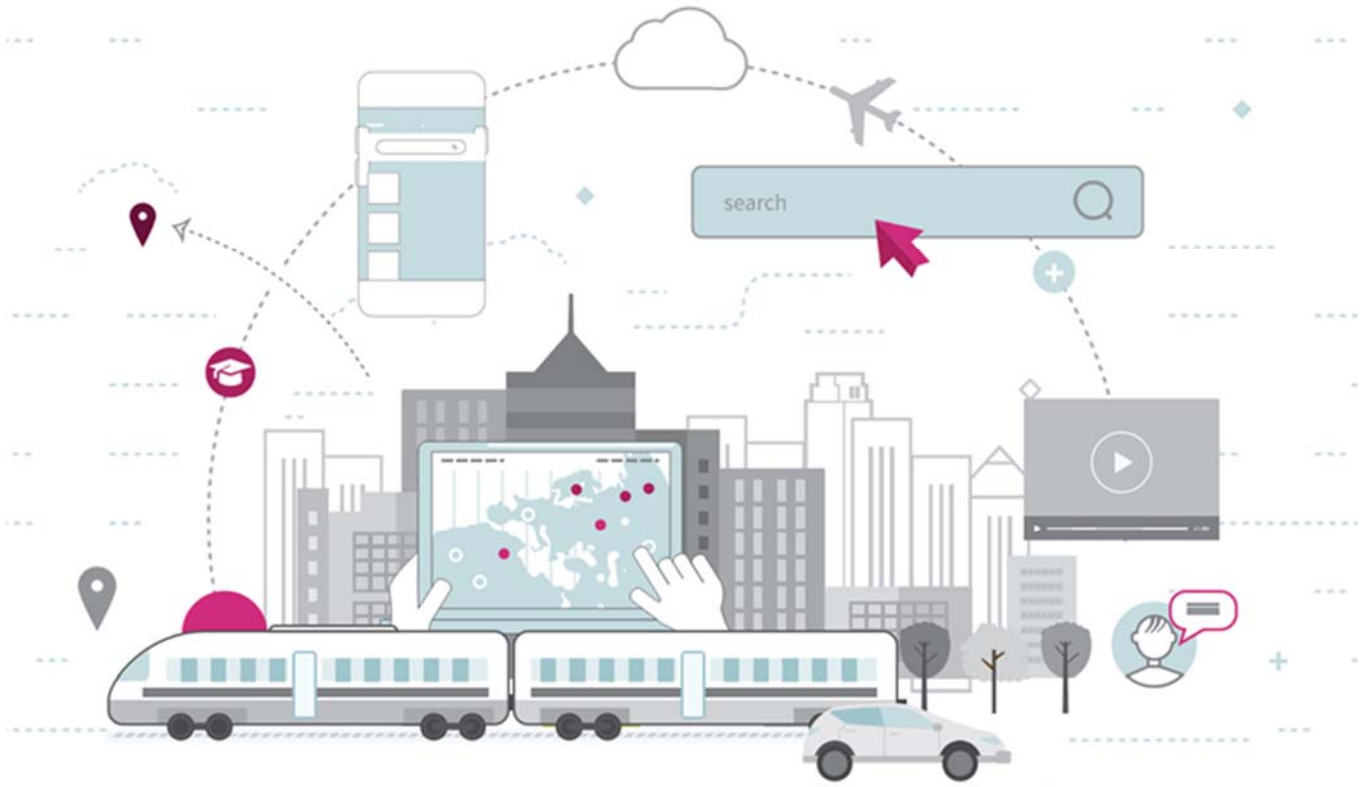
National Infrastructure Commission

Infrastructure and Digital Systems Resilience

Final Report - November 2017

APPENDICES



Ove Arup & Partners Ltd
13 Fitzroy Street
London
W1T 4BQ
United Kingdom
www.arup.com

UCL ARUP

Appendix A

Key terms

A1 Key terms

The National Infrastructure Commission (NIC)	The NIC is an executive agency of the Treasury, operationally independent of the Government. Its aims are to support secure sustainable economic growth across all regions of the UK, and to improve quality of life and competitiveness across the UK. Established in October 2015 the Commission assesses the country's future needs for national infrastructure. Each Parliament the NIC will produce a National Infrastructure Assessment (NIA). The organisation outlines the infrastructure needed and what solutions should be provided to meet those needs, covering a variety of sectors including transport, water and energy.
Digital infrastructure systems	Digital infrastructure: this generally refers to communications infrastructure, both fixed (broadband) and wireless (mobile) assets alongside centralised facilities (e.g. data centres) and the associated hardware and software.
Resilience of digitally-connected infrastructure systems	Resilience, whilst having a multitude of definitions, broadly describes the ability of a system to anticipate, absorb, respond and recover, and adapt to any unexpected event. The *resilience of digitally-connected infrastructure systems* is therefore the ability of such systems to continue to provide the flow of data on which society depends, even when these systems, or the environment in which they operate, do not behave as we expect.
'Normal accidents' theory	A normal accident occurs when two or more failures, none of them devastating in isolation, come together in unexpected ways and defeat the safety devices (i.e. redundancies, circuit breakers, alarms etc.) that have been built into the system. If the system is also tightly coupled these failures can cascade rapidly. It is a normal accident in the sense that it is an inherent property of the system to occasionally experience this event. This does not mean that it is frequent or expected.
Smart infrastructure	Smart infrastructure is the result of combining physical infrastructure with digital infrastructure, providing improved information to enable better decision-making, faster and cheaper. The term Cyber-physical is often used interchangeably to mean the same thing.
Tightly and loosely coupled systems or processes	'Tightly coupled' systems, in computing and system design signifies that components are dependent on each other and cannot be isolated from other parts. Loosely coupled systems are therefore the opposite, where a failure or shut down of one component has less impact on operations and the delivery of services.
Interactive complexity	Components can interact in unexpected ways that cannot necessarily be anticipated. This interacting tendency is a characteristic of a system, not a part or an operator.
Emergent properties	An emergent property is a property, which emerges when components are joined to form a more complex system, and the system has unpredictable properties compared to its simpler components.
Socio-technical systems	Systems that involve interactions between humans and machines. Since the function of national infrastructure is to meet the needs of society, all infrastructure should be considered as socio-technical.
Internet of things	A term for the result of the increasing trend in the use of sensors in both household devices and infrastructure assets. It is becoming easier and easier to deploy sensors and read their results over networks; log their data and infer results.

