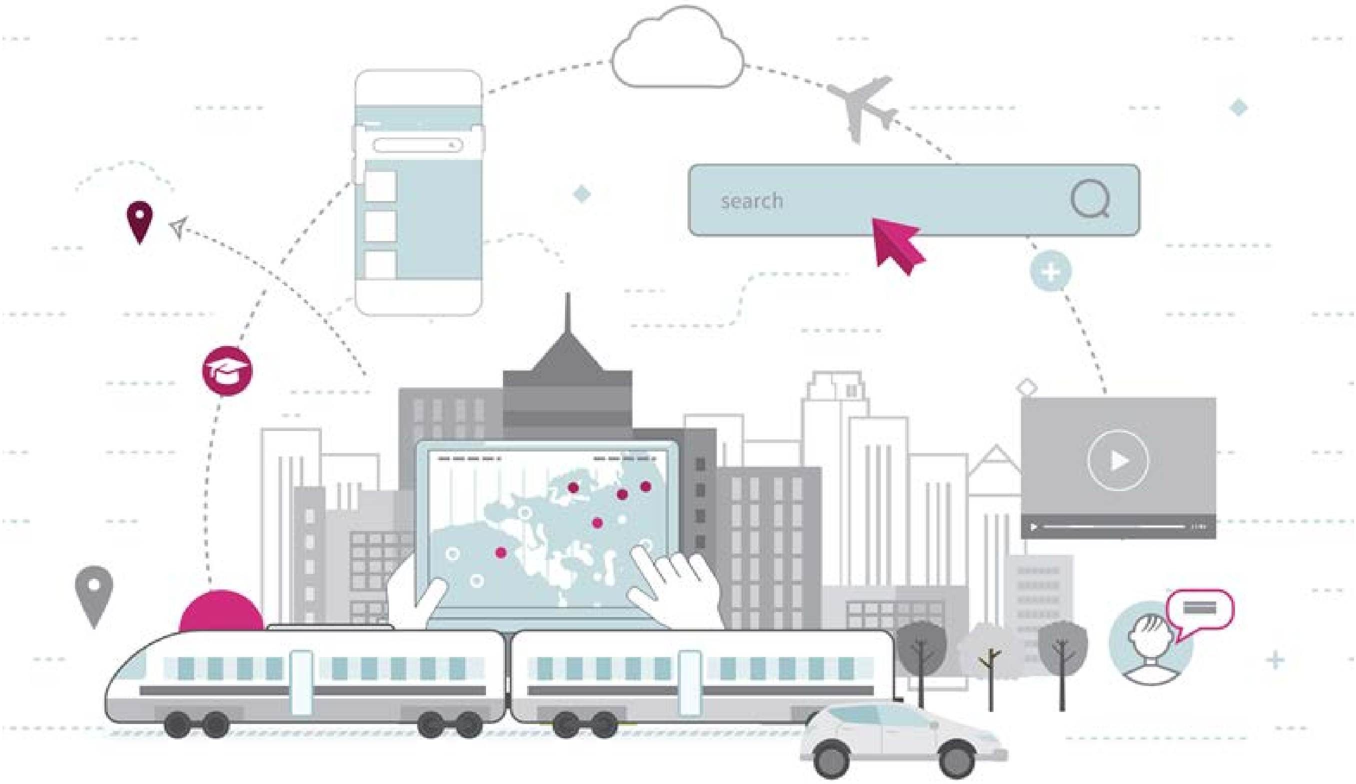
National Infrastructure Commission

Infrastructure and Digital Systems Resilience

Final Report - November 2017



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

UCL ARUP

Contents

Executive Summary

Digital system resilience refers to the ability of increasingly pervasive digital infrastructure systems to operate as intended and recover from incidents responsively.

Networks of **digitally-connected infrastructure systems** (or 'system-of-systems') are widely predicted to emerge and develop in the next 10-30 years. This will create **opportunities**, to enhance resilience through smarter and faster responses, alongside **unintended vulnerabilities**, to accidents and disruption, which are inevitable in tightly coupled and complex systems.

The **National Infrastructure Commission** appointed **Arup and University College London**, to explore the trend towards digital infrastructure systems from a resilience perspective. This was done through a combination of literature review, case studies, and consultation with selected subject matter experts. This report presents the findings, and draws out some key recommendations for the NIC to consider, as it develops the UK's first National Infrastructure Assessment.

Key findings from this brief study include:

- The need to balance the **benefits** of digital technology such as **efficiency and speed** with awareness of **vulnerabilities** that increasing reliance on digital systems can create.
- Infrastructure systems are already **complex, highly interdependent, and tightly coupled**. Overlaying these systems with digital systems is already prevalent, and will become more so in future. This will further increase complexity, and will probably create new **'emergent' properties** that we do not yet fully appreciate.
- Within the situation described in point 2 above, evidence suggests that **not all accidents can be avoided**, and focus should be on the adaptability, flexibility and recovery properties of systems and organisations to mitigate the impact of such 'normal accidents'. There are aspects of best practice, such as the theory behind High Reliability Organisations, which can help.

The report makes some initial recommendations (summarised in the table on the next page), which include both immediate issues for consideration, and areas for further research and/or development, including:

1. Embedding resilience thinking into the planning and design of infrastructure projects requires a collaborative and cross sector approach, and this is not limited to the case of digitally-connected infrastructure.

2. Consideration of resilience in this context may require broader expertise – such as when considering vulnerabilities associated with overlaid software systems. The NIC is in a good position to promote such interactions.

3. Our infrastructure systems are becoming increasingly interdependent, a characteristic that will be exacerbated by the use of digital technology, and methodologies for fully evaluating these interdependencies, including those between people and the systems they rely on, will become increasingly important.

4. This will need to include a better understanding of how the overlaying of digital systems onto infrastructure can affect the behaviour and properties of that infrastructure. Modelling, event simulation and workshops to understand interdependencies should be introduced at an early stage of the infrastructure planning process.

5. Data is an inherent part of digitally-connect infrastructure systems. Data can be considered as part of our infrastructure, and should be valued as such, planned for, understood and used appropriately to inform the right decisions. Data should not be a by-product, and should not be collected 'just because we can'. Better sharing of data between organisations will form an important part of a collaborative and cross-sector approach to this issue.

Theme	Recommendation	Recommended Stakeholder
Behaviours	Embed resilience thinking in infrastructure decision-making	Industry/ Infrastructure Operators led by NIC
	Carry out workshops and understand dependencies	
	Shift focus to understand resilience of complete systems	
Governance	Develop interdependency methodology	Government and Regulators supported by NIC and Academia
	Advocate learning across organisations	
	Cross Government department and regulator interaction	
Technology	Carry out simulations through modelling	Industry led by NIC
	Understand role of data centres as part of complex systems	
	Recognise and exploit existing and emerging data sources and demand this as part of procurement .	Led by infrastructure operators/owners
Research	Research common processes, architecture and oversight for secure networks	Industry/ Academia led by NIC
	Research complexity of human-digital interaction	

Preface

The National Infrastructure Commission appointed Arup and University College London to conduct a short study of the impact of *increasing reliance on digital systems on infrastructure resilience*. We approached this by undertaking a literature review, and gathering evidence including case studies and expert opinion on topics such as complex systems, normal accidents, high reliability organisations and the potential role of new technology.

In order to assess the UK's long-term infrastructure needs, and provide strategic advice to those responsible for decisions about how we deliver and maintain world-class infrastructure systems, we should consider:

- How our existing and planned infrastructure can be resilient to the diverse shocks and stresses it will face, in an uncertain future.
- How increasingly complex and connected systems depend on each other, and what can happen when one of these systems loses its functionality.
- How our networks and systems rely increasingly on digital infrastructure systems, and how this presents both an opportunity and a threat in terms of resilience in the face of disruption.
- How to ensure that, even if accidents and failures somewhere within our infrastructure system-of-systems are inevitable, we can respond, recover and adapt to minimise disruption. What appropriate planning strategies for new or upgraded infrastructure can embed measures to ensure this?

This report's focus is limited to interdependencies between digitally-connected infrastructure systems; the tendency for normal accidents to affect these systems; and how to prepare for, respond to, and recover from such events. Cyber-security and national security threats are excluded from the scope (although in many cases the impacts following a security breach may be similar), as are non-digital interdependencies and resilience issues, such as threats posed to infrastructure systems by flooding and climate change (although again recommendations, particularly those around response and recovery, may be relevant to such issues).

