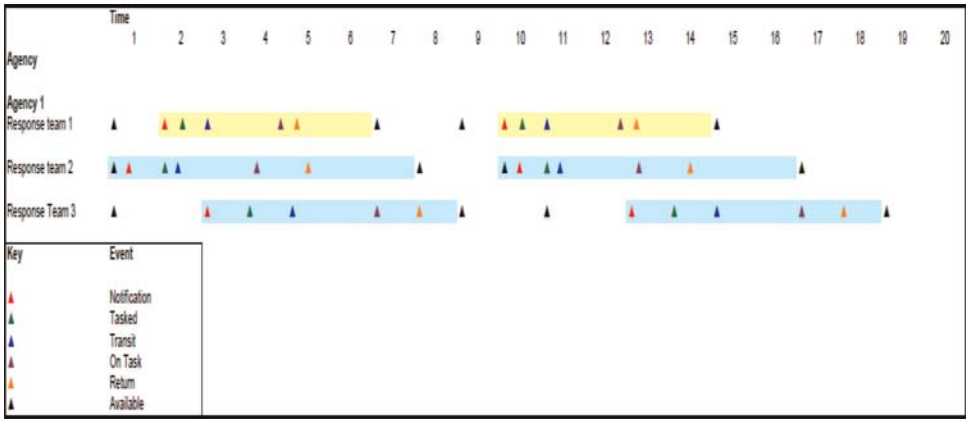


Figure 3 *Single agency planning*

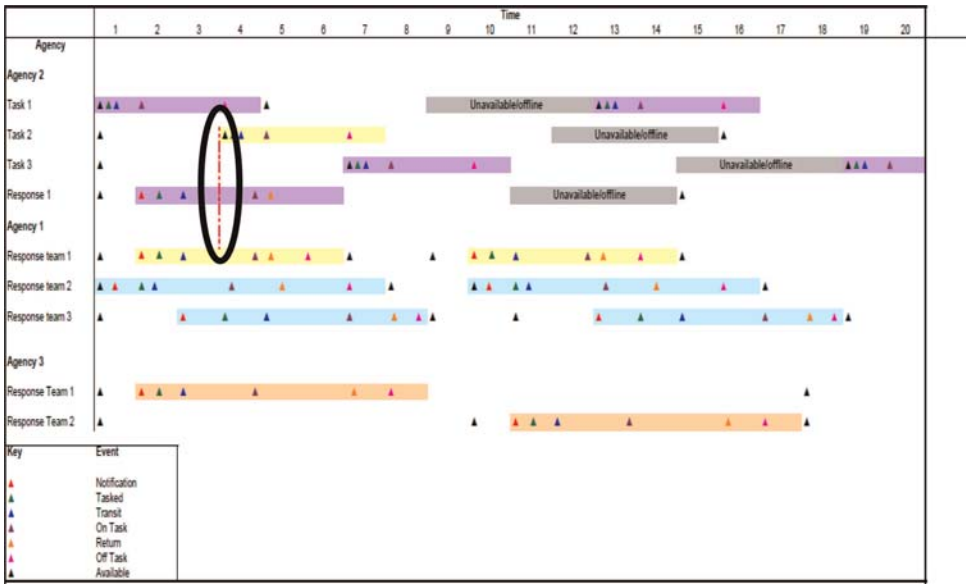


Figure 4 *Multi agency plans*

into legal issues of crew time (see the ellipses below in Figure 5).

Priorities and aim conflict: Rail's aim is business as usual; it wants to route onward its stranded passengers, and to get engineering specialists to the track and bridge. To achieve both actions, Rail needs the same road as the agencies responding to the power station and they are denied access, as they are a low priority against restoring power and saving life. What is not appreciated, however, is that loss of power also makes the passengers on the train more vulnerable, as heating, light and information are lost. Also, loss of power causes the carriage doors to unlock, thus risking loss of control of passengers. Social media spreads erroneous information to passengers faster than the train operator can counter it, and they are minded to leave the carriages, not knowing that they are doing so onto rails that may again become live.

This looks crowded already, but it is only a microcosm of the regional problem of coordination of the huge number of overstretched actors and their conflicting needs and interdependencies. There will be those that consider that no planning can possibly predict the direction a crisis will take and the range of responses it will require. Response to a crisis, however, is but management of a highly complex machine, composed of individual parts that are interconnected, interdependent and where the second and third order consequences of decisions taken on their action, are not always readily evident at first sight. A coordination system can never be perfect, but surely, a systems look at the problem, breaking it down to its component parts from end to end and tracking the consequences, should at least make it more efficient.

There are some organisations that would jointly plan, brief, rehearse, execute, and then engage in a lessons identified process. This is an intensive process for response that the civil sector cannot hope to achieve, due to the need to deliver business as usual. That said, there are some quick wins that are already in existence.

Coordination of emergency responders is achieved through Local Resilience Forums, where planning can be conducted in coordination with other agencies. The National Resilience Extranet (NRE) helps organisations to fulfil these duties by supporting the adoption of common working practices, and ensuring that key information is readily and consistently available to users through a website. This is a good start, but its success requires a collective will of all interested organisations to commit and invest in the process at the right levels. Coordination must be a routine feature of life in the planning phase, and this must happen at many levels from Policy to operations. Top level oversight and agreement is important, but we all know that the really meaningful interaction is that which takes place between those responsible for the detail. Personalities and their targets and aims need to be learned and understood in a calm preparatory phase, rather then when under the stress of the event. A systems approach at this stage will have the effect of designing resilience into the response from the outset. Trust and mutual understanding need to be developed, and this forum is a good place to start this process. Equally, people move on and individual perspectives and aims change subtly, and so regular contact is important. Doubtless, we will all claim to do all of this well already, because it is required, however, ask yourself when you last picked up the phone to, or met with, your counterparts from the Forum.

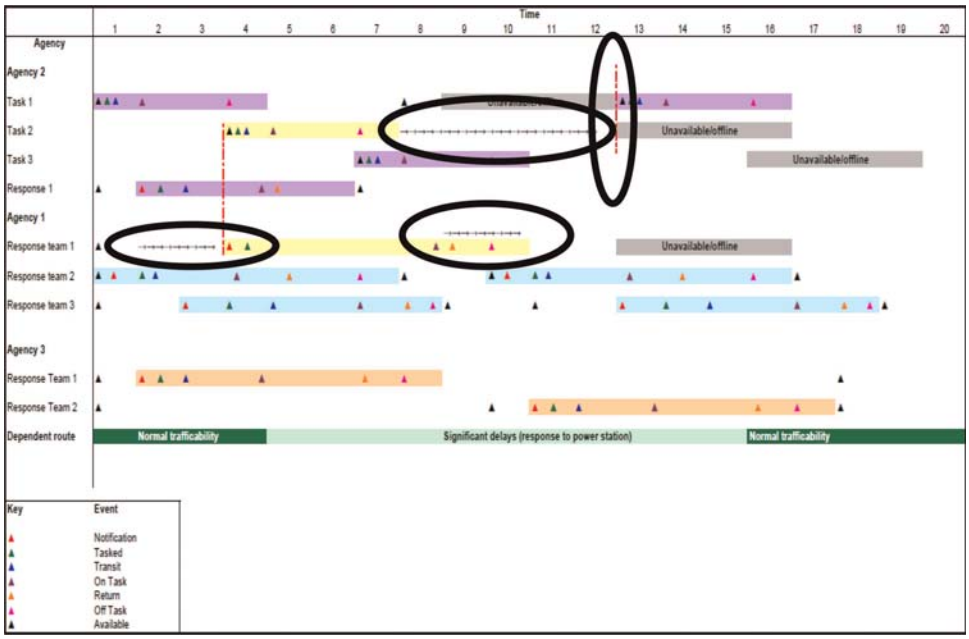


Figure 5 *The whole picture*

However thorough an individual plan, it is only when a series of individual plans are rolled out alongside each other, that the areas of overlap and conflict become really evident. It is clearly too late to be discovering what these are, when the flood waters are already lapping at the gate of the power station. Full-blown exercises are costly and rarely achievable, but time spent walking plans through on a tabletop against a scenario, under the auspices of the various organisations' policy-makers and their details people, is never wasted. It can also be a relatively cheap option and is already utilised for planned events (e.g. festivals) and single point events (e.g. high value target protection). However, it does seem to be a senior management event, and one that tends to look at simple, rather than complex, and wide ranging responses. Time and money will be well spent supporting this at a range of different levels. And this activity could under certain circumstances, even be conducted remotely if time and travel are an issue. The advantage of reviewing plans alongside each other on a tabletop is that you can get a much better insight into the mind of the other parties, and a much better mapping of the moments where all the players are likely to need access to the same resource. You can also explore the conflict lines (like control and resourcing and conflicting aims, and explore areas such as data compatibility) and adjust assumptions and plans as required. Individual organisations can then start to take account of pinch points and to identify ways of circumvention or mitigation: measures could range from the fairly neutral act of sequencing actions or decision making (where this is possible), to the very practical, but more costly, engineering in of protection or extra capability against the perceived need. This clearly needs careful cost/risk benefit analysis, based on a good understanding of the likely scenarios.

A really clear way of seeing all this conflict visually predicted, however, is through the services of simulation and modelling. Modelling allows a cheap and mostly easy way of injecting changing parameters into a situation, to see the effects of decisions and to highlight where the system starts to creak. If the input is good and the parameters realistic, then the output can be startlingly informative. The sort of situational snapshots above could be taken from a desktop computer running a model. Its use can map out the second and third order consequences of decisions and aid decision making afterwards on the ground. Simulation and modelling can, over time, help planners and decision makers gain experience and confidence without dropping a real ball in the process; this over time makes performance better on the day. Complex environmental models, for example, could be used to predict the extent of flooding, and the sort of weather conditions that would be likely to cause it, for example, and thus refine things like likely localised incidents (stranded train) route selection, likely bottlenecks, etc.

Conclusion

Regional crisis are messy, complex affairs where the direction that events actually take, cannot be predicted with any certainty, and where response plans will therefore need adjustment as the situation develops. That is accepted. That said, isolated planning and lack of interaction between the responders and other players, leads to a much less effective response that could potentially be achieved.

The Local Resilience Forum is a good starting place to develop relationships and understanding between, not only the agencies, but also the players that will be involved in the situation (Network Rail, HA, BAA, volunteer bodies, Environmental Agency, etc.), and the mutual confidence and trust to begin coordination early in a crisis. Risk-based planning, taking a multi-agency perspective, can be very effective, with appropriate account being taken of the capability and availability of the resources of each and their applicability and utility in response to different requirements.

Modelling and simulation are a significant aid to identifying pinch points and conflicting dependencies in individual plans. As can be seen above, they can deliver a very graphically visual snapshot of the interdependencies in crisis and readily map the second- and third-order consequences of decisions that are taken.

References

[1] JBA Risk Management, Met Office. UK Flooding April to July 2012 (July 2012)

[2] Department of Energy and Climate Change Report. Climate Observations, Projections and Impacts. P 28, Table 2. (2011)

ISSN 2041-5923

Understanding the impacts of multiple stakeholders on the future security of main English railway stations

Lucy Gregson-Green Andrew Dainty Lee Bosher

The School of Civil and Building Engineering, Loughborough University, Loughborough, LE11 3TU, UK
E-mail: l.e.gregson-green@lboro.ac.uk

Abstract: During the next decade, railway stations in England will be impacted by the billions of pounds being invested in current projects such as High Speed 2, Cross Rail and new refurbishment schemes to modernise and develop rail infrastructure. Railway stations are highly networked and open locations that are often crowded, which makes them particularly vulnerable to security threats. Hence, there is a clear need to identify the range of stakeholders and policies that influence the resilience of railway stations to security threats, and to understand the challenges that are inherent in addressing the legislative and operational requirements of their design. As part of an on-going research project, a state-of-the-art literature review, stakeholder analysis and mapping and interviews with key stakeholders have established critical implications for the future resilience of railway stations. Findings reveal that there is a multiplicity of stakeholders responsible for the complex operational and legal frameworks affecting major railway stations. Regardless of the interdependencies between stakeholders and their intersecting individual operational regulations and legislative requirements, there is a distinct lack of a coherent consistent and collective approach to resilience, with issues being dealt with by separate stakeholders and policies. This paper provides a current and innovative contribution to aid the understanding of the complex and interconnected forms of relationships which exemplify the station. The diverse range of stakeholders will gain an increased knowledge and appreciation of the necessity for a collaborative and integrated strategy, which is essential in both addressing the design and operation of the railway station. The findings advocate changes in institutional practices, so these interconnections are addressed now to ensure the effective assimilation of strategies are cohesive and which safeguard the resilience of railway stations for future generations.

Keywords: Railway station, stakeholders, resilience, security threats, communication

1 Introduction

The railway station is recognised as a fundamental part of the railway network in any location. The Government is investing in a modernisation programme of the railway infrastructure and is demonstrated in the investment in high profile and value projects such as the Thameslink, Crossrail and High Speed Rail 2 (HS2). However, railway stations by their nature are extremely complex systems which are freely accessible and at times crowded spaces, which make them particularly vulnerable to terrorism and other forms of crime and anti-social behaviour. Consequently, as railway stations are newly built or refurbished, there is a clear need to identify the range of stakeholders and policies that influence the resilience of railway stations to security threats, and to understand and incorporate these perspectives into the legislative and operational requirements of their design.

The railway station has numerous roles, a macro approach can be used to define the function of the railway station 'in terms of node (the connectedness with other places) and

place (possible activities around the station)' [1]. Similarly, the spatial 'urban development potentials' [2] can define the role of the railway station as an environment where 'high value activity are recognised as having a positive impact on the city' [3]. The operational complexities of the railway station are intensified with increasing size and importance of the railway station [2]. In terms of providing a public space, railway stations in England are privately owned spaces where the public have apparent free access. Subsequently, they cannot be considered as public spaces; rather they can be described as 'pseudo- public spaces' [4] or a hybrid area [5, 6]. As a consequence of these demands, the complexities, interconnected physical, legal and operational functions of the railway station and together with the concept of resilience to security threats all need to be considered by stakeholders, planners and designers in terms of a 'balance between economic, social and environmental priorities' [7].

It should be noted the emphasis of this paper is on the stakeholders within main railway stations, which are largely Network Rail operated, and not the railway network infrastructure such as tracks, signalling and bridges. Thus mirroring the UK official definition of the railway station under Section 83(1) of the Railways Act 1993

> 'any land or other property which consists of premises used as, or for the purposes of, or otherwise in connection with, a railway passenger station or railway passenger terminal (including any approaches, forecourt, cycle store or car park), whether or not the land or other property is, or the premises are, also used for other purposes' [8].

The aim of the literature and research detailed in this paper through stakeholder analysis is to map and explore the interfaces of the complex range of stakeholders which must be brought together to address the design and operational challenges inherent in both new build and retrofit schemes for railway stations in England. By using selected examples of legislative and operational complexities collected from semi-structured interviews and public documents, stakeholder understanding of the processes and dynamics which influence and regulate the current and future resilience of the railway to security is increased.

2 Resilience of the railway station to security threats

The concept of resilience has increasingly 'become embedded within. . .security and civil contingencies policy' [9] and it has gained prominence in recent years as there has been a growing acknowledgement that 'built assets can never really by future-proofed to be totally resistant' [10] against security threats. Therefore, resilience in terms of the railway station can be considered in terms of their 'embedded security and risk management [11] and 'their ability to absorb or recover from a shock or attack' [12]. To increase the resilience of the railway station to security threats, stakeholders and their interfaces, conflicts both actual and potential created by differing agendas and security vulnerabilities need to be highlighted during the (re)development stages of projects and its subsequent operation should be established at an early stage to ensure the effective assimilation of policies and strategies.

2.1 Security threats

This paper defines security threats as any human malign action from terrorist activity to low-level crime such as anti-social behaviour. The demarcation between terrorism and crime is extremely contested, given they have very diverse purposes and goals. However, it can be argued that terrorism should be perceived as a crime given both actions 'cannot be morally condoned' [13]. In recent years, the greatest threat railway stations and passenger trains have faced is being the target of a terrorist bombing [14]. Also, it is contended the infrastructure of the railway is less of a target than trains or railway stations [15]. Many larger city and international railway stations, arguably, during the rush hour periods, can be classified as 'Crowded Places. . .with a transient population often unaware of the unfamiliar environment' [16] and as such they present an appealing target for terrorist attacks [15]. Historically, in the UK when the Irish Republican Army (IRA) targeted railway stations their aims were to cause maximum fiscal and social disturbance, rather than the loss of life [14]. However, contemporary acts of terrorism against the railway station have shown that both nationally and internationally railway infrastructure offers the terrorists the opportunity to inflict mass causalities in crowded places. Therefore, the concept and fitting of resilience and security measures within the station need to be reconsidered and based on 'more proactive' [17] rather than reactive strategies. Consequently, resilience should be a holistic concept which incorporates a 'good design of infrastructure networks, effective emergency response, business continuity planning and recovery arrangements' [18]. Nonetheless, acts of terrorism are not the only threat posed to the railway station. In fact passengers and the public who use the station, are more likely to be the victims of lower level crimes rather than the victim of a terrorist attack [14].

In the past, railway stations have been portrayed by the media as places rife with crime, which strike fear and concern for passengers [19]. More recently, passengers and customers using railway stations are still expressing dissatisfaction with their perceived personal safety within the railway station [20]. The Association of Train Operating Companies (ATOC) states the continued improvement and investment in the security and policing of the railway network is critical to sustain the increase of passenger numbers [21]. Moreover, the public's fear of terrorism and crime can be reduced by 'manipulating the physical environment to improve perceptions of personal

safety' [22]. Therefore, the stakeholders of the railway station must undertake initiatives in the design stage to reduce these worries over security threats [19].

3 Stakeholders

Traditionally stakeholders are defined as 'any group or individual who can affect or is affected by the achievement of the organisation's objectives' [23]. When examining the stakeholders in the railway station, the research advocates a holistic stance which widens an established view of stakeholders beyond their relationships based on contractual and fiscal associations. Thus, stakeholders are also 'moral actors. . .relationships include social characteristics such as interdependence' [24]. Also, there will be some stakeholders who an organisation will not consider as 'legitimate in the sense they will have vastly different values and agendas' [23]. Therefore, railway stations must acknowledge illegitimate stakeholders such as terrorists and other criminals do have an interest and as such do have a stake in the organisation [23]. Hence, this relationship must be managed through specific actions such as prevention strategies and coordinated multi-agency working.