Cloud computing	Cloud computing is the practice of using remote, managed servers hosted by a third party to store, manage and process data, rather than a local server or a personal computer.

Appendix B

Architecture of a generic digital system

B1 Architecture of a generic digital system

A system is a combination of elements which collectively work together to provide valuable services for its users. Figure B 1 shows the simplified architecture of a generic digital system supporting an infrastructure system. As seen in the figure, the architecture usually comprises:

- Physical infrastructure: Several components, some deployed in the field and some at centralised operational facilities;
- Network/Network links: These connect components together (e.g. connecting the Local Area Networks or cabling between the network and physical infrastructure);
- End-user computers and devices (e.g. phones, PCs, sensors and actuators; using smartphone to control your home heating system)
- Applications: The software elements allowing the monitoring, control and operation of the digital infrastructure.
- Services (e.g. an electricity billing service or signalling service on the railway or the railway service itself)
- An infrastructure system (e.g. railway network or mobile phone network)

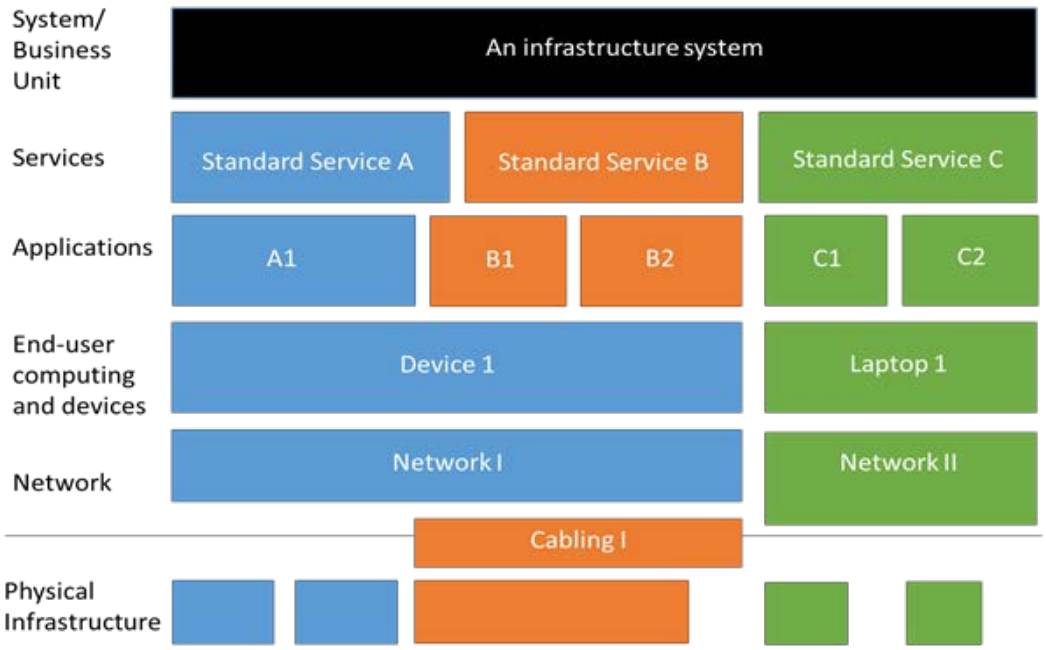


Figure B 1 A generic digital system

Appendix C

UK infrastructure use of digital networks

C1 UK infrastructure use of digital networks

Sector	Sub-sector	Organisation	Digital Network
Transport	All		1. Use of GPS, which has a number of vulnerabilities as identified by the Royal Academy of Engineering in their 2011 report[1]
	Road	Highways England	2. National Roads Telecommunications Services (fibre network). C**losed** network that connects variable message signs, CCTV cameras, emergency telephones and sensors on the network. 3. Highways England also rely on the **public** network to communicate with their users, via social media for example. 4. Highways England users are increasingly dependent on GPS-devices for real-time information about routes, diversions and delays. Modern vehicles are using inter-vehicle communications technology.
	Rail	Network Rail	1. Fixed Telecommunications Network (fibre and copper cables). **Closed**. Runs alongside all main and secondary routes and including some remote branch lines. 2. European Train Management System (ERTMS). Cab-based signalling and train control system that aims to replace all the different national train control and command systems in Europe, which are primarily based on lineside signals. Comprises GSM-R, and ETCS. 3. Global System for Mobile Communications-Railway (GSM-R). Internal mobile network for direct train-control centre communications including within tunnels and deep cuttings. Highly reliable and secure communication between critical operational rail personnel, in particular, train drivers and signallers. The system uses a combination of fixed and mobile digitally-connected infrastructure to an internationally recognised standard, and is used on virtually the whole GB mainline rail network, phased in between 2007 and 2016. It replaces old analogue radio networks, which were becoming costly to maintain and had limited functionality. 4. European Train Control System (ETCS), an automatic train protection system (ATP) to replace the existing national ATP-systems. ERTMS has already been deployed on a limited number of UK rail lines but has not yet been rolled out across the entire network. It is planned to deploy the system on a route-by-route basis, with the initial plan covering the period 2019-2029. 5. Network Rail passengers rely increasingly on the internet for information from the train operating companies about service.