Approach and structure of report

This report is supported by a stand-alone literature review undertaken by University College London, into some of the key concepts identified in the terms of reference[1], and the findings from two industry workshops held on the 16th May and 5th June 2017[2,3]. At these workshops, industry experts and project team members convened to discuss some of the challenges posed by the development of infrastructure that relies on digital systems, both now and in the future.

The structure of this report, which draws on the standalone literature review and workshop findings, is as follows:

Section 1	Context
Section 2	Normal accidents and digitally-connected infrastructure systems
Section 3	Enhancing resilience of digitally-connected infrastructure systems - learning from best practice
Section 4	Digital infrastructure: the next 10 – 30 years
Section 5	Conclusions and recommendations

Supporting information, such as definitions and details of UK infrastructure systems, is presented in the appendices.

1 Context

Faced with a changing world and an increasingly uncertain future, our infrastructure systems need to continue to provide the service on which society depends. Our man-made, tightly interconnected networks are expected by society to be available, and are required to be safe.

Conversely, the complexity of modern life both increases the potential for accidents and unintended consequences, and can amplify the impact of these if they do occur. This report considers this vulnerability, with a particular focus on *digitally-connected infrastructure systems.* These are infrastructure systems – primarily energy, transport and water (including waste water and flood mitigation) and to a lesser extent waste – that have one or more interdependence with a digital technology.

The *resilience of digitally-connected infrastructure systems* refers to their ability to continue to provide the service on which society depends, even when these systems, or the environment in which they operate, do not behave as we expect.

Key terms and definitions are presented within Appendix A.

1.1 What are digitally-connected infrastructure systems?

A recently published report by Pinsent Masons[4], introduces the term "infratech" to describe *"the deployment or integration of digital technologies with physical infrastructure to deliver efficient, connected, resilient and agile assets"*. In this report we use the term "digitally-connected infrastructure systems" (DCIS), but we are essentially describing the same thing.

At a micro-level, the components of digitally-connected infrastructure systems include (see also Appendix B):

- Physical infrastructure (e.g. water treatment works, bridges);
- Network/network links to connect components together;
- End-user computers and devices;
- Software – for monitoring, control and operation;
- Services (e.g. railway services);
- An infrastructure system (e.g. railway network or mobile phone network);
- Data; and
- The human components of the system, both operators and users.

At a macro-level, it is important to recognise that individual systems or sub-systems are becoming connected to other systems or sectors via digital connections.

1.2 Digital infrastructure – opportunities and threats

Digitisation of infrastructure comes with increasing sophistication and ease of use but also brings an increasing chain of dependencies. The many opportunities associated with increasing digitisation include increasing efficiency, flexibility and ability to anticipate issues and respond quickly.

For example, smart infrastructure can create and inform resilience, but conversely can decrease resilience through exacerbating infrastructure fragilities (Figure 1).

1.3 How does UK infrastructure use digital networks?

At our workshops with industry experts, three themes emerged about digitally-connected infrastructure systems in the UK:

1. Much of this has been introduced in a relatively short space of time compared to more traditional forms of infrastructure.
2. Sector specific communications are typically developed in isolation, with no cross-sector regulatory oversight (no ‘controlling mind’).
3. There are increasing chains of dependency through our infrastructure systems with more components that can go wrong.

Our infrastructure systems rely on digital networks, both closed and public, for communications and control. “Closed” networks have a variety of forms, from no shared infrastructure (a “dark fibre” network for example) to using firewalls or VPNs (virtual private networks). Appendix C presents examples of how different organisations use digital networks. In summary, we rely on a combination of demonstrably secure, sector specific communication networks, and the conventional public internet (insecure but accessible and low cost).

The importance of data and information is becoming more commonplace throughout infrastructure as the necessary software and hardware to collect and store data become more accessible and mainstream. Infrastructure decision makers can deliver their services with greater resource efficiency through data-driven decisions. A lack of common data standards, poor data quality and lack of familiarity with data-led innovation alongside a resistance to open data[*], are some of the challenges facing decision makers. However, some Governmental agencies, for example the Mayor of London’s office[5] and Defra[6] are working towards making more data open (within security constraints) for use by other organisations to accelerate innovation within infrastructure and environmental planning.

[*] The NIC are considering this as part of its new technologies study (https://www.nic.org.uk/publications/new-technology-study-second-call-for-evidence/)

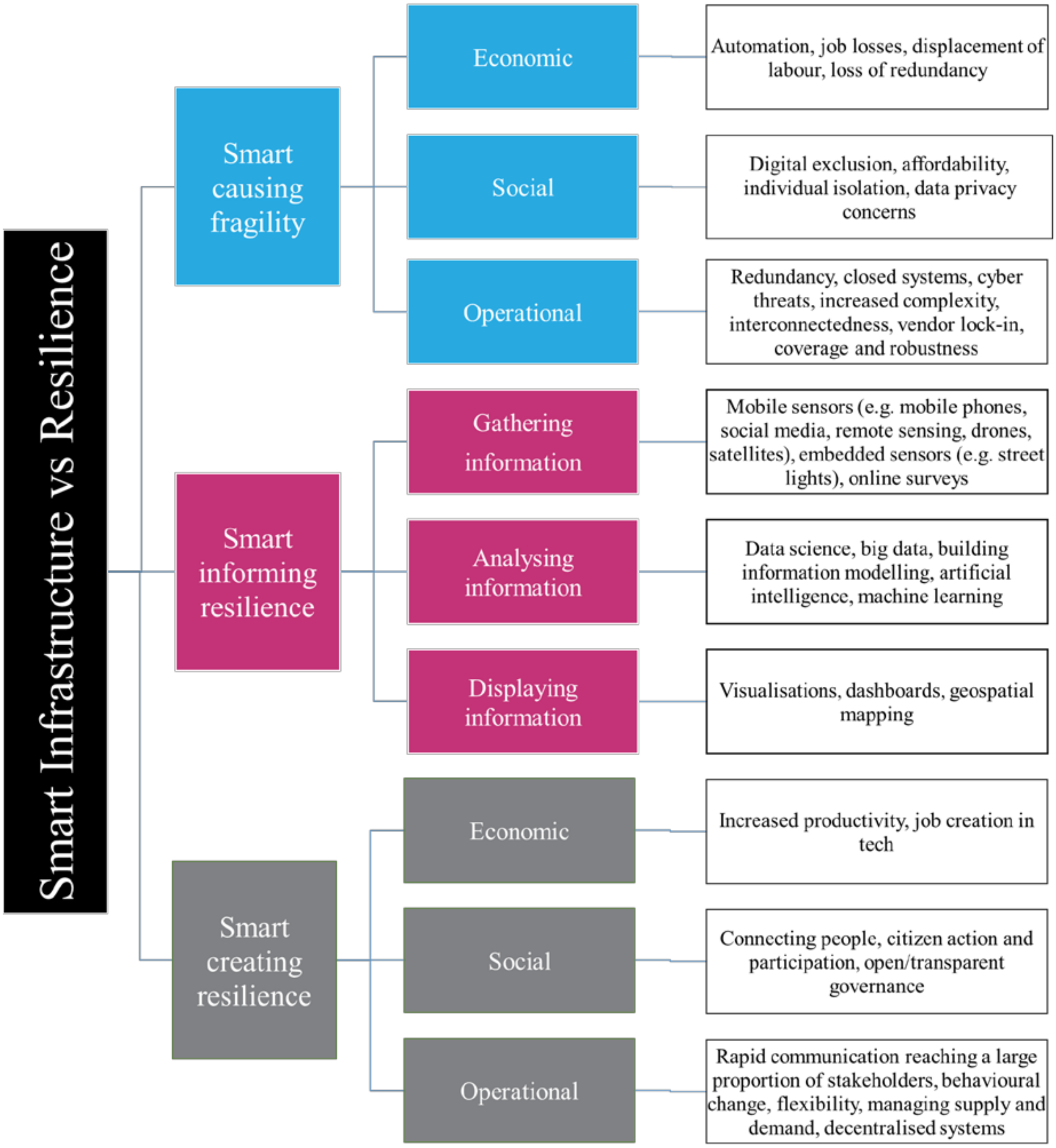

Smart Infrastructure vs Resilience
Smart causing fragility
Economic
Automation, job losses, displacement of labour, loss of redundancy
Social
Digital exclusion, affordability, individual isolation, data privacy concerns
Operational
Redundancy, closed systems, cyber threats, increased complexity, interconnectedness, vendor lock-in, coverage and robustness
Smart informing resilience
Gathering information
Mobile sensors (e.g. mobile phones, social media, remote sensing, drones, satellites), embedded sensors (e.g. street lights), online surveys
Analysing information
Data science, big data, building information modelling, artificial intelligence, machine learning
Displaying information
Visualisations, dashboards, geospatial mapping
Smart creating resilience
Economic
Increased productivity, job creation in tech
Social
Connecting people, citizen action and participation, open/transparent governance
Operational
Rapid communication reaching a large proportion of stakeholders, behavioural change, flexibility, managing supply and demand, decentralised systems