4 Methodology

This paper is based upon research conducted as part of a 3 year multidisciplinary project that is studying the future developments in the UK's energy and transport infrastructure and the resilience of these systems to natural and malicious threats and hazards. A state of the art literature and policy review of English railway stations has been conducted and augmented with semi-structured interviews and observational field notes. The qualitative data collected were specific to a main railway station, and provided a mix of stakeholder perspectives on the legal, operational and physical issues which could impact on its resilience to security threats. The 26 expert research participants took part in semi-structured interviews and were gathered by purposive sampling [25], allowing them to be chosen on the premise of their significance to, and knowledge of the research area. As part of a methodological abductive approach, the interview schedules where developed in a cyclical manner, as each interview involved the development of ideas and influenced further data collection [26]. Additionally, an established method of stakeholder analysis [23], which examines the probable contribution from stakeholders in projects and their 'power. . .and the possibility to influence them' [28], was used to understand the roles and agendas of the pivotal stakeholders in the railway station, this process can be seen in the following original Stakeholder Map. The map permits the visualisation of stakeholder's authority and impact whether in projects or day to day operations [27, 23]. The below results and discussions are an amalgamation of data collected.

5 Results and discussion

The data gathered from the interviews was evaluated using thematic analysis, proposals emerged which highlighted vulnerabilities created by the varying stakeholders responsible for the resilience of the railway station to security threats. It emerged from the analysis in order to deal the complex challenges that are inherent in addressing railway station's design, operational and legal requirements, it is essential that stakeholders undertake to increase their knowledge of such issues, in order to gain an appreciation of the necessity for a collaborative and integrated resilience strategy against security threats. The below original stakeholder map (Figure 1 Generic London main railway station stakeholder map) and discussion highlight a selection of policy disconnects and communication issues for stakeholders in the railway station, which impact on the resilience of the space to security threats.

5.1 Stakeholder map

This original stakeholder map has been generated through stakeholder analysis of the literature and policy reviews. The map established the stakeholders, who are critical to the continued existence of the railway station, and should be used to inform security and operational strategies [23]. The interviews with stakeholders have helped to validate the structure and content of the map and have also established that the map can serve several valid functions; for instance, it visually highlights the magnitude of stakeholders who have an interest in the railway station and how these interconnect and interface with each other. It proved to be a valuable research tool during the interviews as it facilitated discussion points, allowing stakeholders on the map to be categorised as follows: primary stakeholders who are impacted constructively or adversely, by a project or operations; secondary stakeholders have a transitional function and can have a key impact on the project or operations; and external stakeholders do not directly participate, yet can be impacted upon by a project or operations [28]. It should be noted that the map can be altered specifically for individual railway stations projects. Therefore, it can be used as an important visual tool during the design stage of refurbishment or new projects and operational management of railway stations, maximising decision making and ensuring all stakeholder opinions are identified [28].

5.2 Discussion

The interview data revealed a potential future impact to the resilience of security threats at the design and construction stage of building or refurbishing the railway station. Participants have contended that there are policy disconnects around section 17 of the Crime and Disorder Act 1998, concerning the involvement of police crime prevention officers at the design stages of building and refurbishment projects. Home Office police forces must be involved from the design stage of building projects, and to work with a range of responsible stakeholders to ensure

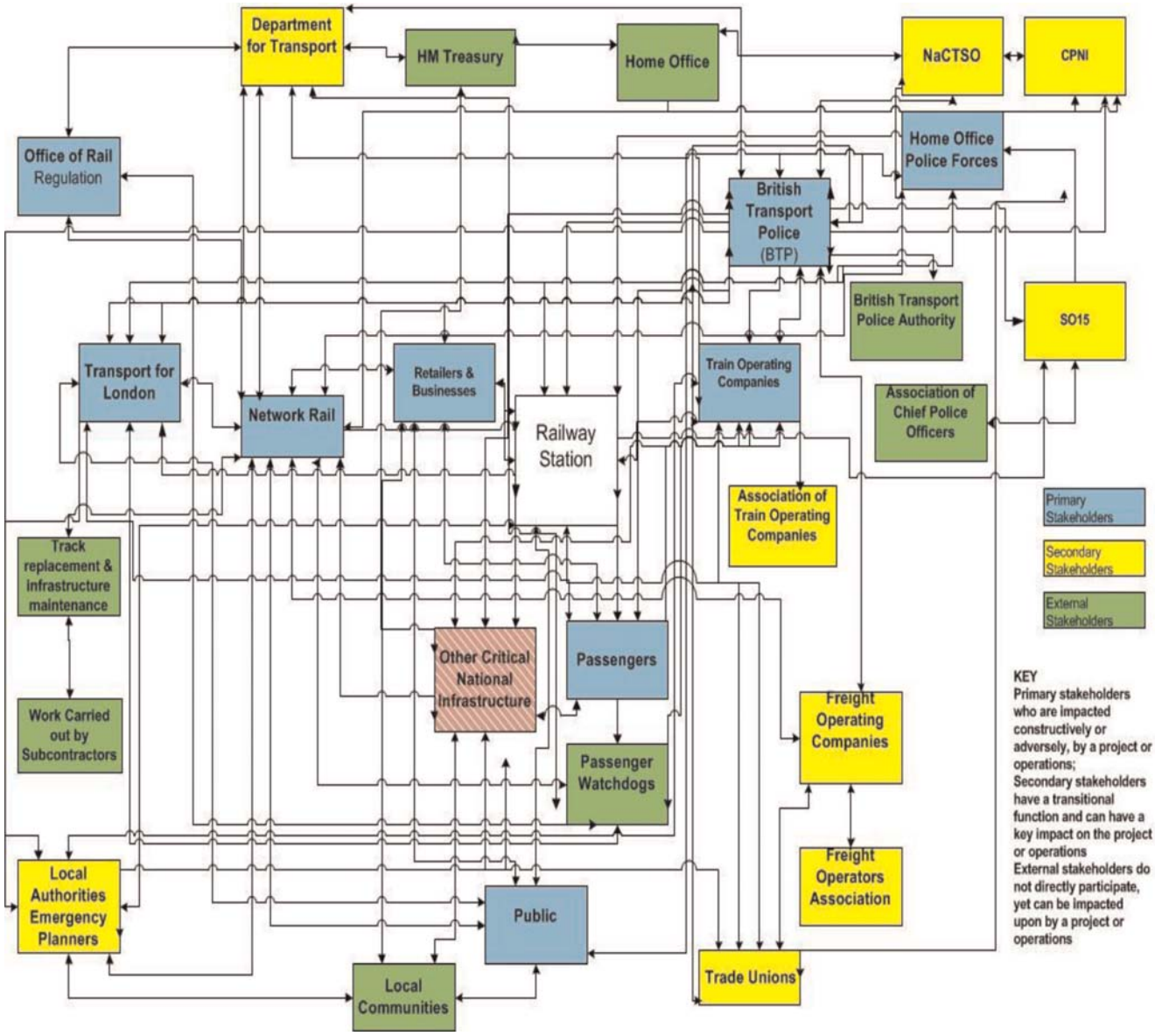


Figure 1 *Generic London main railway station stakeholder map*

crime prevention measures are considered as critical as other legislative duties in the addressing of their design. However, when railway stations are designed or refurbished, the British Transport Police (BTP) are not included in this legislation nor have any other legislation which gives them power to be consulted in the design stage of the building or redesign of such projects. Participants expressed that BTP Counter Terrorism Security Advisers (CTSA) and Principal Architectural Liaison officers (ALO) have to either rely on an informal network of industry contacts to inform them of when projects are upcoming or have to wait to be consulted by the designers. One participant stated if the BTP CTSA's/ALO's 'are asked for involvement once the first brick has been laid, then they have been involved too late on the project'. This voluntary relationship between the BTP and designers and the lack of regulation is seen to be one of hardest to manage and even harder to maintain, with security measures being perceived as an afterthought or a grudge purchase. Given the economic pressures which drive the financial costs of projects, it was felt it inevitable that there will be trade-offs around security measures, yet if inappropriate measures are fitted during the build, they will have to be retrofitted at a later date, thus having future financial implications. However, the Department for Transport (DfT) in 2012 released the 'Security In Design Of Stations' (SIDOS) guidance, to ensure security measures are designed in and the BTP are involved from the earliest stages of projects. SIDOS does make recommendations to address the issues raised above, yet participants have expressed concerns that although the document advises that CTSA/ALOs are involved at the early stages of projects, it is not a statutory requirement and therefore does not guarantee their involvement.

One area of legislation which requires adherence to and the clear communication of are the security policies and

standards in the railway station. The DfT specify the security on the railway and security standards are established and imposed through the National Railways Security Programme (NRSP), a closed access document. This document sets the day-to-day obligatory and recommended security standards for Network Rail (NR) and the Train Operating Companies (TOCs) to adhere to. NR takes the DfT's directives and communicated to their employees, which is then cascaded down to tenants. The security requirements for tenancy in main railway stations are stringent, due to their significant locations, function and capacity. This type of railway station operates to the highest level of the NRSP. It is part of the tenancy agreement that tenants will have in place a security strategy which conforms to the requirements of the NRSP, conflicts can arise when this requirement has to be dovetailed into their corporate policies, and cascaded to their employees on site. Operational participants agreed NR should manage security briefings to tenant's staff, given that the interpretation of security strategies can be watered down by managers, whether intentionally or not, and concurred corporate priorities can affect the implementation of security measures. Furthermore, the BTP frequently work with the tenants, DfT Land Security and NR to support security and awareness strategies in the station. However, many of the communications and meetings, which are held in the station, are discretionary and are instigated by individuals who are trying to improve the complexities of stakeholder interfaces and to improve the communication of security strategies. An example of a voluntary interface between stakeholders is the Police and Communities Together (PACT) meetings. These are held frequently in the station, with NR, BTP, tenants, TOCs and the public to raise awareness and issues concerning the security of the station and to agree on actions to be taken. A limitation of these meetings is the attendance in some stations is poor. Also one participant suggested these meetings are often used to air disagreements concerning others agendas. However, if there is a common issue, commercial agendas would be put to one side for the greater good of the station. These meetings are seen by NR and the BTP as key to maintain good stakeholder interfaces and communication, but it is up to the individuals involved to maintain the relationship and communications. The BTP and NR could proactively raise awareness and reiterate the relationship building and security benefits for stakeholders participating in voluntary security meetings. However, by incorporating such meetings into the mandatory NRSP it would ensure stakeholders' compulsory attendance and create structured opportunities to improve the communication of security strategies and regulation within the railway station.

A concern which was raised regarding the future resilience of the railway station are the complexities of the stakeholder interfaces and how these impact upon efficient communication between stakeholders in terms of security threats and realities. One participant acknowledged the current operational complexities of the railway station could only worsen in the future, as more stakeholders will become involved and not just those within the physical space of the railway station, but those on the margins who have an impact on the resilience of the space to security threats. Solutions need to be sought now as 'anything we do with technology is just going to be a waste of time unless we sort out the fundamental communication issues'. Therefore, key stakeholders and the Government need to urgently seek and embrace an open process of inclusive communication measures and strategies, which will facilitate the understanding of the complex stakeholder interfaces, which influence the current and future resilience of the railway station to security threats.

6 Conclusion

The main railway station in England is disparate and complex in its governance, and its current and future resilience is reliant upon an effective association between all tiers of stakeholders This paper has provided illustrations of how within the railway station there can be inconsistent and disparate approach to resilience against security threats. The stakeholder map clearly highlights the multiplicity of stakeholders responsible for the multifaceted operational and legislations of the railway station. It has briefly highlighted some of the vulnerabilities to current and future security threats, which are compounded by the complexities of managing operational interfaces between stakeholders in the railway station. The findings call for the resilience towards security threats to 'be developed in a transdisciplinary way; incorporating a wide range of stakeholders involved with the structural and non-structural approaches' [29]. It is also felt to ensure the involvement of key stakeholders in the planning and design of projects a more regulatory approach rather than guidance is required. It is too early to say whether the SIDOS guidance will be sufficient to guarantee key stakeholders are involved at the early stages of projects, thereby providing a strategically planned, defined and coordinated approach at the design stages of new build and refurbishment projects. It may be necessary for the guidance to be supported by a resolute and collaborative campaign of awareness raising, which is targeted at key 'decision-makers' illustrated on the stakeholder map. It is also vital the complex stakeholder interfaces in the day to day operations are recognised and understood in the railway station so they do not negatively impact on current and future security strategies and measures. If these issues are tackled now it will help to ensure consistent security strategies are implemented to safeguard the resilience of railway stations against a broad range of security threats for future generations.

7 Acknowledgments

The research for this paper and the 3 year project of which it forms a part of is supported by an Engineering and Physical Sciences Research Council grant (EP/I005943/1).

8 References

[1] REUSSER D., LOUKOPOULOS P., STAUFFACHER M., SCHOLZ R.: 'Classifying railway stations for sustainable transitions – balancing node and place functions', *Journal of Transport Geography*, 2008, **16**, (3), pp. 191–202

[2] ZEMP S., STAUFFACHER M., LANG D., SCHOLZ R.: 'Generic functions of railway stations – A conceptual basis for the development of common system understanding and assessment criteria', *Transport Policy*, 2011, **18**, pp. 446–455

[3] BRUINSMA F., PELS E., PRIEMUS H., RIETVELD P., VAN WEE B.: 'Railway development: Impacts on urban dynamics' (Physica-Verlag HD, Heidelberg, 2007), p. 2

[4] COOPER T., LOVE T., AND DONOVAN E.: 'Research into integrated crime prevention strategies for rail station environs. Final Report'. Office of Crime Prevention. Government of Western Australia, (2007, pp. 14) (http://www.crimeprevention.wa.gov.au/uploads/file/Research%20and%20development%20publications/research_into_integrated_crime%C2%AD_prevention_rail_stations.pdf [Accessed 17.05.11]

[5] RACO M.: 'Remaking place and securitising space: urban regeneration and the strategies, tactics and practices of policing in the UK', *Urban Studies*, 2003, **40**, (9), pp. 1869–1887

[6] NEWBURN T.: 'Criminology' (Willan Publishing, Cullompton, 2007)

[7] BANISTER D.: 'Unsustainable transport. The Transport Crisis', (Abingdon, Routledge, 2005), p. 3

[8] Legislation. Gov. UK. 'Railways Act 1993'. http://www.legislation.gov.uk/ukpga/1993/43/section/83 [Accessed 07.01.13]

[9] COAFFEE J., WOOD M., ROGERS P.: 'The everyday resilience of the city. How cities respond to terrorism and disaster' (Palgrave Macmillan, Basingstoke, 2009), p. 111

[10] BOSHER L., DAINTY A.: 'Disaster risk reduction and 'built-in' resilience: towards overarching principles for construction practice' (Blackwell Publishing Ltd., Oxford, 2007), p. 2

[11] COAFFEE J.: 'Risk, resilience, and environmentally sustainable cities', *Energy Policy*, 2008, **36**, pp. 4633–4638

[12] SCHULMAN P.R., ROE E.: 'Designing infrastructures: dilemmas of design and the reliability of critical infrastructures', *Journal of Contingencies and Crisis Management*, 2007, **15**, pp. 42–49

[13] STEVENS M.: 'What is terrorism and can psychology do anything to prevent it?', *Behavioral Sciences and the Law*, 2005, **23**, pp. 507–526

[14] POWELL J., FLETCHER D.: 'The need for developing an effective and acceptable engineering response to terrorist attacks on railway systems', *Proceedings of the Institution of Mechanical Engineers, Part F, Journal of Rail and Rapid Transit*, 2011, pp. 225–359

[15] KAPPIA J.G., FLETCHER D.I., BOSHER L.S., POWELL J.: 'The acceptability of counter-terrorism measures on urban mass transit in the UK', in BREBBIA G.A. (ed.): *Proceedings of the Fifteenth International Conference on Urban Transport and the Environment* 22–24 June, 2009, Bologna, Italy, pp. 627–636

[16] JONES M.: 'Can railway station design reduce the risk of a terrorist attack or the impact of an incident?', *Proceedings of the Institution of Mechanical Engineers, Part F, Journal of Rail and Rapid Transit*, 2011, pp. 225–351

[17] COAFFEE J., ROGERS P.: 'Rebordering the city for new security challenges: from counter-terrorism to community resilience', *Space and Policy*, 2008, **12**, (1), pp. 101–118

[18] CABINET OFFICE: 'National risk register of civil emergencies' (Cabinet Office, London, 2010), p. 5

[19] COZENS P., NEALE R., HILLIER D., WHITAKER J.: 'Tackling crime and fear of crime while waiting at Britain's Railway Stations', *Journal of Public Transport*, 2004, **7**, (3), pp. 23–41

[20] SMITH A.: 'What do passengers want at stations?', Passenger Focus (2011) http://www.passengerfocus.org.uk/news-and-publications/document-search/default.asp?go=1&topic=120&x=59&y=14 [Accessed 29.09.11]

[21] Association of Train Operating Companies 'Security Briefing', 2012, http://www.atoc.org/clientfiles/File/security2012.pdf[Accessed 03.01.13]

[22] WATERS J.: 'Perceptions of personal safety on university campuses'. Unpublished Thesis, University of Glamorgan, 2006, p. 249.

[23] FREEMAN R.E.: 'Strategic management: a stakeholder approach' (Pitman, Boston, MA, 1984)

[24] HENDRY J.: 'Economic contacts versus social relationship as a foundation for normative stakeholder theory', *Business Ethics: a European Review*, 2001, **10**, (3), pp. 223–232

[25] DENSCOMBE M.: 'The Good Research Guide. For small-scale social research projects' (Open University Press, Maidenhead, 2010, 4th edn.)