[1] http://www.raeng.org.uk/publications/reports/global-navigation-space-systems

	Aviation	National Air Traffic Services	NATS use digital technologies to safely coordinate aircraft movements in the UK. This has now extended to the use of 'digital remote towers' to provide air traffic management services. These can be used both as contingency facilities for international hubs or as possible expansion opportunities for small regional airports enabling air traffic control services from a central location, so smaller airports remain viable for their operators and local communities. This has been realised due to super-fast fibre networks, high definition cameras and remote sensing technology. 'Instead of a tower full of controllers and equipment, there is a camera mast that transmits images and data to a separate control centre that could be hundreds or even thousands of miles away. There, the view of the airfield is stitched back together to create a live 360-degree image that can be augmented with other operational data, from radar labels on individual aircraft, to the location of closed taxiway'[2].
Energy	Electricity and Gas distribution	National Grid	National Grid has a number of fibre networks including one run on top of their national high voltage network which they use to resell bandwidth, as well as a **closed** network for their operations that consists of a number of tiers e.g. mission critical for monitoring and control of substations, business critical for communications and other non-critical networks.
	Electricity and gas supply	Energy companies	Smart meters are currently being installed in private homes and businesses nationally. These use **public** infrastructure networks (e.g. digital cellular networks) for transmitting information captured by the devices. They do not rely on domestic internet connections; they use a low power wireless network (called "Zigbee") within the home (to link a display to the two metering equipment components for gas and electricity) and they use the mobile cellular network to communicate the readings to the suppliers. The supply of energy does not rely on the smart meter.
Water	Distribution and supply	Water companies	The water network in the UK is managed by over 20 suppliers, see Figure C 1, which are to a degree isolated from one another (although it is noted that there are some connections through inter-basin transfers etc.). Digital networks in the water industry are not nationwide for this reason. 1. All water companies use tiered networks, such as their own **closed** networks for control of waste water treatment, water supply etc. and non-critical networks e.g. for their fleet management to coordinate operations on a local level. Some of these networks are linked to the internet. Operational facilities including centralised control rooms and site control rooms (e.g. at treatment works or pumping stations) often require links to the digital infrastructure. 2. The water industry uses the Water Industry Telemetry Standard (WITS), a communication method using a Supervisory Control and Data Acquisition (SCADA) system.
Digital	Supply	Various	The UK's mobile and fibre broadband networks are by definition, public networks. Key issues are around coverage and speed, both of which vary significantly nationally. Providers have service level agreements (SLAs) with their customers. The public network is insecure, but very low cost.

[2] NATS, Control without bounds: The rise of the digital 'remote' tower. http://www.nats.aero/discover/control-without-bounds/