Figure 1. Smart Infrastructure vs Resilience

1.4 Resilience thinking

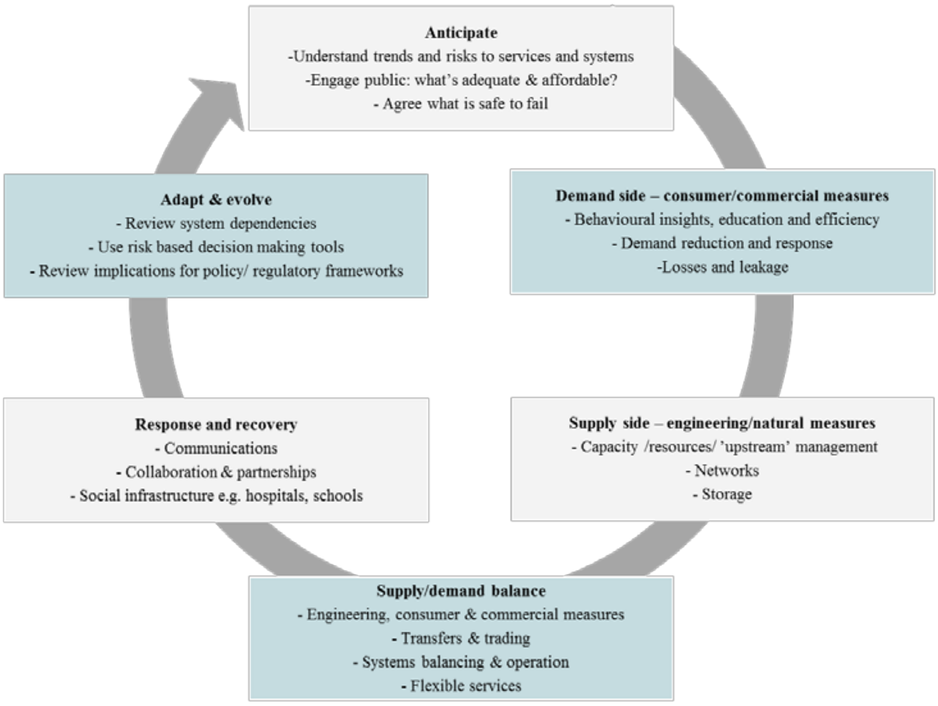

Anticipate
-Understand trends and risks to services and systems
-Engage public: what's adequate & affordable?
- Agree what is safe to fail
Demand side – consumer/commercial measures
- Behavioural insights, education and efficiency
- Demand reduction and response
-Losses and leakage
Supply side – engineering/natural measures
- Capacity /resources/ 'upstream' management
- Networks
- Storage
Supply/demand balance
- Engineering, consumer & commercial measures
- Transfers & trading
- Systems balancing & operation
- Flexible services
Response and recovery
- Communications
- Collaboration & partnerships
- Social infrastructure e.g. hospitals, schools
Adapt & evolve
- Review system dependencies
- Use risk based decision making tools
- Review implications for policy/ regulatory frameworks

Figure 2: Resilience thinking (Adapted from Sustainability First[7])

The components of resilience thinking, illustrated in Figure 2, cover the full cycle from anticipating shocks and stresses and defining acceptable performance; managing supply and demand; through to response and recovery and adapting and evolving post-event. This is a key concept for the issues discussed in this report.

2 Disruption and accidents in digitally-connected infrastructure systems

This section explores whether digitally-connected infrastructure systems are likely to make accidents inevitable, with discussion on the variation between sectors.

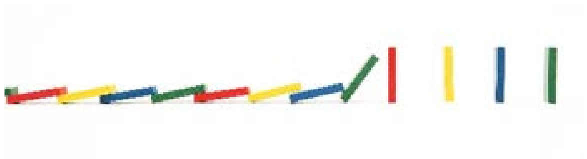
2.1 The inevitability of accidents

A ‘normal accident’ (Perrow, 1984; 2011) 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, or they can even be incomprehensible to those responsible[8]. These are called normal, because although infrequent, we know that nothing is perfect, and it is a normal property of a system to occasionally experience such failures.

Such events are not inevitably catastrophic, and although they can be reduced, they cannot be eliminated[†]. Non-normal accidents, such as component failures, can be planned and prepared for, and in theory, if not in practice, can be eliminated (see Section 2.3).

Normal accidents are only inevitable in high-risk contexts, defined by the two system characteristics described below.

A tightly coupled process ***is one where, once it starts, it cannot be stopped.***



A complex system *is one where the components can interact in unexpected ways, which cannot necessarily be anticipated.*

2.2 Are digitally-connected infrastructure systems high-risk?

Infrastructure systems can be plotted on a matrix of loose to tight coupling, and simple to complex interactivity. Any system that is very complex will inevitably have some components that are tightly coupled. The multiple components of a rail system for example include operators, maintainers, users, environment, physical and digital infrastructure systems, rolling stock, power supply, communications, safety systems etc.

[†] It is worth noting that no case studies of normal accidents leading to significant disruption to infrastructure systems were identified within this study – case studies are typically either normal accidents leading to disruption in other sectors (as in the case of the BA disruption, p10), or non-normal accidents triggered by external threats (malicious intent or floods for example). This does not mean that they haven’t occurred in practice, but they may not have been catastrophic in their impact.

Digitally-connected infrastructure has both the characteristics of tight-coupling and of complexity. Even without a digital ‘overlay’ there are many features of infrastructure systems that have these characteristics, and as systems become increasingly sophisticated (and conversely easier to use), the complexity increases. A characteristic of digital networks is that they suffer ‘brittle’ failure with a failure point that can be conceptualised but is currently hard to predict even when a system is operating near failure point.

Case Study - Transport affected by digital disruption

Transport disruption is one of the most visible examples. There have been several high profile disruptions due to digital system failures in recent months.

In May 2017 there was severe flight disruption to British Airways (BA) flights due to their computer system failing. 75,000 passengers worldwide were affected, with flights being cancelled, delayed and luggage lost. According to BA, it was caused by an “uncontrolled return of power” following an outage that physically damaged servers at its data centre. It was predicted to have cost BA up to £100million in compensation claims[9].

Another recent example was rail ticket machines across the UK being affected by digital system failure in June 2017. Passengers were unable to buy new tickets at stations during the morning rush hour of 22nd June. Southern Rail, Greater Anglia, Great Northern and ScotRail were amongst those affected. It appeared to be a fault with the software systems on the ticket machines[10].

While none of these failures cascaded further, it shows the clear link between digital failures and transport failures.

Case study - Amazon Web Services outage, February 2017

On February 28th 2017 a four hour outage impacted one of Amazon Web Services’ (AWS) largest cloud regions, US-EAST-1 in North America. The cause of the outage was reported by Amazon to be human error, and as AWS had not completely restarted the affected system for some years, “the process of restarting these services and running the necessary safety checks to validate the integrity of the metadata took longer than expected.”[11].

Many users of AWS were affected, including “Internet of Things” providers such as Nest who provide thermostats, CCTV cameras and smoke alarms that are all controlled remotely using AWS capabilities.

The company had not fully understood the complexities of restarting the servers. Changes were implemented as a result, including limiting the amount of capacity that can be removed that quickly, and preventing capacity from being removed when it will take any subsystem below its minimum required capacity level. Although Amazon claims to have 11 nines of durability i.e. 99.999999999% durable, commentators say that there is still a single point of failure, as evidenced by this outage[12].

The Cabinet Office[13] summary resilience plans for each sector, which set out the resilience of the UK's critical infrastructure, focus on significant external threats rather than the potential for a small event to cascade into something catastrophic as a result of tight-coupling and complexity, although dependencies across sectors are considered.