[26] DUBOIS A., GADDE L.E.: 'Systemic combining: an abductive approach to case research', *Journal of Business Research*, 2002, **55**, pp. 553–560

[27] BOURNE L., WALKER D.: 'Visualising and mapping stakeholder influence', *Management Decision*, 2005, **43**, (5), pp. 649–660

[28] JEPSON A.L., ESKEROD P.: 'Stakeholder analysis in projects: challenges in using current guidelines in the real world', *International Journal of Project Management*, 2009, **27**, pp. 335–343

[29] BOSHER L., COAFFEE J.: 'Editorial: international perspectives on urban resilience', *Proceedings of the Institution of Civil Engineers: Urban Design and Planning*, 2008, **161**, (4), pp. 145–146

PARSONS BRINCKERHOFF

A European Commission Security of Road Transport Network project team member

SeRoN

Building resilience

Helping infrastructure owners and operators improve the security of critical infrastructure

Global consultants | Designers | Engineers | Programme managers

E&T

Engineering & Technology Magazine

THE BEST OF THE DAY'S ENGINEERING NEWS

E&T Daily News Alerts.

Award-winning journalism direct to your inbox.

- Breaking news put into context
- Expert coverage on all core E&T subjects
- Informative and quick to digest

Register today for **FREE**

www.EandTmagazine.com/eNEWS

twitter @EandTmagazine

ISSN 2041-5923

Surviving catastrophic events: stimulating community resilience

Alexander H. Hay CEng PEng FICE FInstRE

Member of the Register of Security Engineers and Specialists, Director of the University of Toronto Centre for Resilience of Critical Infrastructure, Canada
E-mail: alec.hay@utoronto.ca

Abstract: Resilience is a characteristic of an operation and distinct from Protection, which pertains to assets. It is achieved through demand and dependency management to limit consequence of a catastrophic event, and so provide an assurance of operational continuity. When one analyses an operation's dependencies in context, it is possible to avoid the boundary conditions that arise between different system networks when they are analysed spatially, as assets. This necessitates a cyber, human and temporal as well as spatial definition of infrastructure. The recent City of Toronto Infrastructure Resilience Study successfully mapped the dependencies of the City operation, demonstrating a scalable application of resilience planning to a large scale complex operation. However, it also raised new questions that directly affect the City's ability to function during and recovery quickly from a catastrophic event. Demand clusters represent some degree of dependency, which can become critical during an emergency and impede even paralyse the City's ability to recover. The communities where these critical dependencies arise would seem to exhibit an imbalance in focus, ownership and infrastructure. Furthermore, an initial investigation of communities that survived catastrophic events clearly demonstrates a coincidence of these traits within a strategic framework and a consenting leadership dynamic between the communities and their higher authorities. This paper proposes a theory on community resilience that is based upon established resilience planning practice and the observed coincident traits in resilient communities, offering a way of potentially stimulating community resilience in the future.

1 Introduction

When Hurricane Sandy, reclassified as a super-storm, struck the coasts of New York and New Jersey states, it caused an estimated US$24Bn of direct damage and some US$62Bn[1] in subsequent business losses. This was sufficient to reduce the regional gross domestic product (GDP) by around one quarter of a percent[2]. Unsurprisingly, questions are being asked whether the subsequent loss in business was avoidable and much, if not most, of it would have been. This question of whether business could have survived such a catastrophic event is a question of resilience. More specifically, resilience relates to an operation and its component infrastructure, personnel and organisations, all within an operating context and environment. If one can understand the dependencies associated with a given operation, it is possible to not only determine how to make it resilient, but also how to stimulate recovery of an operation. The infrastructure applications and the efficiency benefits are significant. This paper looks at the current state of resilience practice and thinking and offers some thoughts on achieving community resilience.

[1]Official figures have not yet been released and these values are based upon news reports and published insurance losses. However, it is the general difference between direct and business losses that is significant.

[2]Taken as a percentage of GDP, however, the longer term effect is likely to result in a boost to GDP through the increase in construction. See also Bloomberg Businessweek 30 October 2012 'After Sandy's pain, there will be gain' by Matthew Philips.

2 The resilience concept

Resilience relates to the operation. It is about the ability of that operation to continue irrespective of what happens to

the components that enable the operation. These components are infrastructure, personnel and the organisation/s, not only during normal routine, but during the catastrophic event and immediately following. If an operation is resilient it will be able to adapt and absorb a catastrophic event within pre-specified performance and time tolerances and quickly recover to full[3] operating performance. The operation co-exists with other operations that describe its operating context. The operating context includes all those operations and functions that affect and are affected by the operation in question. All this exists within the operating environment, which will exist whether the operation exists or not. Fig. 1 illustrates this relationship. Those familiar with ISO31000:2009 Risk Management will recognise that the combined operating environment and operating context are the same as the Risk Context. This is not just a coincidence, because resilience is an application of risk management. As with risk management, understanding the risk is the key to making intelligent decisions about managing the risk of operational failure in a disaster.

Each of the components has a purpose, defined by the operation. Installed equipment and plant are part of the infrastructure, whereas portable equipments are simply tools drawn from the surrounding environment to be used by the personnel and the organisation. Understanding this operation, its components and its context and environment is the key to successful resilience planning. Simply put, one must understand the operation and its dependencies in order to determine how a given event will affect the operation, from which one determines vulnerabilities and mitigation strategies. The US Coast Guard in Florida once did a critical assessment of their infrastructure and operating resilience. The planners reasoned that in an emergency it was always possible to get more airframes, more fuel, change landing sites etc., but they needed a critical assurance that the aircrews would fly. There are many examples around the World where emergency personnel have failed to report for duty because their first priority was to take care of their families. Through understanding this dynamic and acting upon it, the performance of the US Coast Guard helicopter crews following Hurricane Katrina is extraordinary and far exceeded any reasonable expectation upon them. In fact, the US Coast Guard is widely considered to have been the only effective Federal agency during the disaster and their resilience approach is an interesting contrast to the standard Protection approach promoted by the Department of Homeland Security [7]. That human dependency critically defined the assurance of operational survival during and immediately following a catastrophic event, particularly pertinent for an organisation with a domestic responsibility to operate during disasters. So how does one go about understanding the operation?

[3]Practically interpreted as normally acceptable performance.

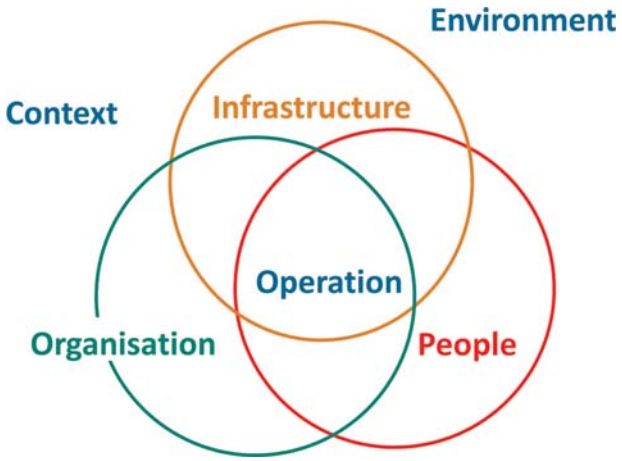


Figure 1 *An illustration of the operation, its components, environment and context*

Operations are generally made up of processes, simple and complex, single and multiple. Each process depends upon specific resources, either consumable or functional, within certain tolerances. For example, a particular aluminium smelter may consume 400 tonnes of bauxite per day under normal conditions. However, if the supply of bauxite falls below 100 tonnes per day, the value of production may no longer exceed the cost of electrical power and the operation becomes unsustainable. Similarly, the operation may not be able to sustain such a reduced supply for more than 10 days, before the operation again becomes unsustainable. One would therefore say that this particular dependency, the bauxite supply, has an operating threshold of 100 tonnes/day over 10 days. Each of the operating dependencies is analysed in this manner. Each of these dependencies is in turn analysed for what it depends upon and so on. Generally, one only analyses to the third degree of dependency, as there is typically a dispersion or concentration of consequence at around the third degree. Looked at in reverse, this dependency tree can be stressed by a particular event. The event will have an effect upon a specific resource which will have consequences for the dependent actions. In this way, one is able to understand how an event can affect the operation and quantify the consequences, as well as identify the possible mitigation measures. This approach is essentially relationship based rather than the traditional 'tombstone' approach to protection planning, which looks at nodes and their criticality. The immediate advantage to a relationship mapping approach to operating dependencies is that it avoids the 'boundary conditions'.

Simplistically, consider a commuter corridor from Etobicoke to downtown Toronto. The spatial networks will show a tram system, buses and a subway. It would appear that there is a diversity of transport means for commuters to use. From an operational perspective, these are tools that enable commuter transport and in looking at the dependencies for each, we discover that directly or

indirectly each depends upon a single electrical substation in Etobicoke. The substation feds the subway and the tram lines, as well as powering the liquid petroleum gas (LPG) compressors that refuel the buses. The indirect association and interdependency between networks and even associated systems is too often missed with a purely spatial analysis, but is brought into stark relief using operational dependencies. This is particularly relevant when one looks at the human and cyber links between the systems, such as the drivers for each of these transportation systems need to get to work somehow. Is the dependency a closed loop relationship?

Infrastructure networks are designed according to the purpose and function of that infrastructure and developed for optimum operating efficiency. Consequently, the infrastructure network for electrical power will be different to that for telecommunications or water supply. When overlaid against each other, it is almost impossible to connect the dependencies between each of the networks unless there is a direct spatial node coincidence. However, when each system is defined by its contribution to the operation where and how, the links/dependencies between the networks are defined first and the network is then built around these links. It is also important to remember that infrastructure is not just spatial, but has temporal, cyber and human dimensions too. For example, a road is built between two communities. Over time, other communities are developed around the road and its use begins to change. Not only has it influenced the development of the communities by its presence, but as its use has also changed so too the dependencies upon it. In time a new dual carriageway is built to connect the two original communities, reflecting the increased traffic demands. This does not mean that the original road can now simply be removed. It has changed in function and use. There has been a temporal change, as well as a human one. As part of its home mission, a military installation is required to continue operations through a catastrophic event and enable local recovery. Over time, the housing on and around the base has been rationalised and the priority given to soldiers or council priorities. The contracted staff who maintain the base and are responsible for emergency power generation and water supply, are now resident in the next town or even the next county. When the area is flooded and the power supply is down, who will bring the emergency power supply on line? Not so hypothetical a situation as one might think. The cyber dimension is less tangible and requires a clear understanding of how essential operating data is accessed and stored. Many organisations are increasingly relying on the internet for control of remote plant through supervisory control and data acquisition (SCADA) systems or the 'cloud' for ubiquitous access to operating data. When a global/regional event such as an ice storm interrupts several cell towers at once, the inherent redundancy in access to the 'cloud' is lost. One's dependency on the data stored in the 'cloud' will determine operational survival.

3 Resilience Practice and Management

This 'understanding' process is still being developed and the recent City of Toronto Infrastructure Resilience Study was the first time that the dependencies of a large scale complex operation were successfully mapped showing the interdependencies between infrastructure and the operational functions and services. The driver for this study was to understand how extreme weather can affect the City's operation, though it remains equally applicable to other threats and hazards, whether natural, accidental or malicious. However, the study did raise some interesting questions, specifically around the concept of demand clusters.

Resilience is managed through a balance of demand and dependency. One can not be successful with one without addressing the other. Dependency is usually managed by adaptation, redundancy and diversity. None of these is really effective unless one can manage demand such that it is proportionate to how the dependency can be managed. For example, if one operates a major supermarket and is entirely dependent upon Grid supplied electrical power, it will be difficult to achieve any cost effective diversity of supply without also managing and prioritising the energy demands by function. The essential electrical demands may be security, refrigeration and emergency lighting. Thereafter, items such as area heating/cooling and general lighting will come a close second. By using light tubes, improved insulation and compartmentalisation, essential electricity demands can be brought to within practical scales of alternative and diverse energy supplies and the capacity of Uninterruptable Power Supply units. Demand is being managed as part of a dependency management scheme. Consider Fig. 2. The normal electrical power usage (green line) for a supermarket is shown against the threshold for high user tariff. This compares with the power usage for essential operations only (blue line). If one then compares these same two power usage curves against

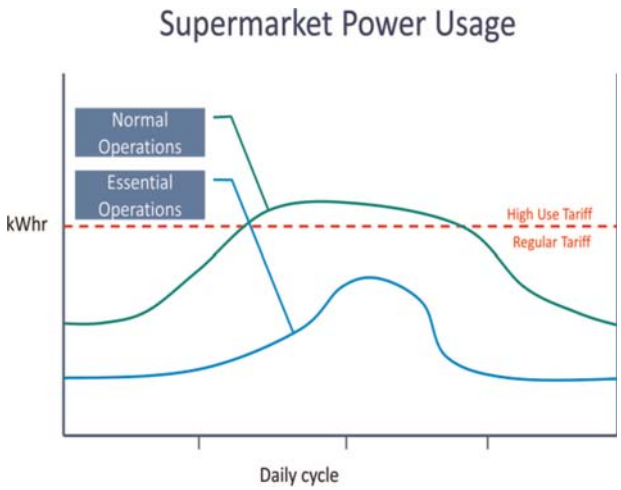


Figure 2 *Supermarket Power Usage*

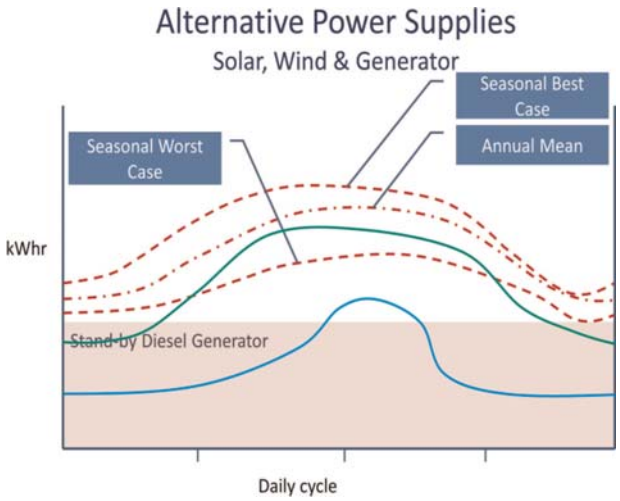


Figure 3 *Supermarket Power Usage against combined alternative power supplies*

the total available by other alternative means (diesel generator plus photovoltaic and wind turbine), it is clear that all the essential operations needs are met by these alternative sources and even, depending upon the season, the normal operating demand. Fig. 3. This means that if one can reduce the peak power demand to within the capacity of the combined alternative power sources, one has a makings of a resilient power supply. However, what happens when demand is concentrated and can affect dependency?

Generally speaking, demand is grouped in clusters around a particular focus, which could be a location or function or identity. Under normal operations each demand cluster will have a managed dependency of some sort. Within a city it would likely be on the city's corporation resources. However, during a catastrophic event the City needs to apply its available resources to manage the situation and enable rapid recovery. Often the routine dependencies of these demand clusters can be suspended for some time, because the tolerances are actually quite accommodating. However, in some cases the dependencies increase significantly during a catastrophic event and are further elevated by political imperative. These are dependency clusters. Occasionally, the dependencies on emergency resources are so significant that they can inhibit or even prevent effective City management of the incident and recovery. These are said to be critical dependency clusters. This begs the question 'How do we recognise critical dependency clusters and how do we manage them?' More to the point, how can a city prevent its neighbourhoods becoming critical dependency clusters? The same applies to counties, provinces or states and countries, though the priority interest is with cities.

4 Community resilience

Many cities are the product of planned and unplanned growth of communities that steadily incorporated smaller surrounding villages and towns. The net result is a patchwork of neighbourhoods, which have been individually developed as self-contained communities. Between these neighbourhoods are the poorly- and un-serviced areas so often used for community housing. These are known as interstitial communities and are quite often food deserts, which are areas without direct access to fresh food. Consider this research project question at the University of Toronto Centre for Resilience of Critical Infrastructure (CRCI) and the complexities become more apparent. 'How does an elderly infirm widow who lives alone on the 24th floor of a community housing block in an interstitial community feed and warm herself during a prolonged winter power outage?' During the Montreal Ice Storms, even essential power was not provided for over 7 days in some areas. She will need to descend 24 flights of stairs, walk 5–7 blocks to a grocery store and back and climb up the stairs because the lifts will not be working and the buses will not have been refilled with LPG because the compressors are run on electricity. Also, in many areas the water supply is through direct demand pumps and so potentially the same widow has no water either. The isolation of the vulnerable creates an increased dependency burden at precisely the time that it can least be afforded. Interestingly, many municipalities will respond to such a situation by using buses to set up temporary shelters, until something more suitable can be found. This will coincide with an already elevated public transport resource burden. Each expedient action moves the city corporation further into the risk funnel and eventually effective control of the incident is lost and with it the intrinsic capacity to manage its own recovery. The 'research question' is well-illustrated in New York tenements following Super-storm Sandy. How does one make a community resilient, so that the dependency burden does not increase unmanageably during a crisis? This is as far as current understanding and practice bring us, yet historical studies may provide the vital framework that allows us to project our current understanding that next bound; to stimulate the development of resilient communities.

There have been some very interesting publications in the last few years on communities destroyed by natural events and others who survived [1–3, 9, 4, 6, 7]. One of the things that come out strongly from these studies is that so much comes down to the attitude of the community. An initial review of the examples would appear to suggest that this attitude arises out of a coincidence of community focus and collective ownership with an infrastructure that supports them. That is not to say an infrastructure that provides perfect protection or one that is undeveloped, but one that is in balance with what the community does and how it sees its survival. This appears to echo the work of Jared Diamond [6] and Jane Jacobs [4], though they were not looking specifically at resilience. However, if one develops this idea a little further it would suggest that the community focus that Jane Jacobs [4] talks about is that essential awareness by the community as a whole of its members and their situation. One can generate this subliminal awareness by having a focal point in the

community that everyone must interact with at some point and so will encounter neighbours and become aware of their situation. It could be as simple as a close proximity of church, pub, general store, grocer, diner, post office and bank. This awareness stimulates multiple individual local actions that are community centric and which combined produce an uncontrolled [collective] community response to an incident. This idea of multiple local actions resonates closely with the idea of emergence, explained so well by Steven Johnson [5]. However, this alone does not deliver the essential resilience attitude. The collective attitude that gives the community awareness a focus is closely related to the community's relationship with its neighbours and the higher authority. Where there is the expectation that the higher authority, say the City, must provide during an emergency, it suggests an aspect of learned helplessness. However, where the community expects to deal with the initial mitigation of consequence itself – checking on and assisting vulnerable people etc., it suggests a sense of ownership of both their actions and influence if not control over their fate. So often, this would appear to be determined at the Parish Council or Residents Association level. Assuming that infrastructure has a purpose, the development of infrastructure within and supporting that community will either impose dependencies or vulnerabilities on the community or be in balance with its demand and operational dependencies. This includes not only the type and capacity of the water, electrical and telecommunications supplies to the community, but how much diversity and redundancy there might be in and around the community and how the infrastructure is used, both in terms of demand and interpretation. For example, some communities will interpret the construction of levees as making house construction on the flood plain a viable activity and others will see it as a mitigation measure that makes the existing community safer and no more. In effect, we are observing the same component construct around resilient communities as the fundamental concept of resilience. The difference is, that through this initial study, we would appear to have identified some of the key stimuli to developing resilience in communities [Operation] – [Infrastructure] delivering demand and dependency balanced infrastructure in and to the community, [Personnel] a focus and identity to foster community awareness, and [Organisation] ownership. What is especially interesting is that in all the cases of successfully resilient communities looked at; it was collective individual actions rather than directed and controlled actions that delivered the vital mitigation of consequences and effects, known simply as emergence. Quite how palatable this concept might be to a municipal or regional authority is not clear, when so often leadership is associated with direct control.