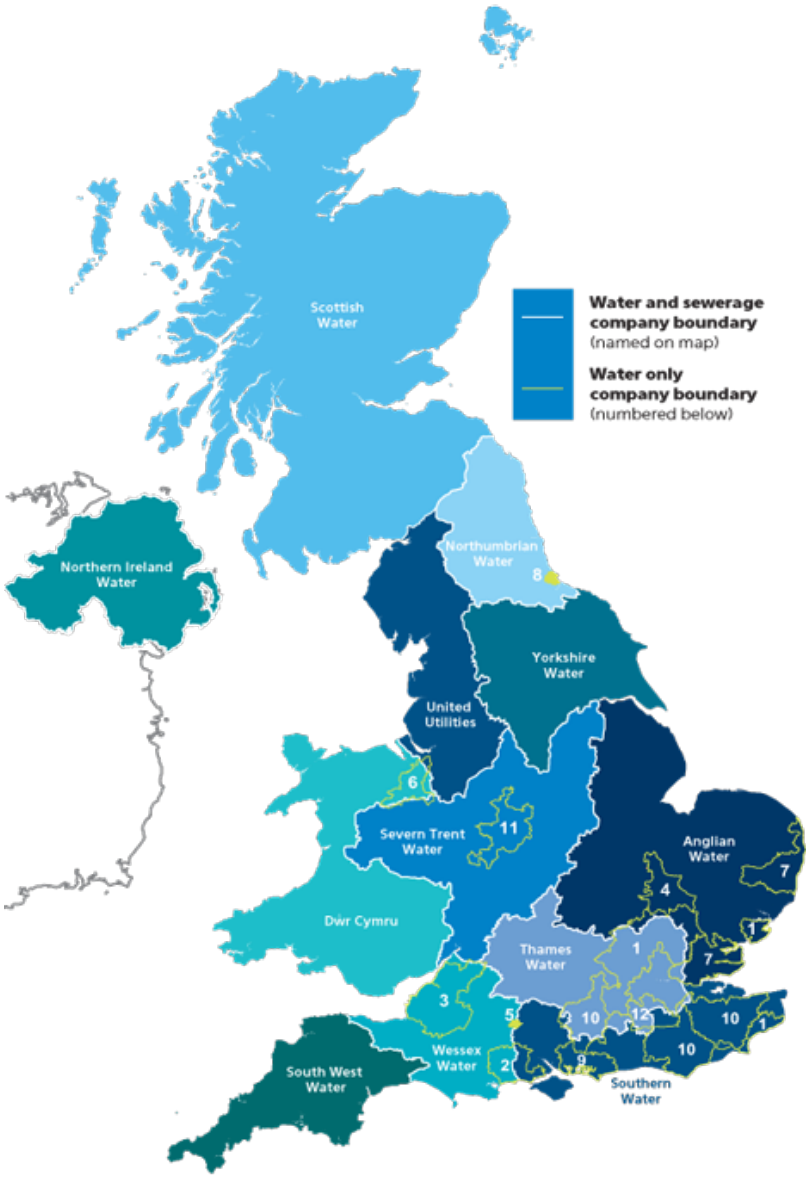


Figure C 1 UK Water Networks[lii]

1. Affinity Water
2. Bournemouth Water
3. Bristol Water
4. Cambridge Water (South Staffs)
5. Cholderton and District Water
6. Dee Valley Water
7. Essex & Suffolk Water (Northumbrian)
8. Hartlepool Water (Anglian)
9. Portsmouth Water
10. South East Water
11. South Staffs Water
12. Sutton and East Surrey Water

[lii] Water UK, 2015. Water industry Map http://www.water.org.uk/sites/default/files/Water-Industry-Map-for-main-page-August-2015_0.png

Appendix D

Learning from other organisations

D1 Learning from other organisations

Learning from High Reliability Organisations

The nuclear industry is a recognised example of a high reliability sector. However, the catastrophic sequence of events that took place at the Fukishima Daiichi plant in Japan on March 11 2001 show that such organisations are not always protected against severe accidents. Furthermore, the measures that must be followed, for example to demonstrate a safety case for a safety critical facility may not be practically transferrable to other sectors, due to the time, cost and manpower requirements.

If high reliability organisations become very process-oriented and heavily regulated and legislated, there is the potential for the organisations to 'stop thinking' for themselves about the threats they face. In practice, flexibility and adaptability are key in developing resilient organisations. Further observations around high reliability theory include:

- High reliability organisations are arguably silos, meaning that their infrastructure planning decisions may not be entirely appropriate for highly interdependent systems.
- By introducing additional safeguards into complex systems, to mitigate the potential for accidents and errors, it should be appreciated that these safeguards themselves will introduce an additional layer of complexity often into both operations and maintenance, an example of unintended consequences.
- There is an important distinction between the organisational structures needed for an *efficient* organisation (in a stable context), and a high reliability organisation in the face of unexpected events (unstable external context). Efficient organizations are vulnerable to disruptive external events because their success typically assumes that operating conditions will remain within a stable range of operating conditions. A high reliability organisation recognises that unexpected events will happen and must be handled with minimal consequences.
- Reversing the five principles listed above, any organisation that (i) ignores small failures, (ii) accepts simple diagnoses, (iii) takes frontline operations for granted, (iv) overlooks capabilities for resilience, or (v) defers to authorities rather than experts they will not be achieving high reliability[22].

On a practical level, it can be concluded that high reliability organisations and the underlying theory can be viewed as a form of good practice capable of increasing the reliability of high-risk systems.

High reliability organisations provide a useful starting point for planning how to increase the reliability of any digitally-connected infrastructure systems.

Learning from other organisations

Any organisation or system that recovers to a stronger position following a shock event can be considered to represent best practice. There are many excellent examples of disaster response in Japan that show a prepared and resilient society. For example, the federal government there put in place an emergency warning system in February 2007, which was used in the aftermath of the 9.0 magnitude earthquake in 2011[i]. The earthquake resulted in a tsunami 9.3m high minutes later. Within 29 seconds of detection, the Japan Meteorological Agency sent signals that initiated the following series of actions:

- The three major mobile networks sent messages to users warning about the earthquake
- TV and radio broadcasts flashed an alert showing the epicentre and areas that would be heavily exposed
- In Tokyo trains were stopped, subways were evacuated, gas was disconnected, and nuclear reactors were shut down
- Airport runways were closed and flights diverted
- Cranes were lowered, cars pulled over and surgeries ceased
- Emergency services were informed of the earthquake and readiness levels were raised.

While difficult to measure, it is likely that the emergency warning system ensured that no trains were derailed and all flights landed safely. It demonstrated that during a natural disaster smart cities can capture data which can then be processed and used to inform emergency services, individuals and companies.

Physical simulation exercises can be hugely beneficial in enabling government and society to respond to events, and the potential for modelling and virtual simulation is increasing. The Dubai airport terminal successfully used simulations and testing prior to opening, learning from some of the problems experienced at Heathrow Terminal 5. This was also the case for Terminal 2 at Heathrow where following completion of construction the site was used for trials focussed on people rather than technical testing of devices. 192 trials were carried out involving 3000 people and even a dummy live flight. The simulations got progressively more complex, starting with people organised in physical units and progressing to entire areas[ii].

Whilst not an organisation as such, nature presents many examples of what are known as anti-fragile systems, which are able to adapt to threats that were not identified at the outset. For example, human skeletons can develop increased bone density as a response to weight gain, and the potential to learn from and be inspired by nature in the planning and design of infrastructure systems (*bio-mimicry)* is an area of emerging interest. An example of an application to infrastructure systems is in energy systems: some advocate designing future energy supply system similarly to an ecosystem[iii]. This would involve encouraging consumers to be active – there are no passive members of

ecosystems. Living systems are differentiated and distributed – if energy systems were the same, that would increase resilience. For example, more community electricity or heat schemes and load balancing on a local scale would create a system more closely similar to an ecosystem. The potential for lessons from ecology and socio-environmental systems to be applied to infrastructure systems needs further research.