Case Study - Ransomware attack, May 2017

While the cause in this case was malicious, and therefore not a normal accident, the impacts of such an event would be similar due to accidental causes. Countries all over the world were affected. The malware locked user's files and demanded USD$300 payment to decrypt the files, primarily affecting computers running Windows XP, which have not been supported by Microsoft since 2014. In the UK 61 NHS trusts reported issues (out of a total 242 trusts). Consequences included cancelled surgeries, MRI/CT scans and appointments. Some trusts asked people not to attend Accident & Emergency or their GP. Diagnostic services such as blood testing, MRI, CT and X-ray scanning were severely affected[14].

Many other systems across the world were affected including: universities and educational institutions, railway stations, mail delivery, gas stations, office buildings, shopping malls and government services. The Russian Central Bank and Russian Interior Ministry; the Deutsche Bahn (railway service) in Germany; Spanish telecommunications firm Telefónica, FedEx, Renault, Nissan were all impacted by the attack[15], showing how dependent all these organisations are on their digital networks.

2.3 What about non-normal accidents?

Normal accident theory does not imply that all accidents are inevitable. Rather, it makes an important distinction between normal (system) accidents, which are inevitable in high-risk systems, and component failure accidents, which are not inevitable, can be readily anticipated, learnt from and prevented. Where systems are not high-risk, an accident causing a failure of one component can be isolated and is less likely to lead to unanticipated consequences.

Accidents can and do happen that are not within the definition of 'normal'. These should be preventable, but it should not be assumed that all preventable accidents have been, or will be, prevented. New digital technologies have a potential role to play in aiding the process of accident prevention, for example by providing near real-time information on asset condition which can allow for proactive maintenance regimes.

Case Study - Holborn electrical fire, March 2015

The electrical fire occurred in a tunnel beneath a pavement in Holborn and took 36 hours to be put out. 5,000 people were evacuated and there were power cuts in the surrounding area, causing many businesses to close. An electrical fault caused the fire, and the electrical cables shared underground space with gas mains, increasing the complexity of the event. Fibre broadband services were disrupted for several days, causing business to reactively switch to wireless internet services.

As well as directly impacting business, the response to the incident required road closures, causing more widespread travel disruption, and therefore indirectly impacting more businesses. This accident was not a normal accident as it was due to a predictable and preventable electrical fault.

2.4 Summary

Many infrastructure systems are already complexly interactive and tightly coupled to varying degrees. These characteristics lead to infrastructure systems being classified as high-risk systems, and therefore vulnerable to normal accidents.

Avoiding these characteristics in planning, design and construction will enhance resilience. This means explicit consideration of whether a design will increase the tightness of coupling, or whether an intervention will increase the complexity of the connections between any components of a system. These findings are highly relevant to introducing digital systems into existing infrastructure systems.

In all cases when dealing with complex and interdependent systems, there is value in focussing on resilience approaches; the ability to anticipate, absorb, respond, recover and adapt with minimal disruption to services, accepting that unexpected events, and events with unexpected consequences are almost inevitable.

Case Study of cascading infrastructure failures – City of Lancaster, December 2015

Over the first weekend in December 2015, Storm Desmond brought unprecedented flooding to North Lancashire and Cumbria, including to parts of central Lancaster. At 10.45pm on Saturday, 5 December, electricity supplies to 61,000 properties in the city were cut and power cuts continued to cause disruption from the 5th to the 9th December[16]. This resulted from the flooding of just one substation.

Sandbags at Lancaster substation

The failure of electricity supply caused widespread and unanticipated consequences. Whether the original cause was preventable or not, the focus here is on learning from this event to improve the response and recovery process.

- Mobile phone coverage was lost over most of the city, and while landline phone services were available many households had replaced their handsets with cordless phones that rely on electricity to operate.
- Local digital radio services were lost and so only FM services were on air. However, many people did not have battery or wind up radios capable of receiving FM signals.
- Of the FM services that were on air, limited useful reporting meant that the local community were not kept aware of the wider impacts and operational response that was taking place.
- High rise buildings where booster pumps are used to get water to higher floors lost water supply. Buildings that use ‘grey water’ (second-hand water from showers or washing) to flush toilets found that without electricity they were unable to flush toilets.
- The rail station could not be opened after dusk without lighting on the platforms.
- Retail and banking were severely affected by both the floods and the electricity cut: card payment terminals that relied on the internet were not working. As a result, any shops that were open relied on cash only. By contrast, some ATMs that used a conventional phone line to contact the bank and had back up electricity (e.g. through a diesel generator) were operational.

Whilst this event was not a failure in digital systems or a normal accident, it illustrates well the dependence society now has on our digital infrastructure, which has a high degree of coupling with electricity supply. The consequences listed above could have been predicted, and the fact that they were not expected shows how planning and response does not always consider the full ‘system-of-systems’.

3 Enhancing resilience of digitally-connected infrastructure

The need to make digitally-connected infrastructure systems more resilient must be balanced with the benefits offered by the digital components, in order to avoid measures that unduly affect the service offered. Without this consideration, simply removing the digital systems would be a valid solution. Digital systems have the potential to significantly enhance not only efficiency but also resilience, through reducing the potential for human error, and making systems faster, smarter, and more adaptive prior to, during, and following an incident.

Section 2 showed that increasing complexity and inter-connectivity of digitally-connected infrastructure systems creates vulnerabilities to accidents, cascading failures, and unexpected consequences that follow initial accidents and errors. This chapter explores approaches that can help to minimise such vulnerabilities.

Robust risk management procedures are important, to identify what could go wrong and how that can be mitigated. However, there are also more holistic requirements for systems to be able to recover quickly, and adapt even to events that cannot be planned for.

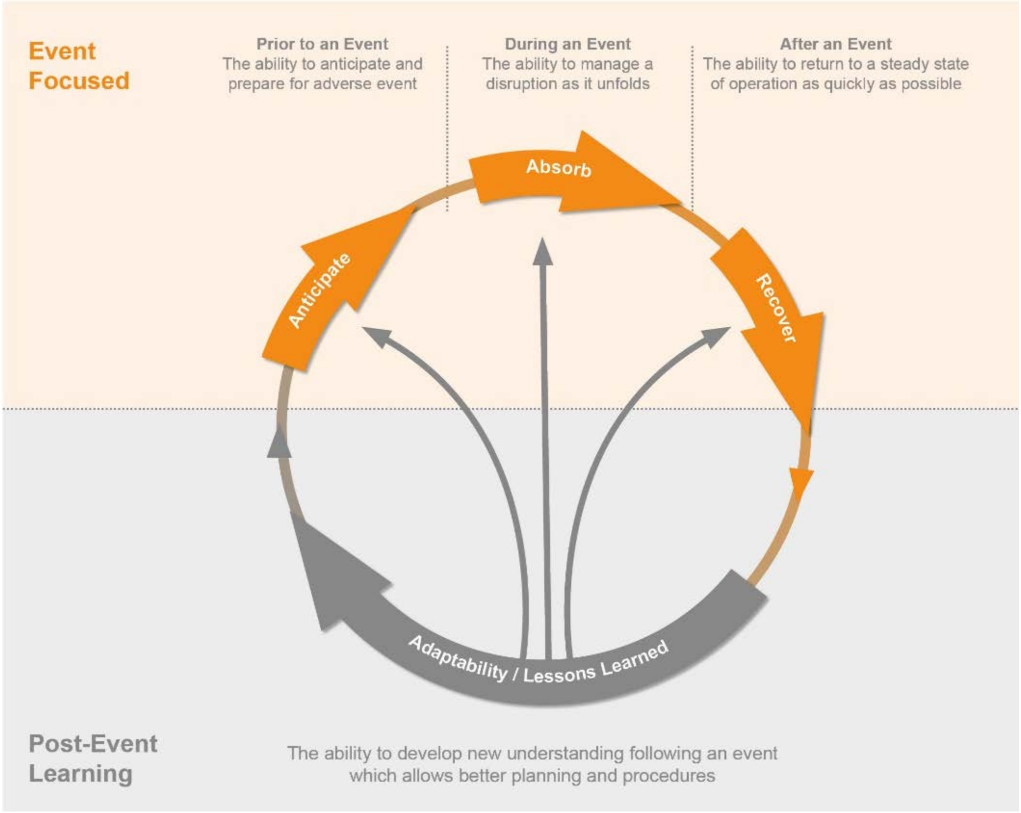

Event Focused
Prior to an Event
The ability to anticipate and prepare for adverse event
During an Event
The ability to manage a disruption as it unfolds
After an Event
The ability to return to a steady state of operation as quickly as possible
Absorb
Anticipate
Recover
Adaptability / Lessons Learned
Post-Event Learning
The ability to develop new understanding following an event which allows better planning and procedures

Figure 3. The resilience construct (adapted from NIAC, 2010[17])

The United States National Infrastructure Advisory Council (NIAC) resilience construct[17] (Figure 3) illustrates the need for a dynamic mind-set and continuous action for systemic resilience. It emphasises four important, time specific abilities of a resilient built system: robustness (prior to the event), resourcefulness (during the event), rapid recovery (after the event) and adaptability/lessons learned (providing feedback throughout).