This theory would appear to hold for localised, such as a terrorist bombing, and global events, such as an ice storm or area flooding. An initial review of both World Trade Centre bombings [1993, 2001] in New York, the Oklahoma Murrah Federal Building bombing [1995], multiple London bombings [ten times between 1990 and 2005], the various Madrid bombings [four times between 1993 and 2006] and various other European bombings, would indicate that this essential balance and coincidence of community focus, ownership and enabling infrastructure mark out those resilient communities. The one anomaly in this initial review appears to have been the behaviour of the population in London following the 7 July 2005 bombing. Experienced in terrorist bombing campaigns by any international city standards, in this case the population of London resumed normal operations, as far as permitted, the following day with London Transport operating a normal service to all intents and purposes. This really stood out. London's responses to other terrorist events were investigated further and there appears to be a different relationship between the governing authorities and the governed. Londoners expect the authorities to get on with it, or put more succinctly they expect leadership. The leadership dimension was looked at for the other cities and it also appears to have influenced resilience. However, effective leadership alone did not correspond to rapid recovery, but instead would appear to set the conditions. In effect, it would appear to be the dominant influence in the Operating Context. There was an interesting study on the political leadership in the US following the 11 September 2001 terrorist attacks [8] and is worth reading.

This idea has also been applied to flooding, drought, wildfire and earthquakes. Indeed, the last of these would appear to provide the starkest comparison. Considering the devastating earthquakes in New Zealand [7 times in Christchurch during 2011], Haiti [Port-au-Prince/Leogane 12 January 2010] and Chile [Concepcion 27 February 2010], it is apparent that the differences in infrastructure were not significant, though the differences in death tolls and recovery were. For example, Chile experienced an 8.8 magnitude event that destroyed 500,000 buildings with a loss of 795 lives, yet Haiti experienced a 7 magnitude earthquake that destroyed 280,000 buildings with the loss of 220,000 lives, most of whom were subsequent to the event[4]. See also Time 'Chile and Haiti: A Take of Two Earthquakes' Tim Padgett 1 March 2010.. The relationship between communities and the authority only really changed in New Zealand, where there appears to be a loss of faith in geological science and the engineering professions rather than an issue over leadership. However, the most significant differences were in community ownership, which corresponded directly to their performance through the immediate aftermath and recovery. It suggests that the pre-existing community and leadership dynamics in Haiti were the single greatest cause of the high death toll and poor recovery.

5 Conclusion

This paper has outlined the concepts underpinning current practice and how this is being progressed through research

[4]Christian Science Monitor 'Chile earthquake much stronger than Haiti's but far less damage. Why?' Witte & Llana 27 February 2010.

into demand and dependency clusters and infrastructure and dependency recognition. The issue of community resilience, whether in isolation or within cities would appear under initial investigation to be an extension of the same underlying resilience concept. The theory that emerges out of this is that one can influence the development of community resilience through community focus and ownership and balanced enabling infrastructure within a reliable leadership context. More detailed research is needed to substantiate the theory, though there are several examples around the world where city planners are seeking to influence the self-reliance of neighbourhoods and communities using one or more of the measures described here. This is perhaps the best laboratory for this investigation. The applications of this theory extend beyond town and city planning, to provincial reconstruction and nation building following war and national policy development for domestic security development.

6 References

[1] RIPLEY A.: 'The Unthinkable: Who Survives when Disaster Strikes – and Why' (Three Rivers Press, 2009)

[2] HADAVI T.: 'Seven Years After Katrina, New Orleans Still Struggles to Rebuild', *Voice of America*, April 2012, **2**

[3] JONES R.: 'Slow Catastrophies: How did farms and agricultural communities survive drought in Australia', *School of History Series*, 2013

[4] JACOBS J.: 'Death and Life of Great American Cities' (Vintage, 1992)

[5] JOHNSON S.: 'Emergence: The Connected Lives of Ants, Brains, Cities and Software' (Scribner, 2002)

[6] DIAMOND J.: 'Collapse: How Societies Choose to Fail or Succeed: Revised Edition' (Penguin, 2011)

[7] FLYNN S.: 'The Edge of Disaster: Rebuilding a Resilient Nation' (Random House, 2007)

[8] BOIN A., *ET AL*.: 'The Politics of Crisis Management: Public Leadership Under Pressure' (Cambridge University Press, 2006)

[9] GOTTESDIENER L.: 'After Sandy Communities Mobilise a New Kind of Relief', *Waging NonViolence*, 3 November 2012

ISSN 2041-5923

A new approach to risk reduction in the railway industry

Eberechi Weli Michael Todinov

Department of Mechanical Engineering and Mathematical Sciences, Oxford Brookes University, Oxford, Wheatley, OX33 1HX, UK

Abstract: In view of a number of fundamental weaknesses in the existing railway industry practice for selecting effective risk-reduction measures, this paper proposes a new decision support approach based on sound, comprehensive and structured engineering principles from which risk-reduction measures are identified. The proposed new approach is based on assessing the amount of risk the risk-reduction measures remove and their cost and on selecting the combination of risk-reduction measures which removes the largest amount of risk within the specified budget. We show that this approach is superior to the traditional cost–benefit-analysis approach, based on prioritising the risks according to their cost–benefit ratio and selecting only risk-reduction measures with benefit–cost ratio greater than one.

Keywords: Railways, risk reduction, cost effectiveness, cost benefit analysis, decision support

1 Introduction

Cost–benefit studies are broadly used in the railways as a decision support tool for selecting accident reduction measures. A number of studies have exposed the inadequacies of the basic economic theories and practices in the transport industry [1].

Uncertainty in accident data have necessitated conservatism leading to an overestimation of the major accident risks on the railways. This paper presents a basic but structured approach to identifying and prioritising risk-reduction measures for specific applications without reliance on accident risk data as currently practiced. The use of expected utility theory to reduce uncertainties associated with the application of cost–benefit analysis has been proposed in [2]. Attempts at developing alternatives to cost–benefit analysis have also relied on economic theories. Currently, no practical and verifiable alternative exists for selecting risk-reduction measures. Common sense suggests that the methodology must not be entirely dependent on historical accident data. A set of accident data is always associated with particular designs and conditions and cannot be transferred to new designs and new conditions. Accident frequencies relevant to old designs and conditions cannot be extrapolated to new designs and new conditions.

One of the primary requirements for risk reduction in the railway industry and similar safety-critical industries is that measures applied to reduce risks must be verifiable. This is a major challenge for the existing methods with their critical dependence on accident risk data. Sensitivity analysis has been considered as a tool for preventing misleading results from risk analysis and subsequently from cost–benefit studies. However, sensitivity analysis methods have been shown to contribute to inaccuracies, as a result of their limitations. These limitations have been well documented in [3–9].

2 Existing cost–benefit approach for risk reduction

The choice of risk-reduction measures is currently based on analysis using historical accident data with varying levels of uncertainty. As a result, the accuracy of decisions is often in question and could potentially lead to serious incidents. Fig. 1 demonstrates the existing approach to reach decisions on risk-reduction measures for investments on a typical railway project.

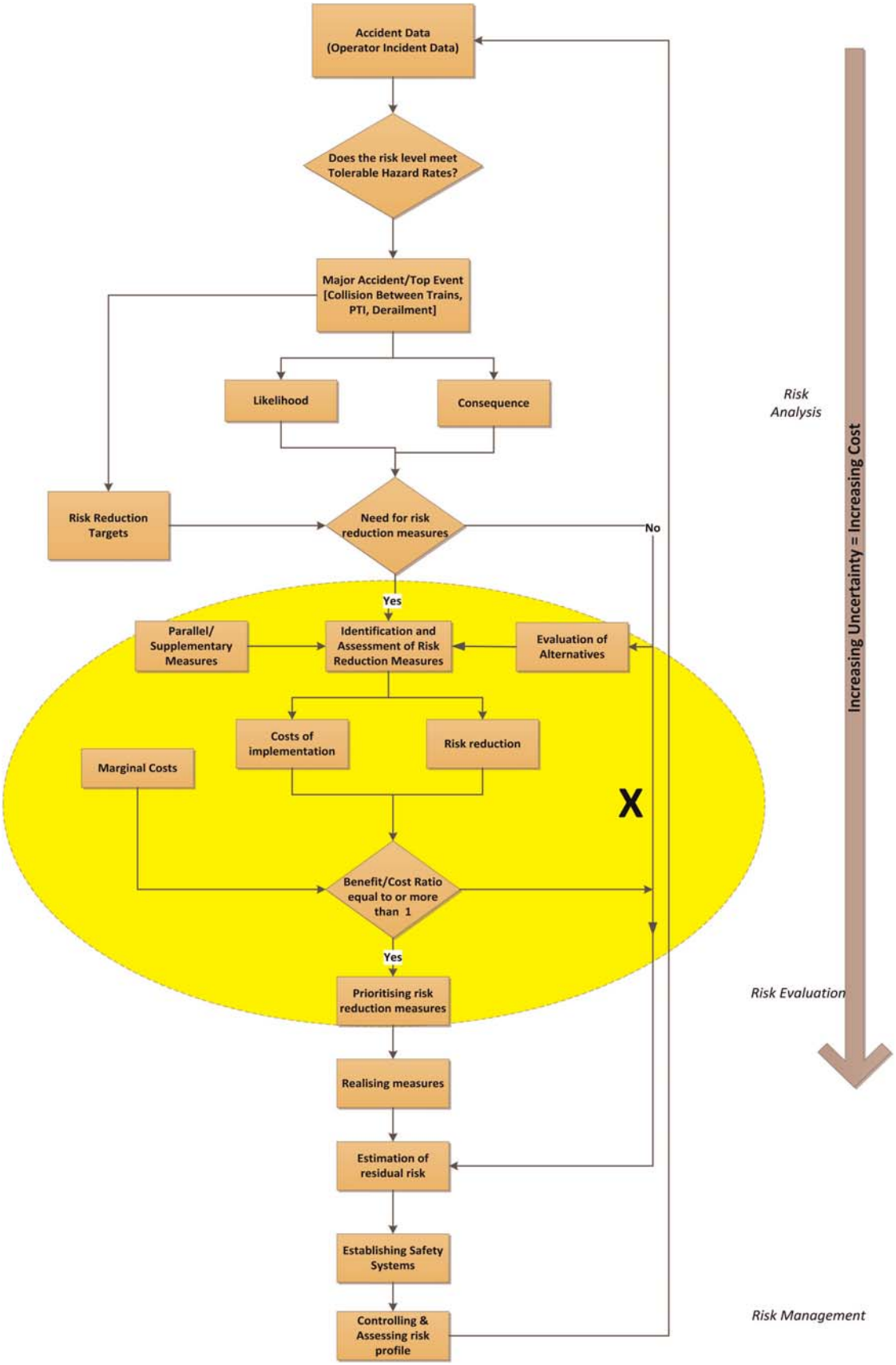


Figure 1 *Existing cost–benefit approach for risk reduction*

As can be seen from the diagram in Fig. 1, the cost–benefit approach to risk reduction is based on prioritising and selecting the risk-reduction measures according to their benefit–cost ratio. Furthermore, despite the broad use of this approach, the effectiveness of the cost–benefit approach *cannot be verified as it is heavily reliant on historical data*. The historic data *are neither representative nor reliable for actual and estimated accident costs*. Furthermore, they are not valid to new designs and new conditions. These circumstances significantly increase ambiguity in decisions, reduce the level of confidence in the selected risk management procedures and make it impossible to develop a robust case for the railway safety application. This paper focuses on the highlighted region X in Fig. 1 by introducing a well-defined and structured approach that replaces the highlighted activities. The proposed approach is based on the functional capability of the risk-reduction measures applied to specific railway risk scenarios.

3 A new decision support methodology for selecting risk-reduction measures

By using the cost-of-failure concept and the generic principles of risk-reduction concept [10], an appropriated set of generic risk-reduction principles can be formulated, specific to the railway industry, from which risk-reduction measures can be derived. These risk-reduction measures reduce the likelihood of a railway accident or the consequence in the event of the accident. Subsequently, the identified risk-reduction measures are assessed with regards to the amount of risk each of them removes and the cost of their implementation. Table 1 presents 24 key generic principles for reducing risks in the railway industry. They are referred to as 'preventive' if they reduce the likelihood of a railway accident or 'protective' if they reduce the consequences, given that the accident has occurred.

Table 1 Key risk-reduction principles (preventive and protective)

Principles for reducing the likelihood of an accident (preventive)	Principles for reducing the consequence of an accident (protective)
Built-in redundancy – e.g. braking systems, route locking systems, position detection systems	**Protective barriers –** e.g. thermal barriers as passive protective systems for risk reduction
Increased connectivity – e.g. on-board train units	**Delaying deterioration –** e.g. refurbishments
Derating -e.g. voltage alterations in track circuits for different operating temperatures	**Blocking pathways –** through which accidents escalate, e.g. platform emergency plungers
Reducing sensitivity to common cause failures – e.g. design diversity in train control systems	**Introducing weak links –** e.g. Crash Energy Management (CEM)
Minimising interfaces, complexities, weak links and connections – e.g. use of closed communications networks	**Reducing the vulnerability of passengers –** e.g. platform closed circuit television (CCTV) or one person operated-CCTV (OPO-CCTV) for stuck at door or falls between train and platform
Simplification of operations – e.g. use of software based systems to simplify application such as automating braking systems	**Use of fail-safe –** devices in isolation techniques, e.g. stick relays to de-energise track circuitry following an accident
Maintaining resistive forces and continuity of action – e.g. wheel-slip and slide control	**Emergency response –** e.g. emergency timetables, incident systems, first aid tool kit
Opposite effect modifications – e.g. stressing track	**Degraded operations –** e.g. speed restrictions
Operations frequency – e.g. introducing trains into service to reduce overcrowding	**Damage arrestors –** e.g. over-voltage or surge protection
Testing, inspections – e.g. to detect latent faults	**Exposure time –** e.g. crowd control
Reducing human errors – e.g. training of drivers, controllers, in-cab designs	**Failure indications –** e.g. Automatic Warning System
Voting systems reducing the likelihood of erroneous signals; interlocks preventing a wrong sequence of actions – e.g. controls and signalling systems	**Prediction, risk planning and troubleshooting –** e.g. use of leading and lagging indicators in risk reduction

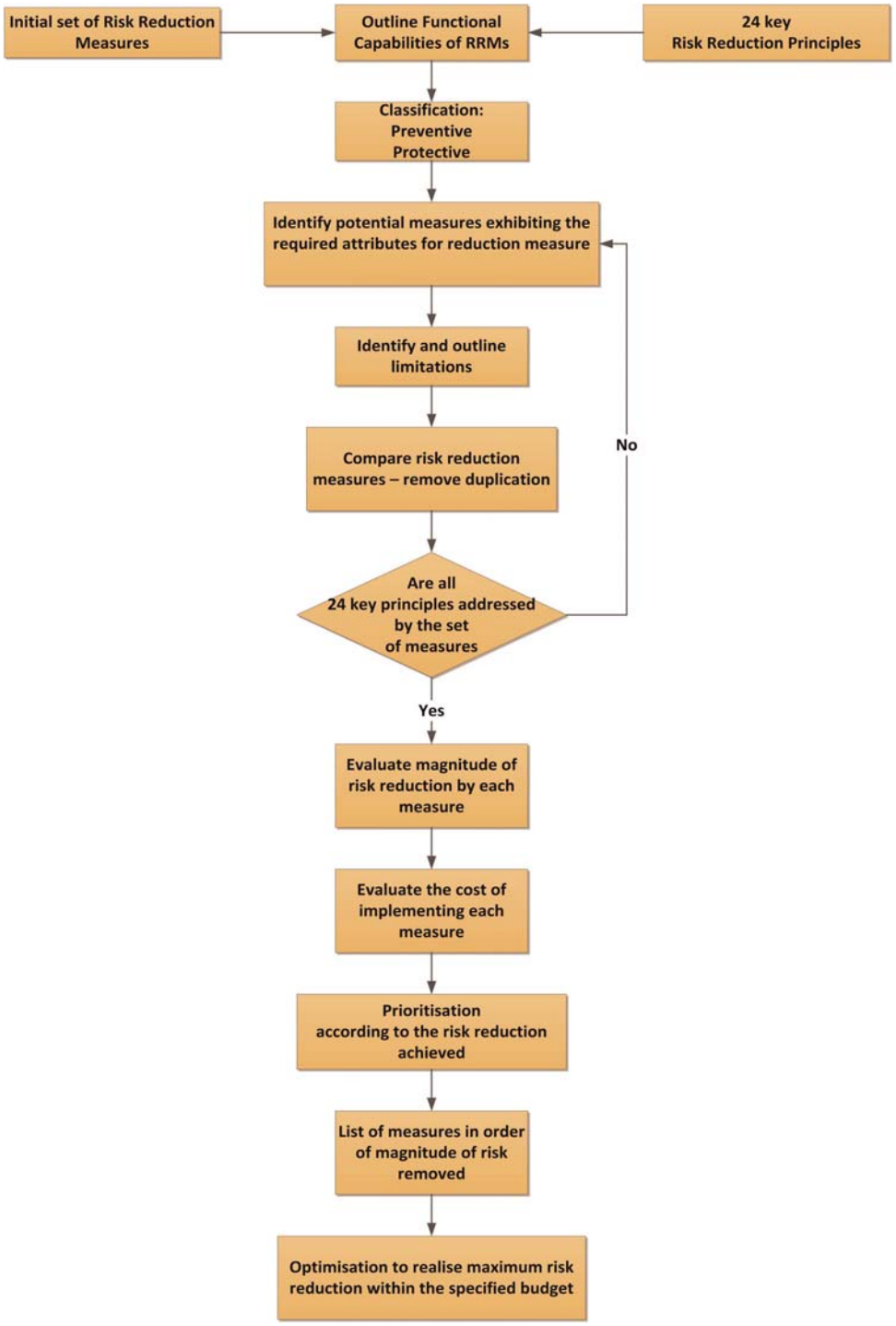


Figure 2 *A simplified new approach*

The X-region in Fig. 1 is replaced with a well-defined set of risk-reduction measures that provides the risk analyst and the decision-maker with a thorough and verifiable decision support system. Fig. 2 presents the proposed decision support technique based on the 24 key risk-reduction principles.