The UK's energy system is generally very reliable and because it is 'always' there most infrastructure systems rely upon its availability. Digital systems cannot be decoupled from their electricity supply and vice versa and it is recommended that this basic consideration is explicitly documented in all infrastructure developments, using multi-stakeholder workshops, and techniques such as the Structured What If Technique (SWIFT) frequently used in safety critical industries. This focusses on scenarios and hence outcomes rather than on the removal of specific hazards. The British Ministry of Defence use the SWIFT technique, as well as other techniques, to aid the implementation of safety and environmental protection in their procurement. This technique is a brainstorming method using "what if" or "how come" questions combined with checklists. It was developed in the chemical process industry[iv].

The Technical Specifications for Interoperability (European Union Agency for Railways)

The Technical Specifications for Interoperability (TSIs) define the technical and operational standards which must be met in order to satisfy the 'essential requirements' and to ensure the 'interoperability' of the European railway system. TSIs also set out expected performance levels[v]. The TSIs represent good practice in that they define a common framework across all European railways that cover everything from design through to operations and maintenance in a fragmented and complex industry. In the UK, Department for Transport is responsible for the implementation of the TSIs. New or upgraded projects are required to comply with them.

[i] Japan Meteorological Society, 2013, Smart City Resilience: Learning from Emergency Response and Coordination in Japan

[ii] Zerjav V., Davies, A, Edkins, A, Jones, P, 2014, Building Progressive Confidence: the Transition from Project to Operational Opening in the Case of a Major New International Airport Terminal, International Symposium for Next Generation Infrastructure Conference Proceedings: 30 September - 1 October 2014 International Institute of Applied Systems Analysis (IIASA).

[iii] Forum for the Future, accessed 2017, Living Grid, https://www.forumforthefuture.org/project/living-grid/overview

[iv] Ministry of Defence Acquisition Safety & Environmental Management System, Structured What If Technique, accessed 2017, https://www.asems.mod.uk/printpdf/toolkit/swift

[v] RSSB, 2017. Technical Specifications for Interoperability. https://www.rssb.co.uk/standards-and-the-rail-industry/standards-explained/technical-specifications-for-interoperability [accessed 9 June 2017

Appendix E

Important elements of best practice

E1 Important elements of best practice

To enhance resilience will require a combination of measures. The following sections present elements of best practice from different disciplines, recognising that some of these are likely to be valuable in any situation.

Human factors

A fundamentally important component of our infrastructure systems is the people who operate, maintain and use them. Human factors, as a science closely related to infrastructure planning, design and operations, should not be neglected.

Human factors are required to be considered in various safety critical industries such as defence[i], rail[ii], oil and gas, nuclear, aviation[iii] and medicine, typically through regulation.

Human factor processes are integrated into design, construction and operation through for example "user-centred design" considerations, and "cognitive task analysis"[iv], workload, safety and fatigue risk management systems, providing existing models to follow. The impact of digital technologies on human factors, and vice versa is an important area to understand.

As we become increasingly used to technology-based systems, which operate with less human intervention, the ability to revert to manual operations must also be carefully maintained. Current rail automation for example, requires drivers to be able to make decisions and operators are still required to know how to operate trains and signals manually.

Although human error and behaviour is a significant contributory factor to normal accidents; the ability to respond when problems occur and to correct problems before they escalate often requires human adaptability, flexibility and decision-making.

Essentially, failing to consider all infrastructure systems as a socio-technical system, and to recognise its interdependence with people, it likely to lead to problems. In the armed forces, there are examples of failures due to leadership[v] and also multiple examples of resilient responses in the face of shocks and stresses, frequently at less senior ranks.

Negative synergies and latent errors

The importance of planning and designing without creating negative synergies, where the sum of equipment, design and operator errors is far greater than the consequences of individual failure should be recognised. Identifying and mitigating these factors falls into the category of good risk management, using for example failure analysis such as HAZOP or Failure Mode and Effect Analysis, Failure Mode and Effects Criticality Analysis (FMEA and FMECA)[vi].

Latent errors are errors or deviations from policies and procedures that in themselves have no direct adverse impacts, but, if unchecked, have the potential

for adverse consequences. There is extensive literature documenting how organisations can remove and manage errors from their operations, including through redundancy, flexibility and culture[vii].

Organisational procedures

In any system, decentralised decision-making meaning that those closest and therefore best placed to respond quickly are able to make decisions, can speed up response and hence recovery from emergency event. In tightly coupled systems, defining who is responsible and accountable can be complex in itself, but this should be tackled.

Resilience as a dynamic system property

To increase resilience and reduce recovery time, an organisation must be dynamic in continually planning for, and adapting to, changing external contexts. This requires regular re-evaluation of desired function(s)/outcome(s), and the business model and mode of delivery to enable those. Upgrading/adapting infrastructure assets only after a failure event, or focusing solely on rapid recovery to business-as-usual performance after a failure event, impedes an organisation's ability to be resilient. Figure E 1 ENCORE Plus Resilience Framework, captures the dynamic characteristics of systemic resilience, and the need for continuous action to manage emergent system properties. This should also reflect the requirement for the recovery phase to not only restore to the system's prior state, but to an improved state.