Appendix D summarises learning from other organisations, and Appendix E summarises best practice used in other sectors. The literature review has provided a full assessment of some of the theory available to support this report[1].

3.1 Learning from High Reliability Organisations

High reliability organisations (HROs) are organisations that follow best practice to minimise the impacts of normal accidents, and normally represent high-risk sectors. Such practice is already embedded into infrastructure systems which are categorised as high risk including nuclear power generation and utility power plants, as well as aviation, chemical plants and offshore oil and gas installations. We have reviewed the principles of HROs in order to identify what may be transferrable into digitally connected infrastructure. This is not the same as recommending that all infrastructure owners/operators in the UK should become HROs.

The five principles underpinning high reliability organisations are that they:

(i) continually track small failures;

(ii) resist simplification of complex tasks;

(iii) are sensitive to operations through continually assessing and updating actual operations, not assuming they are as expected;

(iv) maintain capabilities for resilience through both anticipating potential dangers, and ensuring the capacity to cope with unanticipated dangers (for example retaining manual safeguards); and

(v) monitor shifting locations of expertise – empower those with the greatest experience and expertise to deal with problems.

> *"The hallmark of a high reliability organisation is not that it is error free, rather that an error does not disable it."*[18]

Further observations around high reliability theory include:

- Additional safeguards, introduced into complex systems to mitigate the potential for accidents and errors, will themselves 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).

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. Organisations that find themselves increasingly responsible for complex and tightly-coupled (and hence high-risk) systems should consider the adoption of practices followed by high reliability organisations. This is recommended as a useful starting point, which will improve reliability, but is unlikely to remove all vulnerabilities. HROs are not infallible, and a key feature of adopting the principles should be the importance of knowledge sharing in terms of failure investigations when they do occur.

3.2 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. How Japanese institutions and society respond to earthquake early warning is an excellent example of this (see Appendix D).

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.

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. Notably, there are no passive members of ecosystems (including users). Living systems are *differentiated* and *distributed* – if infrastructure systems were the same that would increase resilience. For example, a transport system where multiple routes are available to connect two nodes, and these routes are managed independently (differentiated). Disruption to customers can therefore be minimised by diverting them to alternative routes to reach their destination.

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[19]. 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 the Department for Transport is responsible for the implementation of the TSIs. New or upgraded projects are required to comply with them.

3.3 Important elements of best practice

To enhance resilience will require a combination of measures. The following headlines describe elements of best practice from different disciplines, described further in Appendix E.

Human factors

Key features: Human factors are required to be considered in various safety critical industries such as defence[20], rail[21], oil and gas, nuclear, aviation[22] 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"[21] , workload, safety and fatigue risk management systems, providing existing models to follow.

Transferrable concepts: Essentially, failing to recognise any infrastructure system as a socio-technical system, and to recognise its interdependence with people, is likely to lead to problems. Socio-technical systems represent large scale systems with large numbers of elements and connections between technical infrastructure (e.g. roads and electricity grids) and the social infrastructure (humans, organisations and governments)[23]. This includes how to communicate and how people respond during and after disruptive events.

For exploration: The impact of digital technologies on human factors, and vice versa is an important area to understand.

Negative synergies

Key feature: Where the sum of equipment, design and operator errors is far greater than the consequences of individual failure.

Transferrable concepts: Failure analysis such as HAZOP or Failure Mode and Effect Analysis, Failure Mode and Effects Criticality Analysis (FMEA and FMECA)[24] help to mitigate the issue of negative synergies through rigorous approaches to define complete failure modes.

Latent errors

Key feature: Errors that in themselves have no direct adverse impacts, but, if unchecked, have the potential for adverse consequences.

Transferrable concepts: Organisations can remove and manage errors from their operations, through considerations of redundancy, flexibility and culture[25].

Organisational procedures

Key feature and transferrable concept: Decentralised decision-making, meaning that those closest and therefore best placed to respond quickly are able to make decisions.

Dynamic and adaptive systems

Key feature and transferrable concept: To increase resilience and reduce recovery time, an organisation must be dynamic in continually planning for, and adapting to, changing external contexts.

The ENCORE Resilience Framework

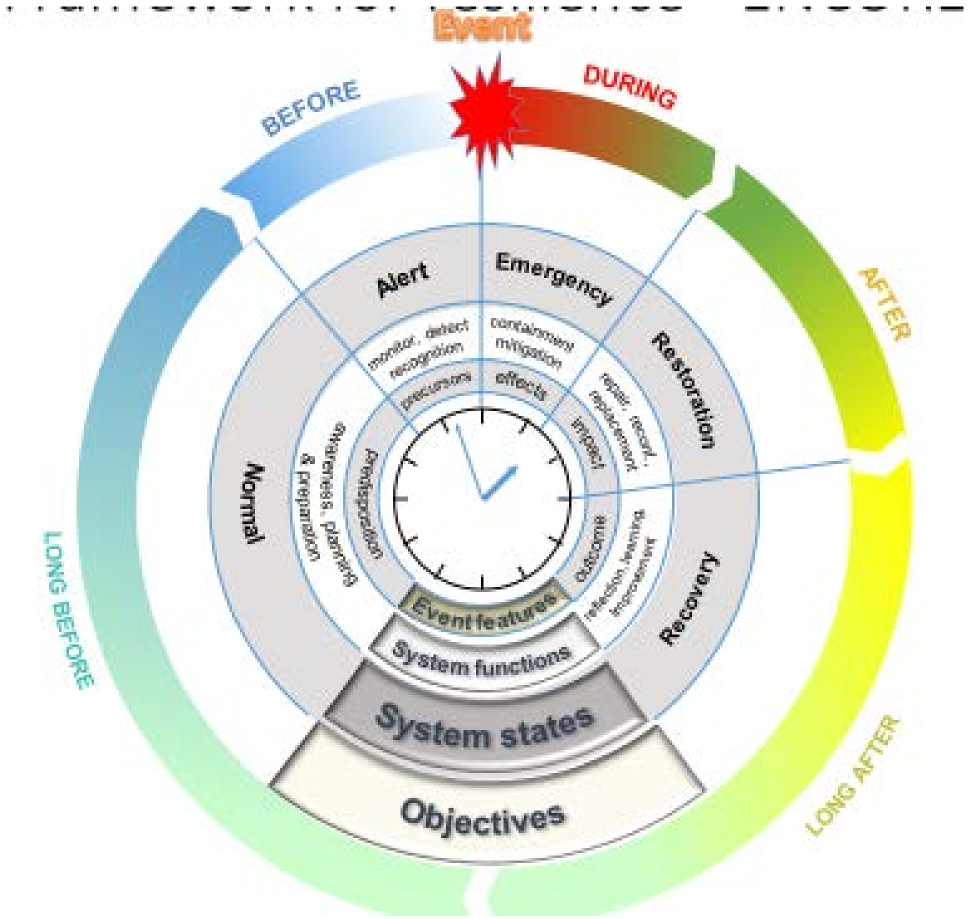


Figure 4. ENCORE Plus Resilience Framework, Source: Punzo et al. (2017)[26]

Resilience Engineering Resilience Engineering is a field of study concerned with the resilience of built systems (including interdependent infrastructure systems) [27], to make resilience a core component of operations.

Tension between resilience and efficiency[28] 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 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) (e.g. Figure 5). The recent launch of the Data and Analytics Facility for National Infrastructure (DAFNI) will create a secure facility for assessing UK infrastructure interdependencies[29].