The process starts with assigning risk-reduction measures to the different risk contributors or risk scenarios resulting in a major railway accident. Using the 24 key risk-reduction principles, the measures are classified according to their potential for reducing the likelihood of the accident (preventive measures) or reducing the consequence given that the accident has occurred (protective measures). Each risk-reduction measure is also assessed in terms of the magnitude of removed risk and its cost of implementation. A comparative analysis informs the decision maker of risk-reduction measures with similar attributes.

Table 2 Risk-reduction measures with the associated costs and magnitude of the removed risk

Risk-reduction measure	Removed risk (in millions £)	Cost of measure (in millions £)	Benefit/cost ratio
A (One person operated CCTV)	2.0	1.60	1.25
B (Platform/passenger emergency stop plungers)	1.5	1.57	0.95
C (Gap fillers)	1.2	1.3	0.92

4 Application of the decision support methodology for cost-effective selection of risk-reduction measures

The significant advantage of the proposed approach to the existing cost–benefit approach in selecting risk-reduction measures becomes clear from the following simple example. Suppose that a budget of £3 million has been allocated for the reduction of platform train accidents, i.e. reduction in accidents involving passengers and trains at the platform area. This is a major risk which is located in the high-risk region of the risk matrix. The first risk-reduction option 'A' requires the driver to operate a CCTV monitoring of the platform. The train will not be started if there are passengers stuck at the door, fallen onto the track or fallen between train and platform. Option B includes stop plungers – wall-mounted alarm devices at specified locations/intervals within the platform area which can be operated by platform staff or passengers. Trains in the platform area will be brought to a halt by operating any of these plungers. Option C consists of gap fillers between train and platform to reduce accidents, where passengers fall between train and platform while boarding the train. The three key risk-reduction options, A, B and C have been evaluated, and the corresponding magnitudes of removed risk and costs are according to Table 2.

To remove the major risk 'platform train accident' from the high-risk region of the risk matrix, risk of minimum magnitude £2.5 millions must be removed. If the cost–benefit approach is used, the first measure, A, with benefit-to-cost ratio greater than one, will be the only selected measure. Measures B and C will be ignored because their benefit-to-cost ratios are less than one. The magnitude of the removed risk within the specified budget is £2 million – insufficient to remove the major risk from the high-risk region of the risk matrix. In addition, the magnitude of the removed risk could be significantly larger, considering the specified budget of £3 million. According to the proposed new approach, options A and C should be selected, because this is the combination whose cost is still in the allocated budget of £3 million and the magnitude of the total removed risk is the largest. Furthermore, the magnitude of removed risk according to the proposed approach will be £3.2 million, by 60% more than the amount of risk removed by using the cost–benefit approach. In addition, the amount of removed risk is sufficient to remove the major risk 'platform train accident' from the high-risk region of the risk matrix.

The next example is a real-life case, which has been an issue on all UK applications of the product 'axle counters', for over 10 years. The introduction of axle counters to achieve position detection for the trains, as a replacement for 'track circuits', is an illustration of the catastrophic effect of the cost–benefit approach which is based on historical data. Train position detection is a primary requirement for a safe operation of the railways. Due to lack of historical data regarding the frequency of failure of the axle counters, the accident history of the track circuit was used in the cost–benefit analysis. The cost–benefit analysis revealed net benefit of £500 per unit, from the use of axle counters. However, the historical data related to track circuits failed to reveal the following dangerous failure scenarios associated with the axle counters: (i) broken rails could easily be detected by the track circuit device but not by the axle counters; (ii) rail grinding wagons frequently brake axle counter heads, which makes them unsuitable for operation. These problems entail inability to detect broken tracks and, in addition, the axle counter heads have to be re-calibrated and re-installed after grinding operations. The result was increased risk levels to passengers, delays and severe operational challenges.

In this particular case, the use of the key risk-reduction principles with the proposed systematic and iterative process would have identified the inherent flaws from the application of axle counters, thereby significantly reducing overall costs.

5 Conclusions

- The proposed decision support approach is a structured and comprehensive methodology for selecting risk-reduction measures, where the likelihood of omitting a risk-reduction option is reduced to a minimum.

- The proposed decision support methodology is capable of identifying a set of risk-reduction measures characterised by a larger removed risk within a specified budget, compared to the cost–benefit approach. The proposed methodology works particularly well in the common cases, where the budgets for risk reduction are fixed and cannot be extended.

• The cost–benefit approach is based on historical accident data, which often results in a failure to detect dangerous new failure modes, if the technology or the operation conditions are changed.

• In contrast, the proposed decision support methodology does not depend on the completeness or correctness of historical accident data, which are often associated with great deal of uncertainty and have only local relevance.

• The decision support approach is an engineering application of sound risk-reduction principles that support accurate classification of the risk-reduction measures. Consequently, the proposed decision support approach provides confidence in the measures selected for risk reduction.

6 References

[1] FLYVBJERG B., HOLM M., SKAMRIS K., BUHL S.L.: 'How common and how large are Cost Overruns in Transport Infrastructure Projects', *Transport Reviews*, 2003, **23**, (1), pp. 71–88

[2] LI J., POLLARD S., KENDALL G., SOANE E., DAVIES G.: 'Optimising risk reduction: An expected utility approach for marginal risk reduction during regulatory decision making'. Reliability Engineering and System Safety, Elsevier Ltd., 2009

[3] CULLEN A.C., FREY H.C.: 'Probabilistic techniques in exposure assessment. A handbook for dealing with variability and uncertainty in models and inputs' (Plenum, New York, 1999)

[4] MENARD S.: 'Applied logistic regression analysis' (Sage Publications, Thousand Oaks, California, 1995)

[5] VON WINTERFELDT D., EDWARDS W.: 'Decision analysis and behavioural research' (Cambridge University Press, Cambridge, UK, 1986), pp. 399–405

[6] WINER B.J., BROWN D.R., MICHELS K.M.: 'Statistical principles in experimental design – third edition' (McGraw-Hill Inc., 1991)

[7] SALTELLI A., BOLADO R.: 'An alternative way to compute Fourier amplitude sensitivity test (FAST)', *Computational Statistics and Data Analysis*, 1998, **26**, (4), pp. 445–460

[8] LINDMAN H.R.: 'Analysis of variance in complex experimental designs' (W. H. Freeman & Co., 1974)

[9] NETER J., KUTNER M.H., NACHTSHEIM C.J., WASSERMAN W.: 'Applied linear statistical models – fourth edition' (McGraw-Hill, 1996)

[10] TODINOV M.T.: 'Risk-based reliability analysis and generic principles for risk reduction' (Elsevier, 2007)

ISSN 2041-5923

Black Swans means business

Atula Abeysekera

The Bow Group[*]*, United Kingdom*

Abstract: Managing its civil and national security risk is one of the greater challenges facing any government. Since 2010, the UK Government has made great strides to firm up the way it predicts and manages these risks. The Bow Group, on the other hand, feels there is a great deal more it can be doing. The government should embrace modern qualitative and quantitative methods of risk management, as it is only with robust governance structures and cutting-edge risk management solutions created by modern enterprise that the government can begin to effectively cope with that elusive beast, the black swan.

1 Introduction

'This man, on one hand, believes that he knows something, while not knowing [anything]. On the other hand, I – equally ignorant – do not believe [that I know anything].' – Socrates in Plato's The Apologies. The notion of Socratic ignorance has been an ideological theme for centuries. As the notion goes, the wise man is not he who thinks he knows everything, rather he who knows that he does not know everything.

Sometimes, from seemingly harmless causes come harmful effects. When those effects make themselves known, it seems obvious what the cause of the effect was; that the effect was always going to happen.

This paper also recommends that the UK government could do more to improve quantitative methodologies for aggregating risks across the country. Expertise needs to be gained to understand correlations between risks, stress test modelling and scenario testing. The point of this exercise would be to design, using simulated scenarios of events that could significantly impact the country, effective contingency plans to mitigate the effect of these risks. Such a programme could help the Government to more to prepare better for risks and create an opportunity to allocate resources in a more effective way.

Managing its civil and national security risk is one of the greater challenges facing any government. Since 2010, the UK Government has made great strides to firm up the way it predicts and manages these risks. The Bow Group, on the other hand, feels there is a great deal more it can be doing. As a starting point for this process of reform, the Bow Group makes the following policy recommendations:

1. Setting up of an 'Office for Risk Management'

2. Bringing in external advice to reducing group think within the government's processes

3. Encouraging an effective risk culture across government

4. Introducing best practice risk management structures from business, including the 'three lines of defence' approach

5. Introducing quantitative risk modelling strategies to both the Office for Risk Management and government departments

2 Full paper

2.1 Black Swans

Sometimes, from seemingly harmless causes come harmful effects. When those effects make themselves known, it seems obvious what the cause of the effect was; that the effect was always going to happen. According to Taleb [1], a Black Swan Event has three key characteristics:

(i) it occurs outside projected expectations (a fat tail to a distribution curve);

(ii) it carries extreme impact; and

(iii) it seems explainable after the fact.

2.2 Examples of Black Swans

2.2.1 Urban unrest (2011): An outlier: The independent Riots Communities and Victims Panel estimated that around 15,000 people were actively involved in the riots, which spread through England in the Summer of 2011 at alarming speed. The Government showed no sign of having predicted the riots and, as expected, the panel concluded that the causes of the riots were complex and were not about, or caused by, any single issue.

Extreme impact: Resources from several police forces were mobilised to deal with the crisis. Five people lost their lives and several businesses and homes were destroyed. The Riots Communities and Victims Panel estimated that the costs to the country was in the region of half a billion pounds. Given the major impact on police resources and the wider economic ramifications, few would argue that the impact of the riots was not extreme.

Explainable after the fact: The Riots Communities and Victims Panel's interim report looked at the August 2011 riots in the context of the English riots of 1981. The Panel noted that 'it is thirty years since the publication of the Scarman report. The Panel is clear that the riots in August 2011 were very different disturbances to those in 1981. However, it is a sad fact that in some respects, the underlying challenges are strikingly similar'.

2.2.2 Volcanic Ash Cloud (2010): An outlier: When a relatively small volcano, Eyjafjallajokull (let us call it 'E'), erupted in Iceland in April 2010, it ejected material as high as 20,000 feet. This event demonstrated the inherent uncertainties of volcano science. Although volcanoes are far more predictable than earthquakes, each volcano is unique, with each one having its own personality and, as such, predicting the timing and scope of their eruptions is notoriously tricky. Volcano scientists are empiricists, who rely primarily on past performance to predict future activity. However, when it came to it, their methods, which included measuring the regularity with which E had previously erupted, proved futile. Whereas the Iceland volcano produced only a small eruption at first, it seems now that the cause of the second, more serious eruption was that a vent, previously unknown to the scientists, had opened beneath a glacier on the volcano and the resulting 'soda pop' effect proved devastating. This phenomenon had previously not been observed.

Extreme impact: The eruption of E had a significant impact on the civil aviation industry, causing thousands of flights to be cancelled and the economic destruction that limited transport entails. The eruption also had an impact on the Royal Air Force (RAF), which had to temporarily suspend flight training after ash deposits were found in jet engines. Indeed, the gridlock produced by the cancellation of air travel was deemed sufficiently serious by the previous Government to require a meeting of Cabinet Office Briefing Rooms (COBRA) to be convened to discuss remedial measures.

Explainable after the fact: With hindsight, the scientific community felt that the impact of the eruption on airspace could have been predicted and better prepared for. Following the event, the UN, through the International Strategy for Disaster Reduction (UNISDR), urged European Governments to integrate volcano risk as part of their air travel policies and legislation. It is interesting that now UNISDR is now working on greater coordination and interaction between decision makers and the scientific community to achieve meaningful results in this field.

3 Fukushima power plant disaster, Japan (2011)

An outlier: When the Tsunami hit in March 2011, among several devastating effects, was the damage caused to a nuclear reactor in northern Japan. Being in an area prone to earthquakes, the Tokyo Electric Power Co., owner and operator of the Fukushima Dai-Ichi plant, had erected sea barriers at the site to protect the nuclear reactors. The waves produced by that particular earthquake were so large that the sea barriers proved 8 m too short to stop the resulting tsunami.

Extreme impact: The damage caused to the reactor in Japan resulted in the worst nuclear disaster since Chernobyl, 25 years previously. The Japan Center for Economic Research, a private think tank, has estimated the remediation costs to be in the region of $250 billion over the next 10 years. Of course, this does not take into the loss of life and injury that will ensue following the exposure of local inhabitants to massive amounts of radiation.

Explainable after the fact: Since Japan's Fukushima disaster, Électricité de France (EDF), has allocated about £200million to protect UK reactors from Black Swan events, such as a giant wave created by a collapse of an island as far away as North Africa. This is emblematic of a number of reactive measures taken by nations, including the United Kingdom, to protect themselves, post 2011 Tsunami from the human and economic cost of poor preparation.

> '…there are also unknown unknowns – the ones we don't know we do n't know. And if one looks throughout the history of our country and other free countries, it is [in this] category that tend to be the difficult ones.' (Donald Rumsfeld, 2002) [2]

3.1 The current UK Government's approach

The UK Government's civil and national security risk is currently managed by the following organs of government:

(i) In the case of managing domestic emergencies, The Civil Contingencies Secretariat ('CCS'), established in 2004 under the Civil Contingencies Act (its executive committee, the Civil Contingencies Committee ('CCC');

(ii) In the case of protecting the country's national security and other interests, the National Security Council ('NSC'), established in 2010; and

(iii) To manage emergencies, both domestic and international, 'COBR(A)', or 'Cabinet Office (CO) Briefing Room (A)', which provides a forum for the CCC to meet and a focal point for the Government's response.

For a full description of these bodies, please take a look at our recent paper, Intelligence Design: UK National Security in a Changing World [3]. We provide below, however, a brief summary of the roles of these bodies, with particular regard to their risk management capabilities.

3.1.1 Domestic emergencies: In recent years, the UK Government has made a good start on firming up its risk management architecture [4]. The Government was one of the first governments in the world to create a National Risk Register ('NRR') for domestic civil emergencies under the CCS. The NRR documents civil emergency risks over a 5 year time horizon including malicious risks (e.g. terrorism) and non-malicious risks (i.e. naturally occurring events and accidents). The National Risk Assessment ('NRA') for civil contingencies is assessed annually to ensure it reflects the latest evidence and draws upon the best available evidence and advice from subject matter experts.

The CCS Preparedness and Response Team systematically and routinely scans the short-range horizon (generally up to 6 months ahead) for potential or emerging civil domestic risks within this timeframe. CCS has links to departments, their agencies and other public bodies which are responsible for monitoring and managing civil emergency-related information. These channels have ensured that CCS receives timely notification of impending events, such events to include wide-area flooding, suspected animal disease outbreaks such as Foot and Mouth Disease, and human health threats such as the swine flu pandemic.

3.1.2 International emergencies: The NSC has adopted the methodology used in the development of the NRR. The methodology used involves thinking around the impact of an event (based on economic consequences, casualties and social or structural factors) and the likelihood of such an event occurring over a determined timeframe.

The National Security Risk Assessment ('NSRA') is reviewed every two years and uses similar concepts to the NRA process described above. It involves making judgements about the relative impact of each risk, alongside an estimation of the likelihood of each risk. The NSRA process assesses all major disruptive risks to the UK's national interest, which are of sufficient scale or impact so as to require action from the Government. Using 5–20 year horizon scanning, the NSRA identifies and analyses a full range of real and potential risks, giving the greatest weight to those with the ability to cause immediate and direct harm to the UK's territories. In general, a risk assessed as high-likelihood and high-impact would also be considered as a high priority for action. Similarly, those risks judged to be low-impact and low-likelihood would be considered lower priorities.

The management of UK risks is overseen by the Joint Committee of National Security Strategy, which is made up of 22 members (12 from the Commons and 10 from the Lords). This provides a forum to challenge conventional wisdom and to hold the organs of Government to account.

3.1.3 COBR(A): The primary function of COBR(A) is to coordinate the national response to both domestic and international emergencies. In addition, the CO engages proactively with central and local Government and other partners in preparing for such events by developing and testing response plans. The COBR(A) mechanism is triggered by emergencies which require sustained central Government coordination and support from a number of Departments and where appropriate, the devolved administrations.

3.1.4 Recent performance: Complex interdependencies in modern societies make it more likely that emergencies will require a large degree of co-ordination across Government.

The Government has made a reasonable start on this. A good example of developments to civil contingencies planning is the extensive contingency measures drawn up by the Government to prepare for extreme flooding in England: 'Project Excessive Watermark'. This was undertaken following the Pitt review of the 2007 summer floods, a Black Swan event. The tests concluded that England and Wales has the capability to respond to severe, widespread flood emergencies. On the other hand, the Government has not always been so proactive. Looking at the fuel protests of 2000 and 2012, the Government was completely underprepared for the former, and by the time the latter came along, only reactive measures had been taken by the Government, such as calling in the military, should the drivers of petrol tankers decide to stage a national strike. Ultimately the military was not required, and these preparations were time and resource consuming for COBR(A) and for Government Departments.

The lack of strategic focus resulted from a failure to be proactive and more robust architecture is needed to mitigate the effects of such occurrences. There is much to do, and the world of business and, in particular, the experiences of the financial sector, offers some useful ideas, which could lead to meaningful progress in this area.