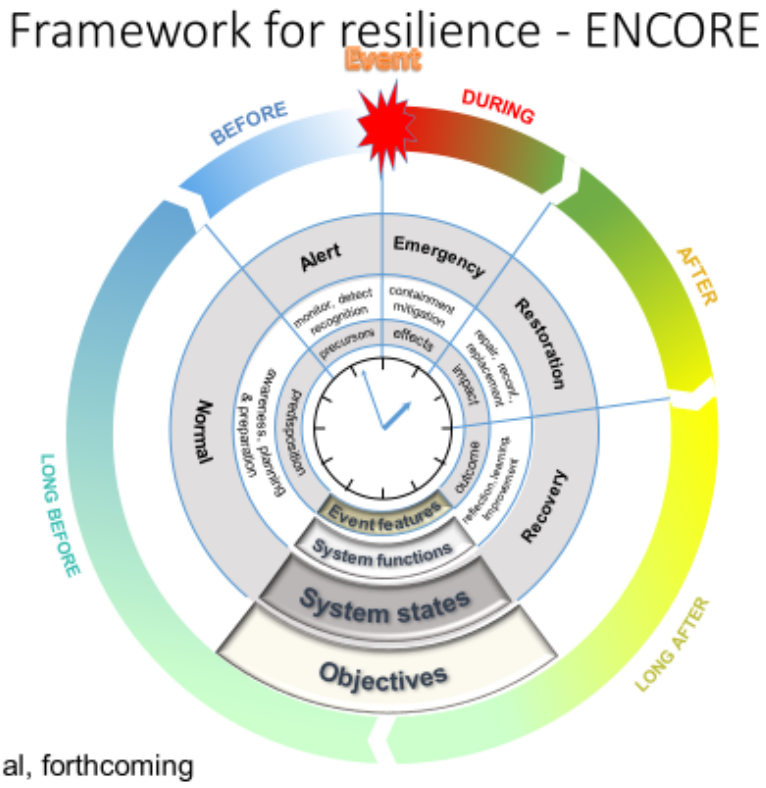


Figure E 1 ENCORE Plus Resilience Framework, Source: Punzo et al. (2017)[viii]

Resilience Engineering

Resilience Engineering is a field of study concerned with the resilience of built systems (including interdependent infrastructure systems). Hollnagel[ix] defines four abilities required to make the resilient performance of dynamic and intentional systems (such as infrastructure), part of 'normal' operations, i.e. to make resilience a core component of operations.

Table 1. Four Abilities of a Resilient Built System[ix]

Ability	Description
The ability to address the ***actual***. (respond)	Knowing what to do: how to *respond* to regular and irregular disruptions and disturbances either by implementing a prepared set of responses or by adjusting normal functioning.
The ability to address the ***critical.*** (monitor)	Knowing what to look for: how to *monitor* that which is or can become a threat in the near term. The monitoring must cover both events in the environment and the performance of the system itself.
The ability to address the ***factual.*** (learn)	Knowing what has happened: how to *learn* from experience, in particular how to learn the right lessons from the right experience – successes as well as failures.
The ability to address the ***potential.*** (anticipate)	Knowing what to expect: how to *anticipate* developments, threats, and opportunities further into the future, such as potential changes, disruptions, pressures and their consequences.

A key challenge in implementing resilience engineering principles in practice is the tension between management for resilience and management for efficiency[x]. This means that resilience of infrastructure systems cannot be managed solely at sector level or by engineering interventions, but will require a level of cross sector oversight and mandating.

Infrastructure interdependence

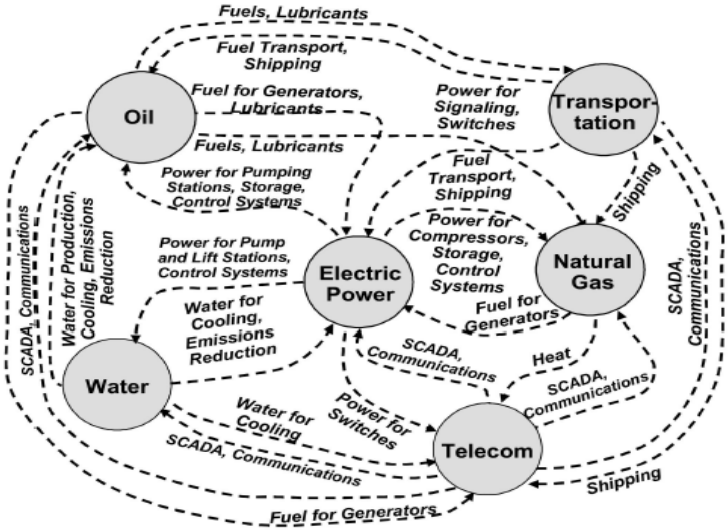


Figure E 2 Examples of electric power infrastructure interdependencies[xi].

Analysis of interdependency can improve understanding of the properties of infrastructure systems that contribute to the high-risk system characteristics (complex interactivity and tight coupling). This can in turn contribute to improved understanding of the impact of digitally-connected infrastructure systems on the likelihood or expected scale of a normal accident.

Trade-offs between system performance under normal operation, and risks introduced by increasing complexity and tight coupling, will be needed. Systemic interdependency analysis can support decisions related to such trade-offs.

The Interdependency Planning and Management Framework (IP&MF)[xii] commissioned by HM Treasury as supplementary guidance to the Green Book provides a method to identify, classify and evaluate interdependencies on a project-by-project basis. Work to tailor the IP&MF specifically to digitally-connected infrastructure system would be beneficial.