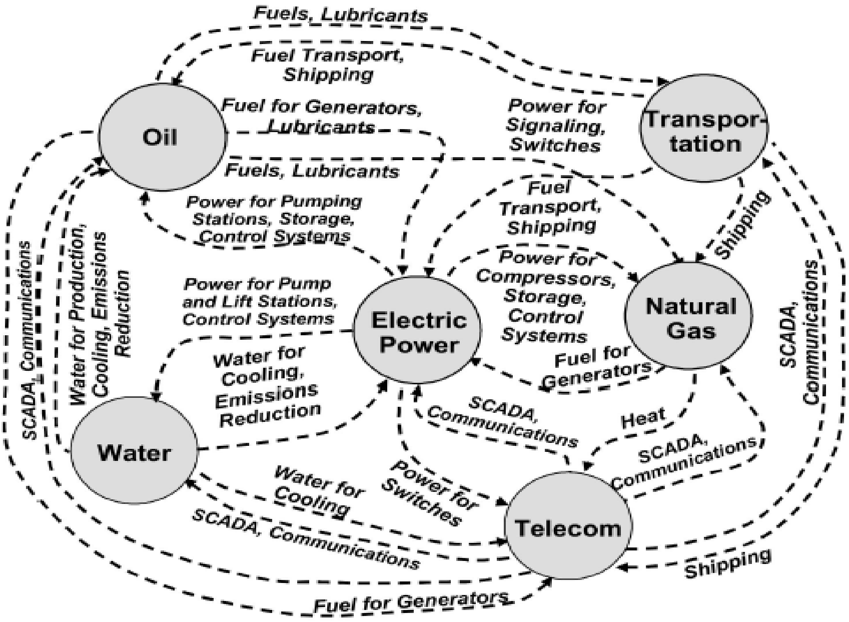


Figure 5. Examples of electric power infrastructure interdependencies[30].

Systemic interdependency analysis

Transferrable concepts: The Interdependency Planning and Management Framework (IP&MF)[31] 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.

Exercises, such as those used by Engineering the Future[32] and Anytown[33] (Figure 6), provide practical methodologies to engage expert knowledge in identifying the most important interdependencies and the possible consequences of these.

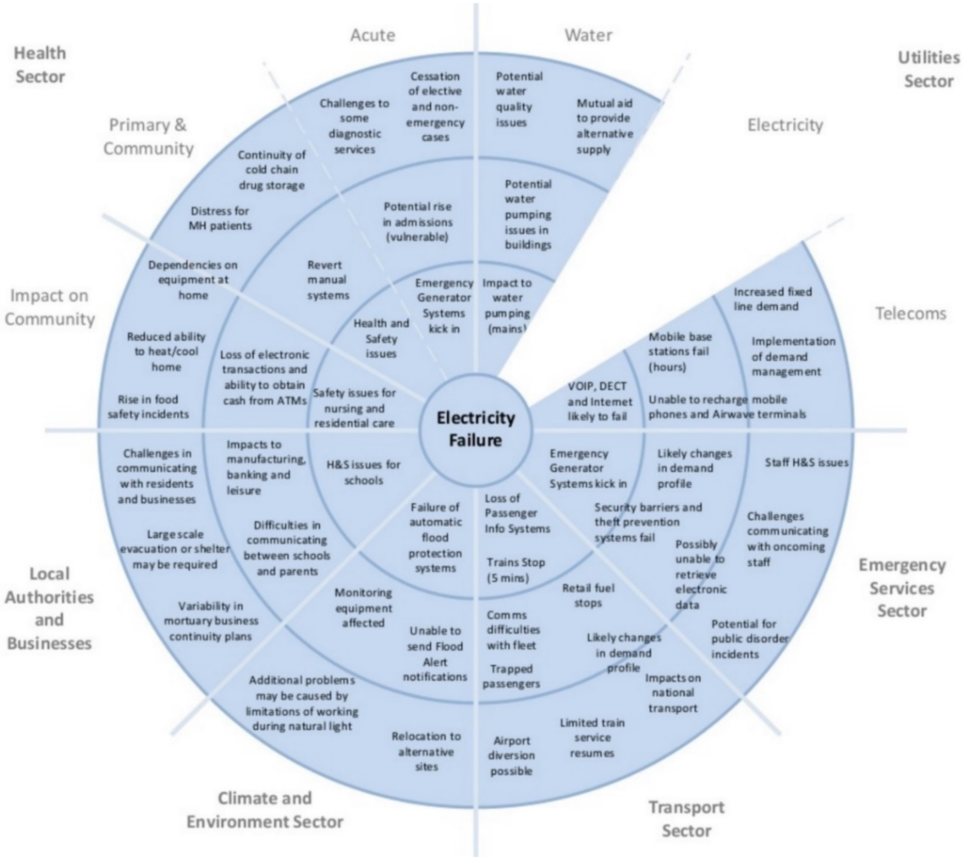

Health Sector
Acute
Water
Utilities Sector
Primary & Community
Electricity
Challenges to some diagnostic services
Cessation of elective and non-emergency cases
Potential water quality issues
Mutual aid to provide alternative supply
Continuity of cold chain drug storage
Distress for MH patients
Potential rise in admissions (vulnerable)
Potential water pumping issues in buildings
Dependencies on equipment at home
Revert manual systems
Emergency Generator Systems kick in
Impact to water pumping (mains)
Increased fixed line demand
Impact on Community
Telecoms
Health and Safety issues
Mobile base stations fail (hours)
Implementation of demand management
Reduced ability to heat/cool home
Loss of electronic transactions and ability to obtain cash from ATMs
Safety issues for nursing and residential care
VOIP, DECT and Internet likely to fail
Unable to recharge mobile phones and Airwave terminals
Rise in food safety incidents
Electricity Failure
Challenges in communicating with residents and businesses
Impacts to manufacturing, banking and leisure
H&S issues for schools
Emergency Generator Systems kick in
Likely changes in demand profile
Staff H&S issues
Failure of automatic flood protection systems
Loss of Passenger Info Systems
Security barriers and theft prevention systems fail
Large scale evacuation or shelter may be required
Difficulties in communicating between schools and parents
Challenges communicating with oncoming staff
Possibly unable to retrieve electronic data
Local Authorities and Businesses
Trains Stop (5 mins)
Emergency Services Sector
Monitoring equipment affected
Retail fuel stops
Variability in mortuary business continuity plans
Comms difficulties with fleet
Unable to send Flood Alert notifications
Likely changes in demand profile
Potential for public disorder incidents
Trapped passengers
Additional problems may be caused by limitations of working during natural light
Impacts on national transport
Limited train service resumes
Relocation to alternative sites
Airport diversion possible
Climate and Environment Sector
Transport Sector

Figure 6. Anytown interdependency “ripple diagram”, used to capture findings from interdependence workshops with front line emergency response professionals[32]

3.4 Summary

The adoption of high reliability organisation principles is unlikely to completely eliminate the risk of normal accidents occurring. If high reliability theory is applied and points (i) and (ii) below are ignored, despite good intentions, the inevitability of normal accidents could actually increase.

i. The interventions prescribed by high reliability organisations need to be implemented in full.

ii. High reliability organisation principles involve direct intervention in a high-risk system, and can inadvertently increase complex interactivity or tighten system coupling.

However, the principles of high reliability organisations, if applied mindfully to reduce complex interactivity and loosen system coupling in digitally-connected infrastructure systems, can have a positive impact.

The body of work on infrastructure systems and interdependency[34,35,36], provides relevant frameworks to build on the concepts of complex interactivity and tight coupling. The Interdependency Planning and Management Framework[31] is one of a range of applicable tools.

A study of resilience could provide useful lessons to reduce the vulnerability of digitally-connected infrastructure systems to normal accidents. One example is the NIAC Resilience Construct (see Figure 3) that views resilient systems as having the abilities to be incident focused prior, during and after an event and adaptable between events.

4 Digital infrastructure: the next 10-30 years

This section explores how the resilience of digitally-connected infrastructure systems might change over the next 10 to 30 years. There are many opportunities in the advancement of digitally-connected infrastructure in the coming years. While these opportunities come with associated threats, technological advances will help to realise efficiencies in the way we design, operate and use our infrastructure. A simple example is the increased use of technology on roads which can manage traffic flows and demand, and reduce congestion.

Appendix F presents a summary of some key cross-sector and sector specific anticipated changes that will lead to increased ability to optimise and automate infrastructure networks and services. Separately, the NIC are currently undertaking a study on how technology can improve infrastructure productivity, which has been supported by a call for evidence[37].

In 2009, the Council for Science and Technology (CST)[38] warned:

> *"We do not believe national infrastructure can continue on its current trajectory …. delivery and governance are 'highly fragmented' and resilience against systemic failure was 'significantly weakening"*

This section reviews the trajectory and uptake of digital technology within our infrastructure sectors, from the perspective of how this may influence findings and recommendations from the earlier sections of the report. This work did not undertake a foresighting study, or attempted to collate all available information on the future of infrastructure.