It should be noted that at the request of the Ministry of Defence and COthe Blackett Review was established to consider 'High Impact Low Probability Risks'. The review considered the high impact low probability events from the perspective of the NRA, though recommendations will be useful for all Departments to consider.

'The Review has approached the issue with fresh thinking, considering the latest approaches to the risk management cycle. The recommendations build on existing practice, with an emphasis on refreshed thinking in a number of areas. The most notable over-arching factor in these recommendations is the repeated need for the inclusion of external experts and readiness to consider unlikely risks. Additionally, the report makes clear that behavioural matters and the role of social science in risk management needs to be enhanced [5]'.

3.2 Business approaches

Recent events such as the Financial Crisis, the BP oil spill in the Gulf of Mexico and the above-mentioned Tsunami in Japan have prompted businesses to plan for extreme events and look again at their risk architecture.

Complex businesses have often developed their own enterprise risk management frameworks to have a holistic view of risks and which would help to capture these emerging unknown–unknown risks. These frameworks employ forward-looking governance structures and quantitative techniques to assist in the decision-making process.

These organisations generally have good risk management practices for specific risks at 'business unit' level, but also have the ability to aggregate these risks across the entire organisation, sometimes applying correlation factors between risks. The ability look at interconnected risks and multiple risk exposure is increasingly important in the current environment.

There are formal and informal processes for escalating risks through the hierarchy of a business but they generally follow a 'three lines of defence' approach, as described below:

The 1st level of defence is the person who identifies the risk (whoever identifies the risk, is responsible for managing the risk);

The 2nd level of defence is a separate risk management department, headed by a senior risk officer; and

The 3rd level of defence is the Board of Directors (or appropriate governing body), supported by an independent audit function.

A risk crystallises if all three levels are breached [6].

The success of the three-level defence system depends upon good management information systems, change management control procedures, strategic planning processes and financial reporting conventions. In addition to this, most business organisations have an annual risk assessment review and material and emerging risks are subjected to extensive stress testing. Should a risk not be accounted for, a remediation plan will then be implemented to reduce the risk to the organisation.

The day-to-day analysis of risk varies in its nature across industries and jurisdictions. Some industries use probabilistic approaches such as planning for 1 in 200 year single or multiple events, while the others take a more qualitative approach. Some take a combination of both. The objective is to have the appropriate governance structure to identify these events, so that contingency plans can be initiated, if necessary, to mitigate the risk.

Most business organisations are aware of the dangers of 'group think' and they will actively seek expertise from outside the industry to formulate, or at least inform, their risk strategy. To promote this enterprise-wide risk management, most Boards are also aware of the importance of risk culture and the role it plays in identifying and escalating risks promptly through the chain of command.

These organisations generally have an experienced Chief Risk Officer who reports to a Board-level Risk Committee. The Risk Committee is generally made up of executive and non-executive directors, with an independent director as its Chairman. The external members, who come from various business disciplines, provide both independent external oversight and bring their own experience and expertise to bear. One of the key strategies for dealing with black swan events is to introduce additional resilience into the organisation so it can deal with shocks more easily, e.g. stockpiles, alternative suppliers, etc. It also means that opportunities can be exploited faster.

3.3 White Swans

The key objective for managing risks in an uncertain world is to reduce the risk of the 'unknown' risks in a cost effective way so that the 'unknown' tail becomes a more manageable phenomenon, as shown in Fig. 1 below.

An holistic governance structure and an enterprise-led risk management culture are urgently required by government to

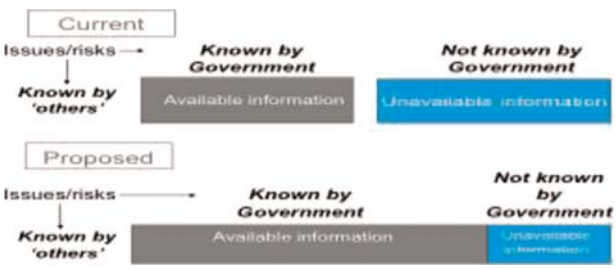


Figure 1 *High-level illustration of Bow Group proposals*

proactively manage 'unknown–unknown' risks. This can, occasionally, create an opportunity from knowledge gained. Government made a start by formulating their thinking in the Corporate Governance Good Practices Code for central Government Departments in July 2011 [7]. Unfortunately, much more needs to be done and the world of business is not a bad place to look for inspiration. We propose that the Government implement the following changes to (i) the way risk management systems are overseen and (ii) the quantitative capabilities of the UK Government in managing risk.

3.3.1 Independent oversight: The Office for Risk Management: To more proactively manage civil and national security Black Swan risks, the Government's risk assessment process needs to be challenged and overseen to a far greater extent than it is currently. Such an ambition could be fulfilled by the creation of an independent office, with external expertise. This should be adjoined to the CO.

The ORM should be chaired by a senior independent person with skills in risk management and corporate governance and experience in Government and Business. It should consist of subject matter experts representing key disciplines. The ORM's fundamental roles would be to challenge the risk management at the heart of the Government and provide an advisory role to the Prime Minister and the Cabinet.

The model for the ORM should be similar to the new Office of Budget Responsibility (OBR) created by the Coalition Government. The oversight of ORM can be by the Public Accounts Committee and the budget would be similar to that of OBR – by our estimations, a grant-aided flat cash funding allocation of £2 million per annum should be sufficient.

Within the ORM, in accordance with best practice, specialist subgroups should be created. Each sub group should be responsible for challenging Governments' risk assessments and providing independent feedback to the Prime Minister and the Cabinet. The ORM should produce an annual report on risk management performance of the Government. The sub groups can be created to broadly mirror the NSC's own sub committees such as cyber security; counter terrorism; hazards; resilience and contingencies; nuclear; emerging powers; economic; and current hot spots (Syria, Afghanistan, etc.). Following the model used in Business, the ORM should be able to instruct the CO to perform specific stress tests on predefined Black Swan events and independently assess their resilience. The ORM should also perform independent incident reviews on the activities of COBR(A).

Group think: The ORM would help to avoid 'group think' by bringing in multidisciplinary external expertise from outside of Government; a useful catalyst for encouraging outside-the-box thinking and for generating new ideas. The point was highlighted by the Science and Technology Select Committee in 2011, when they expressed concern over the exclusion of Government's Chief Scientific Adviser (GCSA) in the NRA strategy, stating: 'we consider that science should be at the heart of the NRA process and have recommended that the GSCA have greater involvement. We urge the Government to do better at embedding scientific advice and an evidence-based approach in risk assessment and policy processes before emergencies occur'.

Risk culture: One of the mandates of the ORM would be to promote and issue guidance on a new risk culture among civil servants. The culture should encourage the capture and escalation of emerging risks at grass root level from departments, their agencies and other public bodies, to better identify potential and emerging Black Swans. This could be achieved by the 'right' policies, procedures, training, remuneration and incentives to promote best practice risk behaviour and at the same time encouraging creative and entrepreneurial risk decision-making by civil servants.

3.3.2 Quantitative process changes: Three-lines of defence: We propose that the Government adapts best practice used in multinational companies where a sound risk framework should have three-lines of defence, as described above and represented in Fig. 2. From a UK Government perspective, this would look like the following.

The 1st level of defence (illustrated as the red ring in Fig. 2, above) is the Government department where the risk originated and is responsible for managing that risk. The 2nd level of defence (the white ring) is the Civil Contingencies and National Security Secretariat's efforts on risk mitigation, which would likely operate out of the CO. The 3rd level of defence (the blue ring) is the responsibility of the Prime Minister and his Cabinet, supported by the newly formed independent ORM. As with the Business approach, the risk crystallises if all three levels are breached.

Cause: Horizon scanning is a methodical way of identifying opportunities and threats that are starting to emerge. The UK's Foresight Horizon Scanning Centre, currently based at the Department of Business Innovation and Skills, is a good starting point to gather information on and quantitatively analyse emerging Black Swans. We believe

Figure 2 *The targeted approach*

that the Foresight Horizon Scanning Centre should be expanded, given its strategic importance, and moved permanently to the newly-formed ORM. This will ensure that the study of emerging risks is joined-up and coordinated centrally.

Effect: We recommend that the UK Government could do more to improve quantitative methodologies for aggregating risks across the country. Expertise needs to be gained to understand correlations between risks, stress test modelling and scenario testing. Modelling techniques used by business could contribute to a better understanding of risk interactions quantitatively.

In addition, a robust stress-testing program is needed to simulate extreme events involving UK's civil and national security risks. The point of this exercise would be to design, using simulated scenarios of events that could significantly impact the country, effective contingency plans to mitigate the effect of these risks. Such a programme could help the Government to prepare better for risks and create an opportunity to allocate resources in a more effective way.

4 Conclusions and recommendations

Managing its civil and national security risk is one of the greater challenges facing any government.

Since, 2010 the UK Government has made some strides to firm up the way it predicts and manages these risks. However, there is a great deal more it can be doing.

The world of business, and in particular, the financial world, has seen considerably more progress than the public sector in this respect. But rather than lament this point, the Government should actively seek to replicate best practice techniques in risk management, which could have an enormous value impact on both the UK's finances and the life of the nation.

As a starting point for this process of reform, we make the following policy recommendations:

1. Setting up of an Office for Risk Management (ORM). This would be structured as an enlarged base for the UK's Foresight Horizon Scanning Centre.

2. Bringing in external experts to advise the ORM, which should have the effect of reducing 'group think' within the Government's risk management processes.

3. Encouraging a more effective 'risk culture' across Government Departments by raising the level of awareness about these black swan type events, but also take additional risks in order to deliver change.

4. Introducing 'best practice' risk management structures from business, including the 'three lines of defence' approach.

5. Introducing more qualitative assessments and quantitative risk modelling strategies to both the ORM and Government Departments. These techniques are increasingly used by business and might usefully be replicated by Government in managing Black Swan risk.

It is essential that the Government acts to reform its risk management framework. The policy proposals put forward in this paper and summarised above are a pragmatic and cost-effective way of achieving meaningful results for the country. The Government must act swiftly, as what is at stake is nothing short of the life of the nation and the security of our citizens.

5 Acknowledgments

The author is grateful for the co-operation of UK Government Ministers and the support of the Risk Management community in producing this paper.

The Bow Group is a leading Think Tank based in London. Founded in 1951, the Bow Group exists to publish the research of its members, stimulate policy debate through an events programme and to provide an intellectual home to Conservatives in the United Kingdom. Although firmly housed in the Conservative family, the Bow Group does not take a corporate view and it represents all strands of Conservative opinion.

6 References

[1] TALEB, NASSIM NICHOLAS: 'The Black Swan' (Random House Publishing, 2008)

[2] US Department of Defense Briefing: transcript of then Secretary of State, Donald Rumsfeld (2002)

[3] A STRONG BRITAIN IN AN AGE OF UNCERTAINTY: 'The UK National Security Strategy'. (October 2010: The United Kingdom Stationary Office (2010)

[4] GLOBAL RISKS 2012: 7th Edition: World Economic Forum (2012)

[5] Blackett Review of High Impact Low Probability Risks, Department of Business, Innovation and Skills (2011)

[6] 'The Three Lines of Defense in Effective Risk Management and Control' Institute of Internal Auditors January 2013

[7] Corporate Governance Code for Central Government departments, HM Treasury (2011)

ISSN 2041-5923

Understanding how tunnel ventilation analysis decreases risk and increases resilience

Kate Hunt Chermac Rolle

Parsons Brinckerhoff, Westbrook Mills, Godalming, Surrey, GU7 2AZ, UK
E-mail: huntk@pbworld.com, rollec@pbworld.com

Abstract: Understanding and being able to predict the aerodynamic and thermodynamic behaviour in transit tunnels is vital for two reasons. It promotes the reduction of the risks or consequences of accidents and deliberate acts of terrorism; and increases resilience by aiding the provision of reasonable thermal comfort within an infrastructure which uses increasingly energy intensive train systems and operations against a backdrop of increasing ambient temperatures. This paper shows how, with a detailed understanding of the system's energy balance, the engineer can use a combination of one-dimensional and three-dimensional thermal and airflow analysis techniques, along with passenger evacuation modelling, to optimise the design of the system. The subject is vast however and so this paper can only briefly introduce each topic. The principles introduced are also applicable to other infrastructure such as road and cable tunnels, car parks, buildings and stadia.

Keywords: Ventilation, aerodynamic, thermodynamic, egress, simulation

1 Reducing the risk from fires and deliberate acts

Ventilation systems are very commonly used for the control of smoke during a fire or similar incident. A well-designed system can significantly reduce the risk to human life during such incidents. Controlling the smoke is important in allowing passengers sufficient time to evacuate to a place of relative safety. If a major fire were to occur, without smoke control the confined nature of underground spaces could result in a huge loss of life from persons becoming incapacitated before they can evacuate. Although this may be an extremely infrequent event, such large losses of life are not acceptable to society. With ever-increasing improvements in the fire safety of materials, coupled with more rigorous operating procedures, major fire incidents are thankfully becoming rarer occurrences. The same ventilation system might also allow better access for fire fighters to control the fire thus improving asset protection. For designers, asset protection usually takes a lower priority to supporting emergency evacuation. The following sections give an overview of how ventilation and passenger flow analysis can be used to optimise the system's design.

1.1 One-dimensional techniques

Having established or agreed a credible design fire scenario and associated heat (and smoke) release curve, it is usually required to undertake some analysis to determine whether forced ventilation is required and, if so, what system and capacity is needed. In most transit systems, reference to common international standards and guidance such as NFPA130 [1] and simple inspection of the tunnel network is sufficient to conclude whether forced ventilation is required. Next, the designer must determine the manner in which the ventilation system will be used to support the evacuation of the tunnel or station.

For underground stations and shorter tunnels, ventilation systems may be adopted that exhaust the smoke from ceiling level allowing a tenable environment for evacuation below. This is not normally practicable in longer tunnels and hence the most common form of smoke control is to

provide sufficient airflow to prevent backlayering of smoke (that is, to prevent smoke from travelling in the opposite direction to that which is desired). The velocity required to achieve this (the 'critical velocity') can be conveniently calculated using common empirical formulae. Such formulae are presented in the documentation for the Subway Environment Simulation program (SES) [2], which has been extensively validated over a period of almost 40 years. The critical velocity depends on the tunnel gradient, the relative sizes of the train and tunnel and the design fire's heat release rate.

The SES program is a one-dimensional modelling tool with the ability to simulate very complex tunnel networks, as long as the flow is fully mixed and moving as a bulk flow in the forward and backward direction. The designer can develop a computer model of a proposed transit system and use SES to conduct short-term fire analyses of agreed design scenarios. Depending on the complexity of the tunnel network, developing the base dataset might take between a week and several weeks but the subsequent simulations can be undertaken very quickly (from minutes to a few hours). The results show whether critical velocity is met at the fire location and, therefore, whether the fan capacity installed is sufficient to keep the tunnel upstream of the fire smoke-free for evacuating passengers. It is important to note that the SES program is a design tool: it does not determine the ventilation system capacity required, rather it confirms the effectiveness of the ventilation capacity selected by the designer.

Fig. 1 below shows the results of a typical fire simulation, in the form of a network diagram with steady-state air flows at all locations in the network. Close inspection shows a velocity of 3.8 m/s at the fire location which, in this case, is in excess of the critical velocity. Therefore, the tunnel to the left of the fire remains smoke-free. The case also shows the impact of opening cross-passage doors between the incident and non-incident tunnel. The flows through the open cross-passages are all towards the incident tunnel and so the other tunnel is also maintained smoke-free.

Using a series of iterations of the fire analysis for the (many) design scenarios, the designer can optimise the capacity of the ventilation system and determine the impact of losing critical items of equipment. Depending on the level of safety (or Safety Integrity Level – SIL) required by the client, the likely maintenance regime and other operational factors, the designer may recommend a certain level of redundancy (standby capacity) in the system to reduce risk and/or maintain system resilience. The designer may also conduct further simulations to find alternative ventilation responses that will satisfy the required safety level using a lesser level of system redundancy.

For complex geometries, where the flow patterns are predominantly three-dimensional, more complex computational fluid dynamics (CFD) techniques can be used. CFD analyses would generally take longer to conduct than a one-dimensional analysis, with simulation time in the order of days of simulation time compared to hours of simulation with SES. CFD techniques are discussed in the next section.

1.2 Reducing the risk from fires – CFD techniques

The one-dimensional techniques described above cannot be used for complex geometries such as large, open stations, enlarged tunnel sections, car parks and other similar areas. In these large, open geometries, very complex three-dimensional flow patterns exist. Therefore, the assumption that the flow can be approximated to a slug of air moving 'forwards' or 'backwards' would be wholly wrong and inaccurate. In these cases, three-dimensional analyses are needed. Several computer codes are available to the designer, including Fire Dynamics Simulator (FDS), FLUENT and the like. Each of these programs has its

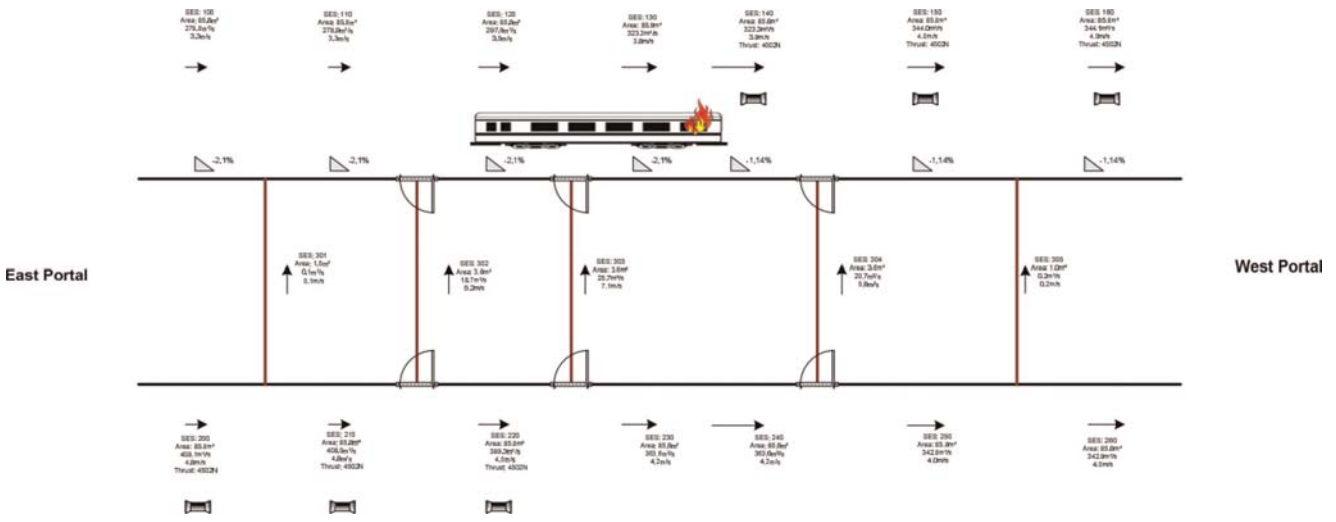


Figure 1 *One-dimensional smoke control results*

own limitations and the user must be fully conversant with the limitations of the software selected and the physical processes being modelled. CFD techniques are commonly applied to transient scenarios, such as the development of a fire or smoke over the critical evacuation period, but they can be used to determine steady-state conditions as well.