Additionally, exercises, such as those used by Engineering the Future[xiii] and Anytown[xiv], (Figure E 3), provide practical methodologies to engage expert knowledge in identifying the most important interdependencies and the possible consequences of these, and how these might be managed in mutually beneficial ways. Focused application of these methodologies to the interdependencies created by digitally-connected infrastructure systems, would be beneficial.

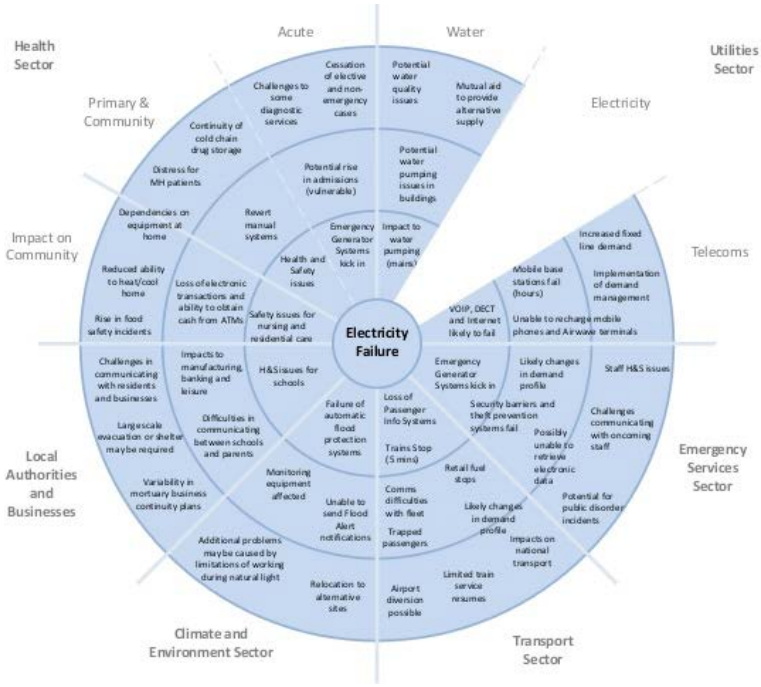


Figure E 3 Anytown interdependency "ripple diagram", used to capture findings from interdependence workshops with front line emergency response professionals[xv]

[i] http://www.ergonomics.org.uk/defence/
[ii] https://www.rssb.co.uk/Library/improving-industry-performance/2008-guide-understanding-human-factors-a-guide-for-the-railway-industry.pdf
[iii] http://www.caa.co.uk/Safety-initiatives-and-resources/Working-with-industry/Human-factors/Human-factors/
[iv] Rail Safety & Standards Board, 2008, Understanding Human Factors – a guide for the railway industry, https://www.rssb.co.uk/Library/improving-industry-performance/2008-guide-understanding-human-factors-a-guide-for-the-railway-industry.pdf
[v] Haddon-Cave, C., 2009. The Nimrod Review. An independent review into the broader issues surrounding the loss of the RAF Nimrod MR2 Aircraft XV230 in Afghanistan in 2006.
[vi] British Standards Institute, 2010. Risk management – risk assessment techniques. BS EN 31010:2010
[vii] Hoffman, D. & Frese, M. (Eds), 2011. Errors in Organizations. Taylor & Francis
[viii] Punzo, G, Tewari, A, Butans, E, Vasile, M, Purvis, A, Mayfield, M, Varga, L (2017) Complexity and Resilience: Conjugating Apparently Opposed Properties of Engineering Systems, Reliability Engineering and Safety Systems, submitted Apr 2017
[ix] Hollnagel, E., 2014. Resilience engineering and the built environment. Build. Res. Inf. 42, 221–228. doi:10.1080/09613218.2014.862607
[x] Lloyds Register Foundation, 2015. Foresight Review of Resilience Engineering: Designing for the expected and unexpected. Lloyds Register Foundation, London.
[xi] Little, RG., Loggins, RA., Wallace WA, 2015, Building the right tool for the job: Value of stakeholder involvement when developing decision-support technologies for emergency management. Natural Hazards Review. 16(4).
[xii] Rosenberg, G., Carhart, N., Edkins, A.J., Ward, J., 2014. Development of a Proposed Interdependency Planning and Management Framework (Report). International Centre for Infrastructure Futures, London, UK.
[xiii] Royal Academy of Engineering (Great Britain), Engineering the Future (Organization), 2011. Infrastructure, engineering and climate change adaptation: ensuring services in an uncertain future. Royal Academy of Engineering, on behalf of Engineering the Future.
[xiv] Hogan, M., 2013. Anytown Final Report.pdf. London resilience, London.

[xv] Anytown, 2013, Infrastructure interdependencies and resilience. https://www.slideshare.net/mtthwhgn/anytown160513-final

Appendix F

Cross sector and sector specific anticipated changes

F1 Cross sector and sector specific anticipated changes

Digital communications

Advances in digital communications such as widespread 5G connectivity will provide near-total connectivity will allow closer integration of digital and physical infrastructure. This will mean that more infrastructure will become digitally-connected infrastructure.

Real time monitoring and analytics

Real-time monitoring and analytics will result in predictive maintenance instead of reactive maintenance. Densified microcomputers are predicted to become more widespread for running secure software, which will enable stakeholders to integrate control systems onto their assets. This could improve operational efficiency and operate independently in the event of a communication system failure.