In principle, it is reasonable to assume that, despite many uncertainties, uptake of digital technologies, and integration of these with every aspect of society, will continue to grow, as illustrated by the following principles.

Metcalfe's Law *The value of a telecommunications network is proportional to the square of the number of connected users of a system. This signifies that the more users are connected, the greater the economic value of that system – a single computer connected to the internet is useless.*

Moore's Law *The number of transistors in a dense integrated circuit doubles approximately every two years. Broadly speaking this means that processing power of computers will continue to increase.*[‡]

The National Needs Assessment[39] summarises the drivers of demand for infrastructure services in the medium term:

[‡] Moore's Law is frequently challenged, either due to physics (computers components cannot continue to get smaller) or business (the benefits become less evident). Nonetheless, the principle of the rapid pace of development of computing power is still relevant for this section.

- Population will be 75 million by 2050, and GDP will continue to grow;
- Total energy demand is expected to move from 900TWh/year to 1200TWh/year, although this depends on technology uptake;
- Housing needs are estimated to be at least 300,000 new homes per year for foreseeable future;
- 26% of morning trains arriving in London were over capacity in 2014;
- Direct cost of road congestion was estimated at £2bn in 2010 and expected to rise to £8.6bn in 2040 if no interventions are made;
- Airports in the UK are delayed more than the European average. It is predicted that Heathrow, Gatwick and Luton will all reach capacity in the next decade; and
- Disruption from flooding is already costing £1bn per year and is only expected to increase in the future due to population growth and climate change.

The NIC's driver paper on technological change[40] presents a review and analysis of how changes in technology could affect the UK's infrastructure in the future, recognising the uncertainty associated with this. The report shows the diverse effects, for example:

- A reduction in demand for some new infrastructure (e.g. through energy efficiency and transport demand management).
- An increase in demand for certain infrastructures (such as electric vehicle charging and data centres).

4.1 Future changes

Some key cross-sector and sector specific anticipated changes – as presented more fully in Appendix F - are as follows:

- Many technological advances will apply across many sectors, such as widespread 5G connectivity that will provide near-total connectivity and allow closer integration of digital and physical infrastructure.
- Computing and information gathering processes such as sensor-generated data, blockchain and crowdsourcing will change the way resources are procured and paid for.
- Technological advances that will affect the UK road network include connected and autonomous vehicles (CAVs), which can increase capacity due to shorter vehicle separation distances, and allow faster cascading of information about incidents to reach vehicles.
- Digital technologies leading to more effective remote working will enhance economic and societal resilience to travel disruption. Conversely resilience of digital networks will be of increasing importance as people come to rely on applications over owning their own mode of transport.

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 and digital systems are embraced without being part of a sound engineering process, along with other checks it could lead to failures being missed.

- The Digital Railway[41] industry programme to enhance capacity and performance of the UK rail sector will increase the complexity of an already complex system, but at the same time, the increased information available, more efficient operations, and opportunities for smarter maintenance approaches will enhance aspects of resilience. This program is also an example of how digital systems can be integrated in both new and legacy infrastructure.
- The energy sector is likely to focus on how technology can increase capacity and reduce demand in the next 10 to 30 years.

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[42].

- 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[43].
- According to DEFRA, efficiency will need to play a significant role in order to achieve a sustainable supply/demand water balance[44]. 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 to facilitate resource trading and information sharing across a large number of autonomous urban water networks[45].
- The increasing sophistication of metering with digital transformation and smart technologies enables more effective monitoring to determine pricing, improves demand management and can provide the potential to reduce leakages via tracking variation in demand. ITRC projects a 100% roll out of smart meters by 2020[46].

4.2 Some observations about data

The creation of new data is a common feature of all of the advances described above. There is an increasing amount of data being collected and stored associated with our infrastructure systems, both in terms of physical assets, and their demand (for example traffic data[47]).

The ICE[48] argues that these datasets needs to be managed as significant assets themselves**Error! Bookmark not defined.**. With the global volume of 'big data' set to grow by approximately 40% year on year for the next decade[49], this will prove a particular challenge for organisations and Government.

However, such data can benefit infrastructure systems through data-driven approaches to infrastructure decision making. There is an increasing utilisation of big data analytics and machine learning as well as developments in artificial intelligence to help inform decision-making. The value of the data being collected and stored should therefore be explicitly realised. Organisations should recognise and exploit existing and emerging data sources, whilst being mindful of any vulnerabilities this approach could create, considering for example:

- Is available data being used to support decision-making in the best way possible?
- Where data is essential to operational decision making, is it being stored and managed in a resilient manner?
- Is the system to collect data, for example through networks sensors or harvesting data from smartphones, resilient? How could this be impacted and recover from shocks and stresses? How would decisions be made in the event of loss of access to data?
- Is a reliance on data replacing the traditional ability to make decisions based on experience and judgement, and if so, are we confident that the appropriate decisions are being made?

The value of data cannot be de-coupled from the storage of data. Data centres, although not always integral to the running of infrastructure networks, may store and provide information regarding asset and system-level information[50]. This can prove vital in enhancing resilience through planning and communications to customers during an incident.

Due to their high energy consumption, data centres are very reliant on energy supply. This interdependency should also be acknowledged.

4.3 How will this affect infrastructure resilience?

Section 4.1 illustrates that most future changes have the potential to increase complexity and coupling, and therefore negatively impact on system resilience. Contrastingly, they present opportunities for example through managing demand, enabling communications to users and increasing the speed of operational responses.

The resilience of a digitally-connected infrastructure system is inherently linked to:

- Pre-existing vulnerabilities within the underlying infrastructure system;
- Vulnerabilities within the digital technologies; and
- New vulnerabilities from the creation of new interdependencies between the digital technology and infrastructure system that comprise the digitally-connected infrastructure system.

Digital technologies cannot be separated from the vulnerabilities in the infrastructure systems they support. Therefore overall, notwithstanding the observation above, that digital technologies will enhance specific aspects of resilience, we conclude that the transformation toward digitally-connected infrastructure systems will:

- Have little impact on the systemic resilience or inherent vulnerabilities in underlying infrastructure systems; and
- Introduce new vulnerabilities into the infrastructure system, and will increase interactive complexity and tighten system coupling.

This leads us to suggest that the trend of declining systemic resilience identified by the Council for Science and Technology[38] will continue as we undergo a digital transformation.

> *"However, there is an excellent opportunity to use best practice to place resilience at the core of all infrastructure planning, delivery and operations, and explicitly prioritise systemic resilience as part of the digital transformation towards a world where all infrastructure systems are digitally-connected infrastructure systems."*[38]

5 Summary

The resilience of digitally-connected infrastructure systems is a multilevel and multi-stakeholder challenge. Resilience requires consideration of technology, society, organisational, environmental and physical systems. No single organisation is responsible for the entire system, and enhancing digitally-connected infrastructure resilience is in fact a global issue. The NIC has an opportunity to provide a “golden thread” that runs through government and industry long term infrastructure planning decisions across all sectors.

A methodology for better addressing resilience, capturing cross-sector issues, digital and physical infrastructure as well as the human elements of the system is required. Enhancing resilience should have a wider perspective than the specific issue of resilience to systemic accidents in digitally-connected infrastructure systems considered in this report. These findings and recommendations, whilst specific to the scope of this report, are relevant to the broader topic of infrastructure resilience to all hazards.

Our recommendations are underpinned by the following important findings:

1. The need to enhance the resilience of digitally-connected infrastructure must be **balanced with the benefits** of digital systems (for example demand management, reducing the potential for human error, and making systems faster, smarter, and more adaptive prior to, during, and following an incident), in order to avoid introducing measures that unduly affect the service offered.
2. Digital systems, overlain onto existing, legacy, infrastructure, cannot fully remove the inherent vulnerabilities in this existing infrastructure. They will in fact add complexity to already complex systems, and this has been observed to potentially lead to unintended consequences.
3. If digital technologies are not to undermine system resilience, their introduction and planning must be grounded in deep understanding of the systemic context in which they are implemented. **This means that resilience of infrastructure systems cannot be managed solely at sector level or by engineering interventions, but will require a cross sector approach.**

5.1 Recommendations

Resilience thinking should be embedded in all infrastructure systems – flexible approaches, which allow systems to respond, recover, adapt and evolve, as well as anticipating and absorbing shocks, are essential to provide continued services. Each principal infrastructure system needs a high level “controlling mind” to own the issue of digital resilience. This could be organisations such as National Grid, National Air Traffic Services, Network Rail or Highways England. Where no controlling mind exists, one should be identified. They should be challenged to create active resilience plans so that the issue is mapped, including interdependencies to other related systems.