The development of a CFD simulation model is a significant undertaking and commonly takes several days to build, even for a relatively modest, straightforward geometry. Similarly, each scenario to be assessed takes a number of days to compute. In order to limit the number of cells to be computed, it is common practice to construct models of part of the network of interest and to use one-dimensional modelling to provide suitable boundary conditions, to apply representative of conditions prevailing in the remainder of the network at the start of the simulation.

Like the SES program, CFD analyses do not predict the amount of ventilation needed, they are only able to determine the outcome of using the ventilation response defined by the designer. If a scenario is considered unacceptable, the designer can alter the geometry to include, for example, smoke curtains at strategic locations or to optimise the height of a smoke reservoir in order to improve smoke control within the station. These alterations can greatly influence the architectural features of the station design. Although usually more costly than one-dimensional modelling, the use of CFD techniques can generate substantial risk reduction and associated capital cost savings when carried out early in the design process.

Figs. 2 and 3 show the results from two identical fire incidents. The plots are taken at the same instant in time; the fire ignition time and development are identical and the only difference between the two simulations is the height of the smoke curtain downstand adjacent to the train. The plot shows the light extinguishing coefficient alpha (which effectively indicates the visibility distance). In each plot, the areas in red are equivalent to a visibility distance of less than 10 m, while dark blue areas have much greater visibility. A visibility distance of less than 10 m is commonly considered 'untenable', since it would be extremely difficult to find an exit or even a solid surface such as a wall in such limited visibility. The results show clearly that the smoke is contained more effectively when the deeper smoke curtain is employed.

2 Increasing resilience to natural phenomena

Even under the moderate emissions scenarios being developed by the Meteorological Office, tangible warming of the climate is predicted in the next 30–50 years. In addition, increased weather variability is predicted with more frequent and longer duration heat wave events.

Increased temperatures above ground can be expected to warm the environment below ground to some extent. Mitigation of the external climate through energy efficiency of the train and train operations has a major role to play in managing this increase, but the additional crowding and service demands being experienced by many cities may

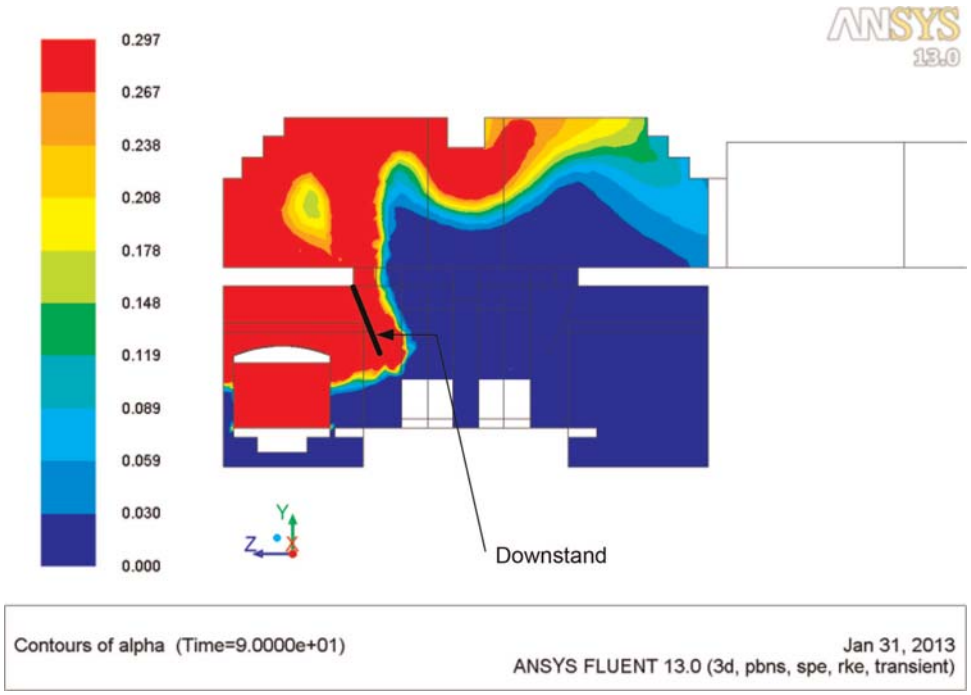


Figure 2 *Smoke movement with downstand to 2.4 m above platform level*

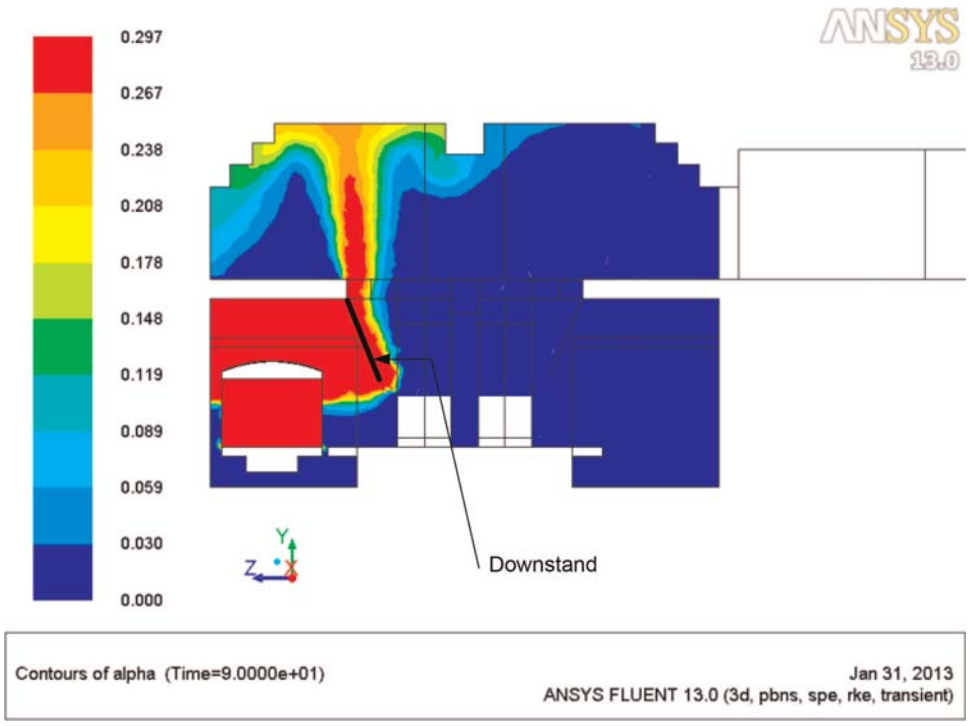


Figure 3 *Smoke plume with downstand to 2.1 m above platform level*

eclipse these opportunities, leading to warming of the tunnel network.

2.1 Understanding the system energy balance

In all modern transit systems, a balance has to be established between the energy demands of moving trains through the tunnel network and the thermal safety and comfort demands of the travelling public. In most systems, the train operations are the major source of heat. The train operations have two major facets: the energy efficiency of the train and its traction technology and the service intensity.

Advances in traction systems and regenerative braking have provided significant improvements in energy efficiency over the last 40 years. However, increased requirements for crash worthiness, increased passenger demand, increased train frequency and the need for reduced journey times and increased demand for comfort and saloon cooling collectively result in major increases in energy usage.

All the excess energy (whether from the inefficiency in the propulsion systems, from losses in the traction power system or from auxiliary loads) ultimately degrades into heat and this heat is transferred to the tunnels.

2.2 Using analysis to improve resilience to thermal change

Using the SES program, the designer can develop an analytical model of the transit system and then assess the thermal performance of the trains as they move through the system. The designer can vary the acceleration, speed and braking profiles of the trains, as well as the thermal storage characteristics of the braking system in order to determine the temperatures at all points through the network – both at stations or in the tunnels themselves. The SES program determines the thermal conditions resulting from operations over a long period of time, typically 30 years and so it can be used to determine the likely impact of progressively warming ambient conditions, perhaps due to climate change.

For new-build projects, the SES program can be used to determine robust predictions of long-term temperature within the tunnels under the predicted train operations. Where temperatures are expected to be unacceptable, the designer can investigate the likely benefit of including passive ventilation measures, such as air exchange shafts (commonly known as draught relief shafts). Fig. 4 shows such an example. Here, we can see the temperature predictions for a long rail tunnel (over 10 km long) both with and without draught relief shafts at intervals along it.

Constructing air exchange shafts may be considered excessive but if there is also a need for forced ventilation (as typically there might be where smoke control is required), then the air exchange provision can be incorporated for a relatively modest capital cost.

However, using the SES program, the designer can also determine just what energy savings might be available to

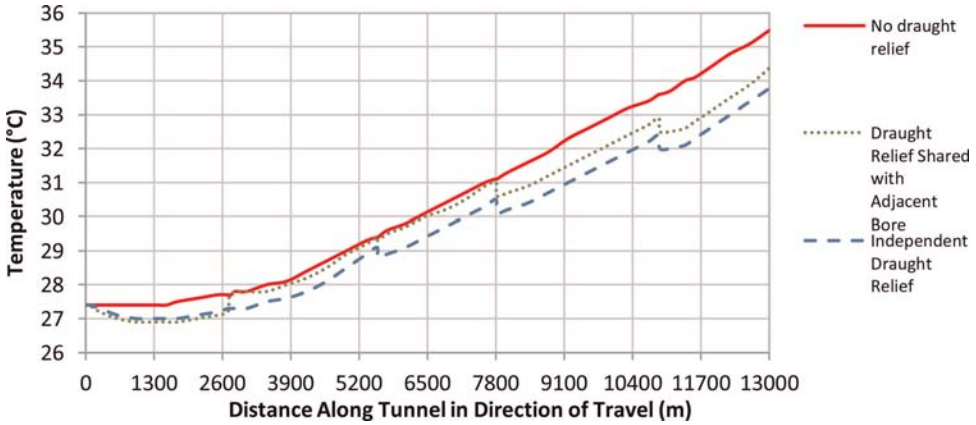


Figure 4 *Impact of air exchange shafts on tunnel temperatures*

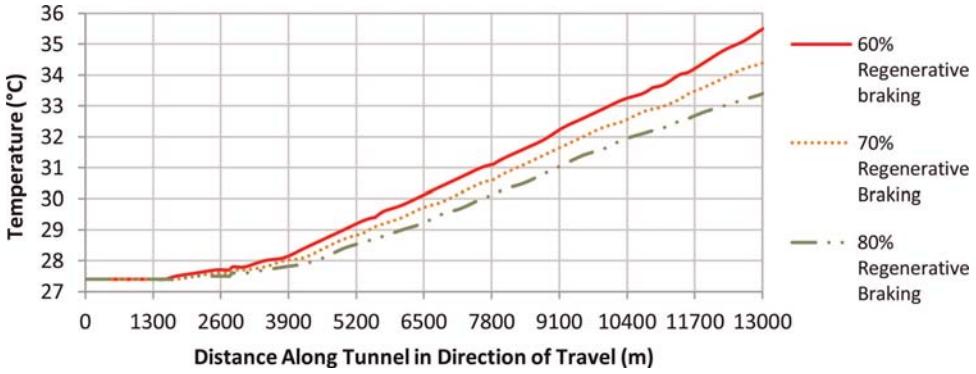


Figure 5 *Impact of regenerative braking on tunnel temperatures*

owner/operators for both new-build and existing transit systems, for example, by introducing coasting if journey times can be relaxed, by employing regenerative braking technology (if sufficient line receptivity is likely to be available) or by renovating ventilation assets to provide enhanced cooling to allow an increase in services. Fig. 5 shows, for example, the impact of incorporating increased regenerative braking into a transit system. Various levels of regeneration are considered in order to establish the value (in terms of energy saving) of the technology.

Clearly, the reduction in tunnel temperatures can only be realised if the line has sufficient receptivity (that is, trains demanding energy at the same time as others are braking), although high line receptivity is a common feature of many closely spaced metro-style networks.

3 Using passenger flow analysis to improve system resilience

Like the one-dimensional and CFD analyses described previously passenger flow analyses can be used to optimise the station layout to improve passenger movements and egress. By describing and analysing a range of scenarios and station layouts, the designer can improve the station's resilience to many potential scenarios including fire, unavailability of normal circulation routes, variations in way-finding and the like.

Passenger flow analysis can be particularly useful to determine the egress times for complex geometries or where passenger escape routes merge in order to assess the level of queuing that might result and the impact this might have on platform clearance times. Similarly, the impact of differing station layouts can be assessed well before construction begins. For example, Figs. 6 and 7 show the effect on passenger crowding of extending a station by one platform and changing the over bridges between platforms to a more modern concourse arrangement. In these figures, the dark blue colour shows passengers using that particular floor area but with little crowding. The increasingly vivid colours indicate increasing levels of passenger crowding in a particular time interval (expressed as passengers per square metre).

In Fig. 6, we see that the platforms are relatively uncrowded but that crowding occurs on the over bridges. In Fig. 7, the modern concourse arrangement mitigates crowding at the upper level. However, moving the escalators closer together has increased platform crowding at the foot of the escalators, which may have a detrimental

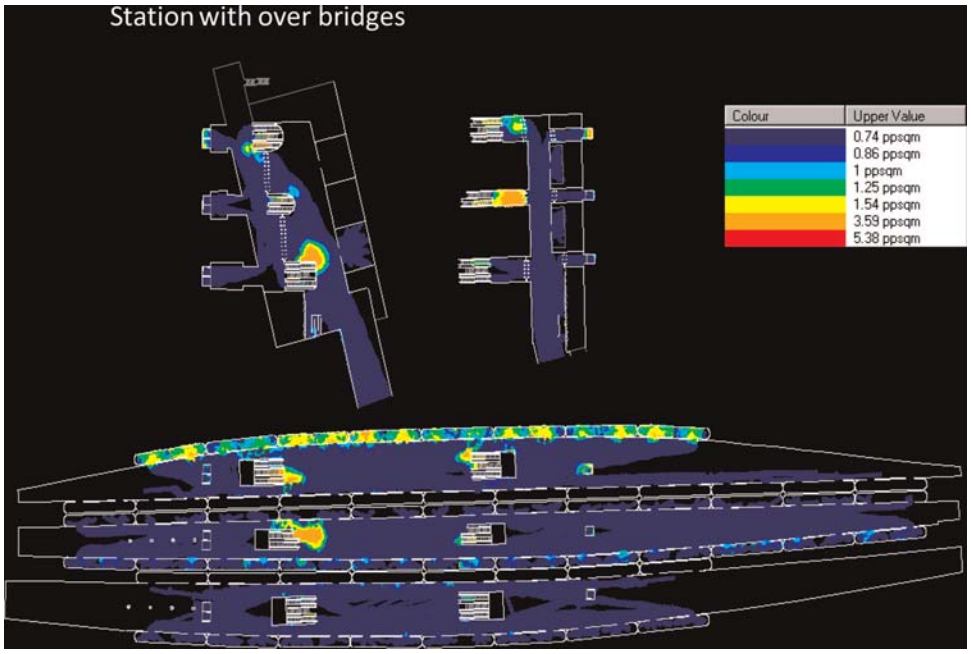


Figure 6 *Station suffering from crowding on the over bridges*

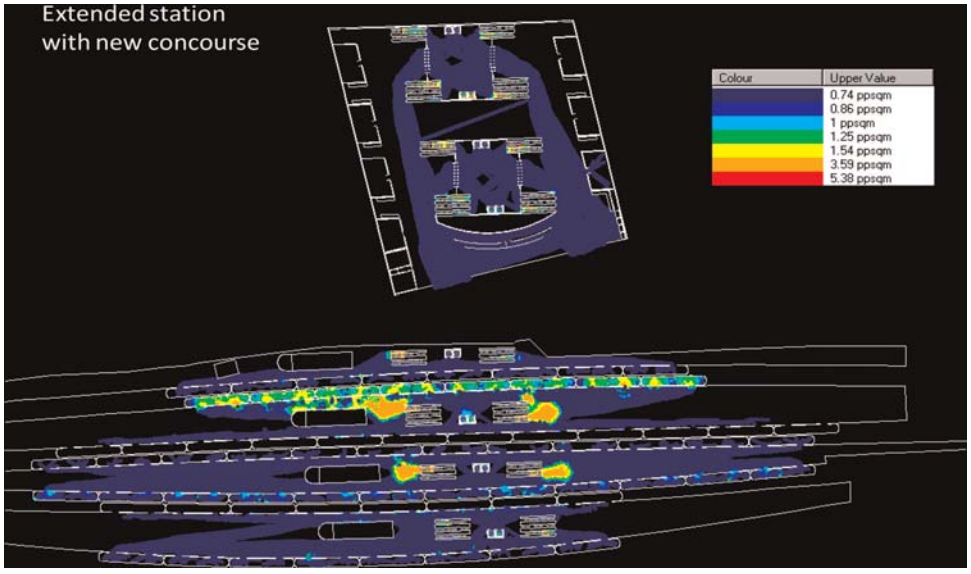


Figure 7 *Extended station with crowding on platforms*

impact on platform clearance times during, say, a fire evacuation.

4 Conclusions

The use of simulations to assist the designer in developing infrastructure that is robust and resilient to the many natural and imported risks is a vast topic and this paper can only touch lightly on the major issues to be considered. This paper shows how the engineer can use a combination of numerical modelling and analysis techniques to optimise the design of the infrastructure to reduce the risks posed by fires and deliberate acts and to provide enhanced resilience towards naturally occurring changes.