Introducing new vulnerabilities

Machine learning can be used, for example, to teach a programme how to identify defects in structures such as cracks in concrete by showing it hundreds or thousands of photographs of such cracks. If a series of photographic surveys of a structure are taken over time, the programme can then be used to automatically detect deterioration. However, if the technology is embraced without robust engineering judgement being embedded within the algorithms it could lead to failures being missed or overstated.

Blockchain

Blockchain is an emerging technology that has found most use in cryptocurrency such as Bitcoin. Blockchain is expected to expand use from Bitcoin due to its distributed ledgers which have the ability to replace intermediary centralised systems of record. This has the potential to reduce costs, delays, and also to provide more timely and accurate data and enhance reporting accuracy (PwC, 2016). Blockchain may increase resilience as there is no single point of failure. Since much of the work is automated and dispersed, blockchain could require fewer humans to operate than current government and financial recordkeeping systems, which require complex reconciliation of separate records and transactions and rely on people to run huge centralised computer infrastructures.

Crowdsourcing

Crowdsourcing is where a large number of people input into a task, either paid or unpaid, and primarily through the internet. This can result in better public

consultation and engagement where individuals have the opportunities to co-create. An example is the charity Missing Maps which crowdsources to map areas where humanitarian organisations work so that they can use the maps and data to better respond to crises. Another example is the CleanSpace company which crowdsources air quality data by distributing personal portable air pollution sensors. This type of data can lead to better long-term design and maintenance.

Transport

Transport is one of the sectors that will become increasingly digitally-connected over the next 10 to 30 years.

Technological advances that will affect the UK road network includes autonomous vehicles, which many predict will be on roads in 10-15 years. This is also associated with platooning of freight which could yield greater capacity on the existing road network through shorter headways distances required.

A key opportunity could be the potential for digital technologies to suppress some demand on road networks due to more effective remote working. This will mean an increasing reliance on digital communications infrastructure to ensure the roads are not congested. However, a reduction in demand will mean there is greater slack in the system, thus increasing resilience.

Another trend that is expected to affect the road network is the rising prevalence of mobility as a service through use of digital technologies e.g. applications such as Uber or Lyft. Resilience of digital networks will be of increasing importance as people come to rely on applications over owning their own mode of transport.

The use of digital infrastructure within rail will also increase over the 10 to 30 year timeline. It will be used for:

- more driverless trains,
- realtime monitoring of rolling stock and infrastructure,
- improved accuracy of passenger information,
- predictive maintenance planning,
- seamless journeys integrating with other modes of transport.

Energy

To put the changes to the energy system in context, the total energy demand in Great Britain could move from its current level of around 900 TWh/year to 1200 TWh/year by 2050, depending on the adoption of potentially disruptive new technologies such as energy storage and the electrification of heat and transport[i].

Technologies in the next 10 to 30 years are therefore likely to be focused on increasing capacity. A recent example is the application of artificial intelligence to optimise the national grid. DeepMind (the Google owned AI company), is

working with National Grid to reduce the UK's power usage through optimising the power transmission network balancing of supply and demand[ii].

In other countries there are already efforts to use peer-to-peer platforms to share trade energy, for example from solar sources. These use blockchain to provide an auditable and automated market trading platform[iii]. Both of the above examples will provide an increase in efficiency but may lead to a reduction in resilience.

Microgrids, and more use of local energy sources such as photovoltaic panels on buildings, will provide a more diffuse and diverse energy infrastructure, which should enhance resilience by reducing the impact of single points of failure.

Water

Demand is also expected to increase in the water industry. According to DEFRA, efficiency will need to play a significant role in order to achieve a sustainable supply demand water balance, with high standards of water efficiency in new homes, and water-efficient products and technologies in existing buildings[iv]. There will be increased deployment of digital infrastructures and data analytics to manage, reduce or eliminate system peaks and fluctuating demand patterns. This digital infrastructure will be used to facilitate resource trading and information sharing across a large number of autonomous urban water networks[v].

Greywater recycling systems and rainwater harvesting systems are likely to rise in use. These require energy for treatment and pumping and are likely to need a connection to the internet in order to manage the system. This is especially true if coupled with other systems for a site. An example would be using weather data information to inform when tanks should be emptied to create storage for large storm events[vi].

The increasing sophistication of metering with digital transformation and smart technologies enables more effective monitoring to determine pricing and can provide the potential to reduce leakages via tracking variation in demand. ITRC projects a 100% roll out of smart meters by 2020[vii].

---

[i] Atkins, ICE, ITRC, 2016. National Needs Assessment: A vision for UK infrastructure. https://www.ice.org.uk/getattachment/news-and-insight/policy/national-needs-assessment-a-vision-for-uk-infrastr/National-Needs-Assessment-PDF-(1).pdf.aspx

[ii] Business Insider, Google's Deepmind wants to cut 10% off the entire UK's energy bill, accessed July 2017, http://uk.businessinsider.com/google-deepmind-wants-to-cut-ten-percent-off-entire-uk-energy-bill-using-artificial-intelligence-2017-3

[iii] Power Ledger, accessed July 2017, https://powerledger.io/

[iv] DEFRA and HM government, 2008, Future Water: The Government's water strategy for England https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/69346/pb13562-future-water-080204.pdf

[v] Arup and Sydney Water, 2015 The Future of Urban Water: Scenarios for Urban Water Utilities in 2040.

[vi] Aquality, 2017. Home Page http://www.aqua-lity.co.uk/

[vii] ITRC, 2013, ITRC Second assessment of national infrastructure pilot results report. 4th ITRC Stakeholder Engagement Workshop, July 2013. http://www.itrc.org.uk/wp-content/PDFs/ITRC-second-assessment.pdf