5 References

[1] National Fire Protection Association. 'NFPA130 – Standard for Fixed Guideway Transit and Passenger Rail Systems', 2010

[2] Subway Environment Simulation (SES) Computer Program, version 2000

ISSN 2041-5923

Do we have the skills and knowledge to adapt transport infrastructure to climate change risks?

James Dunham Andrew Heather Kristina Kueng David Viner

Mott MacDonald Limited, Demeter House, Station Road, Cambridge, CB1 2RS, UK
E-mail: climate.change@mottmac.com

Abstract: The UK is becoming increasingly vulnerable to changes in weather extremes as a result of climate change. In response to the current and projected climate impacts, actions are required to manage this increasing vulnerability in the form of climate change adaptation. Capacity building actions are a fundamental foundation of delivering adaptation actions. This paper will explore the current capacity for the transport sector to address climate change adaptation, highlight gaps in training that need to be addressed, and make recommendations to help address these.

Keywords: Climate change adaptation, skills, transport

Introduction

The UK is becoming increasingly vulnerable to changes in weather extremes as a result of climate change. In response to the current and projected climate impacts, actions are required to manage this increasing vulnerability in the form of climate change adaptation. Climate change adaptation refers to adjustments or changes in decision environments, which work to enhance resilience or reduce vulnerability to current or projected changes in climate or their effects, or which moderate harm or exploit beneficial opportunities. In working to manage such risks [1], climate change adaptation can be categorised into initiatives that either [2]:

- **Deliver adaptation actions** – Deliver direct actions that help to reduce vulnerability to climate risks or to exploit opportunities

- **Build adaptive capacity** – Initiatives that build capacity to adapt, creating the information (research, data collecting and monitoring, awareness raising), support social structures (organisational development, working in partnership, and institutions), and support governance (regulations, legislations, and guidance)

Capacity building actions are a fundamental foundation of delivering adaptation actions. A key aspect of capacity building is to develop the skills and knowledge to support climate change adaptation activities, through information sharing, learning, training, and development. Learning capacity is important, highlighted by evidence that the UK does not have adequate skills to adapt some of the vulnerable sectors. For example, decision-makers need to learn how to interpret and use climate change adaptation information, particularly the UK Climate Projections (UKCP09) [3], which will require appropriate training.

Developing a successful response to climate change risks will depend on individuals and organisations from different sectors preparing for a changing climate not only in the long term but also in the short and medium term. This requires a strong unifying vision, scientific understanding, openness to face challenges, develop solutions, overcome barriers, stakeholder inclusion, and commitment at the highest level. The development of climate change adaptation skills, training and knowledge can support the building of an adaptive capacity which can provide the base from which these decisions can be made. However, this requires recognition of the necessity to adapt, knowledge

about available options, the capacity to assess them, and the ability to implement the most suitable ones.

Understanding organisational learning, in relation to why and how sectors and organisations change their behaviour, is a key consideration in developing adaptive capacity. Determining how different organisations learn from direct experience, how they learn from others and how they develop conceptual frameworks for interpreting that experience all can help shape capacity building responses.

Methodology

A desk-based literature review was undertaken to develop basic information on which stakeholder engagement was based. A Training Needs Assessment process was used following this to consider the skills, knowledge, and behaviours of the people in stakeholder organisations and how to develop them, both to deliver the organisation's strategic objectives and support the individual's career progression. This information was gathered by engaging with over 200 stakeholders through an online survey targeting a broad spectrum of stakeholders, a workshop, and structured telephone interviews.

Overview of current learning adaptive capacity

Research has shown, and the impacts of observed events have demonstrated that climate change will have significant implications for infrastructure. As infrastructure assets have long operational lifetimes (often 50–100 years or more [4]) they are sensitive not only to the existing climate, but also to climate variations over the decades of their use [5].

Infrastructure is fundamental to how our economy and society operates. Infrastructure sectors are increasingly interconnected, which means failure in one sector can quickly lead to problems in others. For example, all sectors require power and are increasingly dependent on information and communications technology (ICT) for control systems, communications, and general business operations [6]. Managing national infrastructure is a systems issue, requiring collaboration, planning, and sharing of information between all sectors. Systems resilience, rather than sector resilience is required to adapt to climate change. Current geographical and organisational boundaries and barriers need to be overcome by culture and any other available levers to build a picture of the state of the entire infrastructure system and local subsystems [7].

More highly-skilled engineers able to deal with complex infrastructure systems will be needed to develop and implement adaptation measures (this would require new engineers to be sufficiently trained and existing engineers to have training or continued professional development [CPD] to update their skills set). Adaptation, mitigation measures, and the demands of a growing population and economy all make demands on engineering capacity. There is a need, therefore, to simultaneously balance these demands and expand capacity.

The anticipated impacts of climate change in the UK will lead to conditions no more extreme than those currently experienced and dealt with elsewhere in the world. For example, Spain is hotter and many other places are wetter. Sea level rise poses a more persistent threat, with many coastal areas becoming increasingly vulnerable. Technologies for adaptation exist in many of these locations, and given that many UK engineering firms have worldwide experience, particularly within civil engineering, there are good opportunities to learn from technologies and regulatory frameworks overseas. The challenge is to build the necessary partnerships and information sharing networks to be able to efficiently spread knowledge.

Engineers need to develop further their ability to use probabilistic methods and flexible solutions to deal with complex risk scenarios. Promoting these skills is essential, as is using modelling techniques and the methods of scenario planning. Professional engineering bodies should lead on promoting and developing skills in systems thinking within the workforce under the sustainable development attributes required for chartered status. These include, but are not restricted to:

- the Institution of Civil Engineers
- the Institution of Engineering Technology
- the Chartered Institute of Logistics and Transport
- the Institution of Highways and Transportation
- the Transport Planning Society.

A concerted, coordinated approach to various adaptation investments, research and other activities is required in order to avoid duplication of work, and to ensure results are disseminated and prevent maladaptation. This depends in turn on common means for defining resilience and classifying vulnerabilities [8].

Operation and maintenance of the UK's transport networks is vulnerable to weather, with the greatest risks for all modes posed by individual 'extreme' weather events (e.g. windstorms and flooding) and long term changes such as sea level rise. The transport system in the UK is vulnerable to climate change as extreme weather events increase in frequency and magnitude. Analysis of the three transport authorities' (Highways Agency, Network Rail and Trinity House) Adaptation Reporting Power Benchmark Reports suggests that there is a focus on risk analysis rather than risk management and adaptation planning. Further work on the interdependencies of climate change risks is required, together with training to fully understand climate risk assessment methodologies [9].

Alongside the requirements for low carbon skills, developing the right skills is an important element of adaptation within the transport sector. The skills to deliver effective adaptation are likely to be relevant to all transport modes, and be specialisations or extensions of existing technical disciplines such as climate and environmental science, risk management, surveying, planning, and engineering [10].

Building learning adaptive capacity

Awareness of current and future climate change risks facing the infrastructure sector is high in comparison to other sectors. Although it is believed that adaptation should be a priority within the stakeholder group, there are challenges associated with the design of climate resilient infrastructure.

Stakeholders identified that the sector would benefit from a greater level of strategic thinking, so that it is possible to understand the potential impacts and locations of a changing climate prior to the engineering commission. As can be seen by comparing in Fig. 1, leadership and long term business planning are identified as key skills to be developed which will improve strategic thinking. Research and climate change science were also highlighted as key skills to be improved. Engaging appropriately qualified town planners and engineers with a high level of climate change expertise would help alleviate this which could form a part of their CPD training.

The technical capability of the infrastructure sector to be able to incorporate climate risks and uncertainty into projects is relatively high. Planners and engineers are already comfortable working with uncertainty when conducting risk assessments and the key requirement would be a new set of specifications (in terms of climate data) to work towards when putting together designs. Government-led guidance documents, design standards, and tools that are widely used such as WebTAG [11], for example, will be an ideal lead on providing information on a managed approach to risk.

It was suggested by stakeholders that there needs to be a shift in thinking about design in general. Instead of focusing on infrastructure that is completely resilient to climate change, it should be accepted that specific weather events will have a negative impact which will simply be inconvenient. It may be agreed, for example, that a certain stretch of road will flood and that it is not worth the cost of protecting it from all flood events.

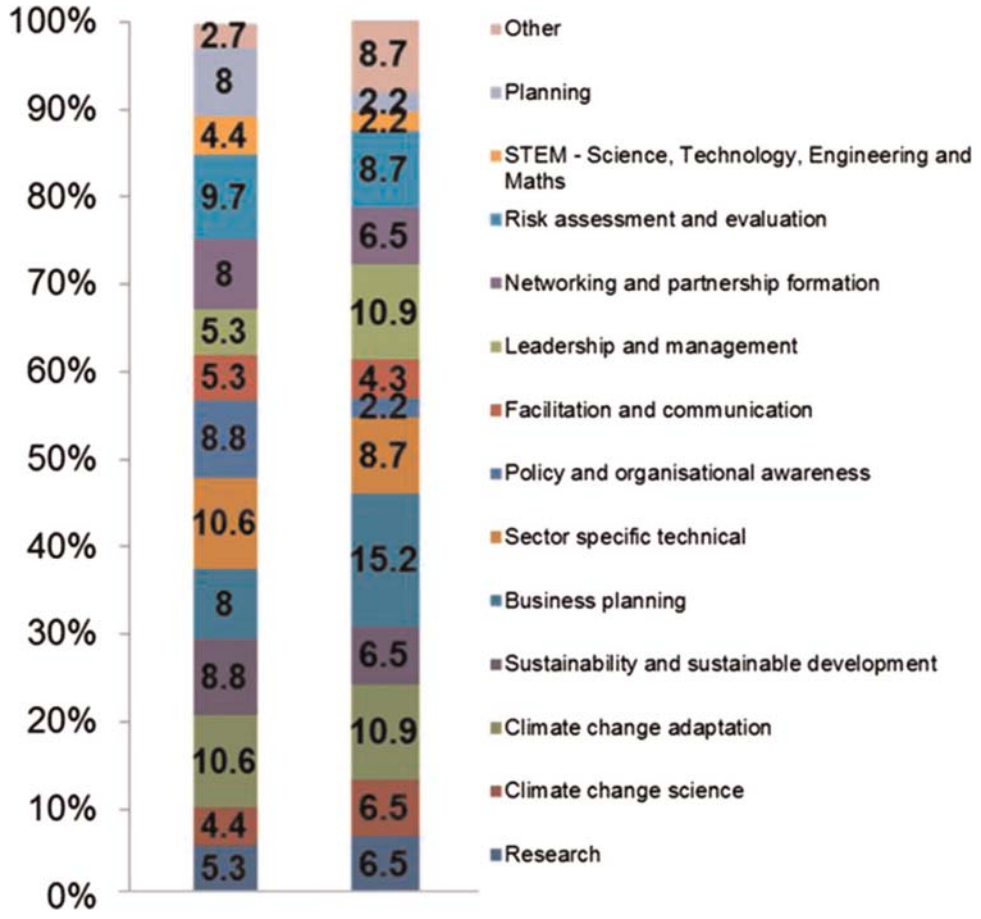


Figure 1 *Cumulative responses to 'What skills do you believed the infrastructure sector currently has (left) and which need to be developed (right) to be able to build its adaptive capacity'*

There is a cost–benefit argument for this kind of approach: completely climate-proofing a road or coastline, for example, is likely to be more costly than letting it flood during specific events. However, critical infrastructure may require an increasingly risk adverse response to resilience planning due to the significant costs associated with loss, as demonstrated by the 2007 floods. For example, when the Mythe water treatment works in Gloucestershire was flooded in July 2007, 350 000 people were left with no water for 17 days [12].

While climate change and resistance to severe weather needs to be considered when designing an infrastructure project, it also needs to be considered during its use. Specialist training for staff such as train operators may also be necessary so they are prepared for snow in winter months but also warmer summers. Work performed outdoors should be addressed in particular as it may be necessary, for example, to make the use of sun protection mandatory.

Recommendations and conclusions

The analysis of our stakeholder responses shows that although the potential technical capability is high, gaps in training needs for the transport sector have been identified. These gaps can begin to be addressed by carrying out the following:

A greater emphasis on cross-sector knowledge sharing will help to quickly build the knowledge base from which engineers and planners can find solutions. There is a potential to find solutions to address future climate risks in other countries, and there is also a need to understand how adaptive solutions here may adversely impact on the adaptation capacity of other sectors.

Professional institutions mentioned above can assist with promoting climate change adaptation by offering information and including the issue in training they provide. For those currently working in the sector, the role of CPD in building learning adaptive capacity is identified as a significant and effective tool. Professional bodies are pivotal in ensuring that new concepts and ideas are taken up by their professions.

Promoting sustainable development is one of the core attributes required by engineering professionals. In support of this agenda engineering undergraduate and postgraduate degrees should have climate change adaptation included in core modules to help raise awareness and promote long term planning so that graduates are comfortable with these subjects before entering the profession.

It has been found that engineers are generally willing and capable to consider climate adaptation if the right tools are there to use. If long term climate risk considerations are incorporated into building regulations and tools such as WebTAG, it can be ensured that climate adaptation is considered in a consistent manner. Information sessions and webinars aimed at engineers or planners can help raise awareness initially which can then be followed by more detailed training.

Acknowledgments

This paper has built on a wider Environment Agency/Mott MacDonald national project to identify opportunities to build learning adaptive capacity to support the management of climate change risk to key sectors, under the UK National Adaptation Programme. Thank you to Richard Lamb at the Environment Agency Climate Ready Service for supporting the publication of this paper. We would also like to acknowledge the following from Mott MacDonald's Transportation Unit for their contributions to this paper:

- Jo Baker, Divisional Development Director
- Dick Dumolo, Technical Director
- Andrew Gordon, Technical Director
- Kim Hampton, Deputy Environment Team Leader.

References

[1] ADGER W.N., AGRAWALA S., MIRZA M.M.Q., CONDE C., O'BRIEN K., PULHIN J., PULWARTY R., SMIT B., TAKAHASHI K.: 'Assessment of adaptation practices, options, constraints and capacity', in PARRY M.L., CANZIANI O.F., PALUTIKOF J.P., VAN DER LINDEN P.J., HANSON C.E. (eds.) 'Climate Change 2007: Impacts, Adaptation and Vulnerability. Contribution of Working Group II to the Fourth Assessment Report of the Intergovernmental Panel on Climate Change' (Cambridge University Press, Cambridge, UK) pp. 717–743

[2] UK Climate Change Impacts Programme (2013) Adaptation Types. Available at http://www.ukcip.org.uk/essentials/adaptation/adaptation-types/, last accessed 30/01/2013

[3] UK Climate Projections. Available at: http://ukclimateprojections.defra.gov.uk/

[4] URS Corporation Limited. Adapting Energy, Transport and Water Infrastructure to the Long-term Impacts of Climate Change. 2010. Available at http://archive.defra.gov.uk/environment/climate/documents/infrastructure-full-report.pdf, last accessed Jan 27 2013

[5] HM Government. Climate Resilient Infrastructure: Preparing for a Changing Climate. 2011. Available at: www.defra.gov.uk/environment/climate/sectors/infrastructure-companies/, last accessed Jan 27, 2013

[6] Council for Science and Technology. A National Infrastructure for the 21st Century. 2009. Available at http://webarchive.nationalarchives.gov.uk/+/http://www.cst.gov.uk/reports/files/national-infrastructure-report.pdf, last accessed Jan 27, 2013

[7] Environment Agency Climate Ready Support Service. Infrastructure. 2012. Available at: http://www.environment-agency.gov.uk/research/policy/132331.aspx, last accessed 27 Jan, 2013

[8] Engineering the Future. Infrastructure, Engineering and Climate Change Adaptation – Ensuring services in an uncertain future. 2011. Available at: http://www.raeng.org.uk/news/publications/list/reports/Engineering_the_future_2011.pdf, last accessed 27 Jan, 2013

[9] DEFRA. UK Climate Change Risk Assessment: Climate Change Risk Assessment for the Transport Sector. 2012. Available at: http://www.defra.gov.uk/environment/climate/government/risk-assessment/#sectors, last accessed 27 Jan, 2013

[10] Department for Transport. Climate Change Adaptation Plan for Transport 2010–2012: Enhancing resilience to climate change. 2010. Available at: http://archive.defra.gov.uk/environment/climate/documents/dft-climate-change-plan.pdf, last accessed 27 Jan, 2013

[11] The Department for Transport. Transport Analysis Guidance – WebTAG. 2013. Available at http://www.dft.gov.uk/webtag/, last accessed Jan 21, 2013

[12] Institution of Civil Engineers. The State of the Nation – Defending Critical Infrastructure. 2009. Available at http://www.ice.org.uk/getattachment/5e93aedd-3b4c-44db-acfa-d176e0ccbb0e/State-of-the-Nation-Defending-Critical-Infrastruc.aspx, last accessed Jan 28, 2013

ISARR

ISARR is a web based system that gives a graphical representation of all of the assets and associated risks across the organisation, and watches and notifies of any changes in real time.

It provides the tools to manage and mitigate any incidents or crisis, and ensures competency, compliance and standards are maintained and exercised.

Integrated Security and Risk Resilience

CONTACT US FOR A DEMONSTRATION
+44 844 736 2544

LinkedIn www.linkedin.com/company/isarr

www.isarr.com/contact-us

The Institute of Risk Management

LEADING THE RISK PROFESSION THROUGH DELIVERY OF EDUCATION AND LIFELONG LEARNING

Understanding the importance of risk management from those in the know...

At IRM we help organisations link risk management to business needs. We are passionately committed to supporting you through our world-renowned qualifications, executive programmes, conferences and thought leadership activities.

IRM provides you with:

- Internationally recognised qualifications
- Professional recognition
- Access to a global network of risk professionals
- A wealth of information on topical risk issues
- On-going career support

Call us today to find out how we can help you and your organisation.

T +44 (0)20 7709 9808 W www.theirm.org

irm

Leading the risk profession

The Institution of Engineering and Technology

Built Environment

Smart innovation for tomorrow's urban landscape

The IET has prioritised five sectors: **Built Environment, Design and Production, Energy, Information and Communications** and **Transport** to make it easier for you to source essential engineering intelligence, access expertise, find current and reliable information, participate in active communities and attend industry leading events.

Get involved...

www.**theiet**.org/infrastructure