To support and promote resilience thinking, infrastructure sectors should more widely **learn from other organisations** (see Section 5.2), such as high reliability organisations, or those who have previously suffered an event impact and have recovered appropriately. Gaining such knowledge of systems recovery is increasingly important as digitally-connected infrastructure systems become inherently more complex and tightly coupled. It is also important that infrastructure sectors **share lessons and insights** between themselves.

This is subtly but importantly different from recommending that infrastructure companies *become* High Reliability Organisations, which could be over-prescriptive and create new vulnerabilities if not fully implemented or embraced.

Interaction should be sought across all infrastructure sectors through working with the appropriate Government departments and with regulators (for example through the UK Regulators Network). Cross-government interaction will continue to be essential to share lessons, developments and priorities, and examine interdependency issues. For example, the annual update of the *National Risk Assessment* and the sector specific *Sector Security and Resilience Plans* produced by the Cabinet Office may include recommendations for specific interdependencies between infrastructure and digital networks, and therefore infrastructure planning should reflect these findings.

As outlined in Section 3.3, understanding interdependencies will be essential to manage the complexity of digitally-connected infrastructure. **Simulations** (both actual and virtual) and **workshops** will aid understanding of the interdependencies between digital systems and other infrastructure systems. Models at a city scale are now possible, and when combined with advanced system models or “digital twins”, they could be effective in deepening understanding of digital resilience[§].

Digital networks are likely to be split into demonstrably secure sector communications and conventional public internet in the future. Secure networks, although being developed in silos, would benefit from a **common processes, architecture and oversight** across all the sectors where they are being developed, to avoid the creation of unforeseen problems in the future. In creating this architecture there should be a “no regrets” policy i.e. retain adaptability and avoid locking systems into one option only.

Data should be valued explicitly (Section 4.1), and the benefits of collecting, storing and using data should be considered at project planning stages. If the full potential of digitally-connected infrastructure systems to improve our infrastructure is to be realised, organisational tools are needed to purposefully convert data into meaningful information that enables more effective decision making as well as ensuring that data does not stay in silos and data is actively transferred between, within and beyond infrastructure systems in a safe way, in order to fully realise its decision-making potential. The value of data cannot be de-coupled from the storage of data. **Data centres**, for example, even if located

[§] Note that the security implications of developing model simulations of infrastructure systems are outside the scope of this study.

outside the UK, should be recognised in infrastructure planning in order to safeguard them.

Infrastructure operators are gradually deploying more data-driven components to improve operation of physical infrastructure, and to make the most out of these, independent elements should be transformed into a more cohesive '**overlay network**' as recommended by the Smart Water Networks Forum, UK[51]. This is applicable to more than just water networks.

5.2 Learning from best practice

Infrastructure operators should be aware that the networks they are responsible for are increasingly likely to have the characteristics of high risk systems, and should therefore seek to learn from relevant best practice.

In seeking to identify best practice, it is worth considering the four components of resilient systems; the ability to anticipate, absorb, recover from and adapt to shocks and stresses. Robust risk management procedures are important, to identify what could go wrong and how that can be mitigated, but there are also more holistic requirements for systems to be able to recover quickly, and adapt even to events that may not have been identified. Specific considerations include:

- A dynamic approach to all phases of the resilience cycle (Figure 3), through regular evaluation, and regular review of interdependencies.

- Physical simulation exercises can be hugely beneficial in enabling government and society to prepare for, anticipate and respond to events, and the potential for modelling and virtual simulation (using "digital twins") is increasing. The recent launch of DAFNI[29] will help the UK to accelerate and realise such modelling capabilities in a secure environment.

- Explicitly documenting in all infrastructure developments that digital systems cannot be decoupled from their electricity supply and vice versa.

When planning and assessing digitally-connected infrastructure systems a productive mind-set to draw from the normal accident theory explored in Section 2 is to understand that not all accidents are preventable in complex, tightly coupled systems. Planning, design and construction should therefore explicitly consider whether decisions will increase the tightness of coupling, or whether an intervention will increase the complexity of the connections between any components of a system. While avoidance is not always going to be possible, awareness is essential.

The five principles that underpin high reliability organisations are that they:

- continually track small failures

- resist over simplification

- are sensitive to operations

- maintain capabilities for resilience

- monitor shifting locations of expertise

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

5.3 Knowledge gaps and areas of further research

A **consistent methodology** for specific studies based on the principles of systemic resilience, infrastructure as a complex system and interdependency analysis should be developed. This should include the interdependency planning and management framework (IP&MF), an approach that was commissioned by HM Treasury to make planning for interdependencies an explicit part of any infrastructure project. Developing the IP&MF for digitally-connected infrastructure systems would be beneficial.

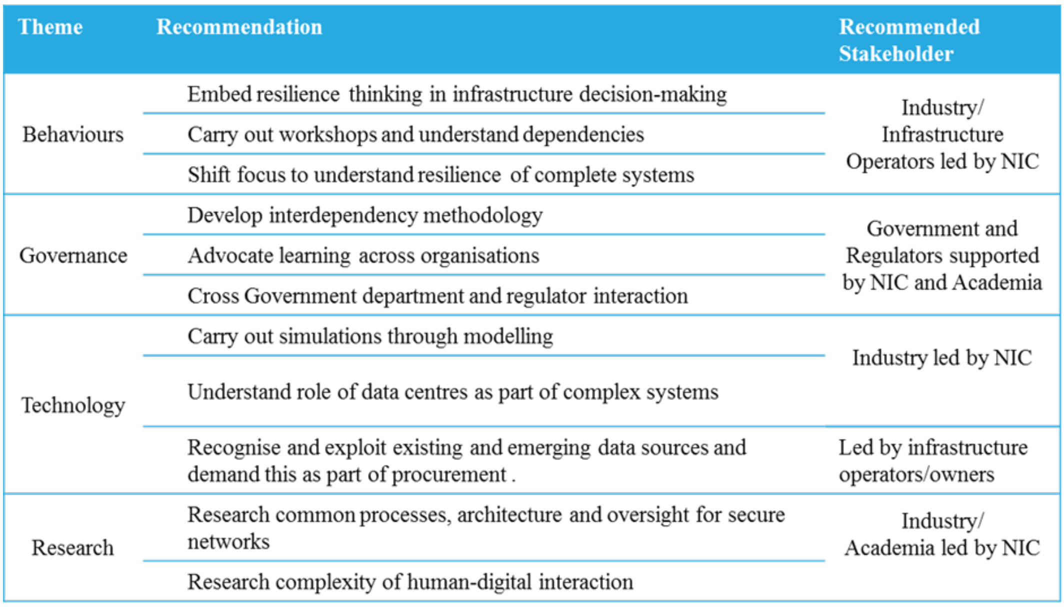
Focus should be directed towards dealing with vulnerability to accidents and disruption as systems become more complex and tightly coupled. There is also a need to identify the long term value of reducing disruptions to infrastructure, noting that conducting sector-specific analysis and fully implementing recommendations will require leveraging the expertise and resources of the relevant organisations operating across this space.

Consideration around the trade-off between systemic resiliency and efficiency should become explicit in decision making. Additionally, the affordability question should be reframed from “how much will resilience cost?” to “can we afford not to be resilient?”

The **impact of digital technologies on human factors**, and vice versa is an important area to understand.

Further recommendations for research are presented in the literature review[1].

The recommendations above are summarised below and in Figure 7 broken down into their relevance to people, technology and processes.



Theme	Recommendation	Recommended Stakeholder
Behaviours	Embed resilience thinking in infrastructure decision-making	Industry/ Infrastructure Operators led by NIC
	Carry out workshops and understand dependencies	
	Shift focus to understand resilience of complete systems	
Governance	Develop interdependency methodology	Government and Regulators supported by NIC and Academia
	Advocate learning across organisations	
	Cross Government department and regulator interaction	
Technology	Carry out simulations through modelling	Industry led by NIC
	Understand role of data centres as part of complex systems	
	Recognise and exploit existing and emerging data sources and demand this as part of procurement .	Led by infrastructure operators/owners
Research	Research common processes, architecture and oversight for secure networks	Industry/ Academia led by NIC
	Research complexity of human-digital interaction	

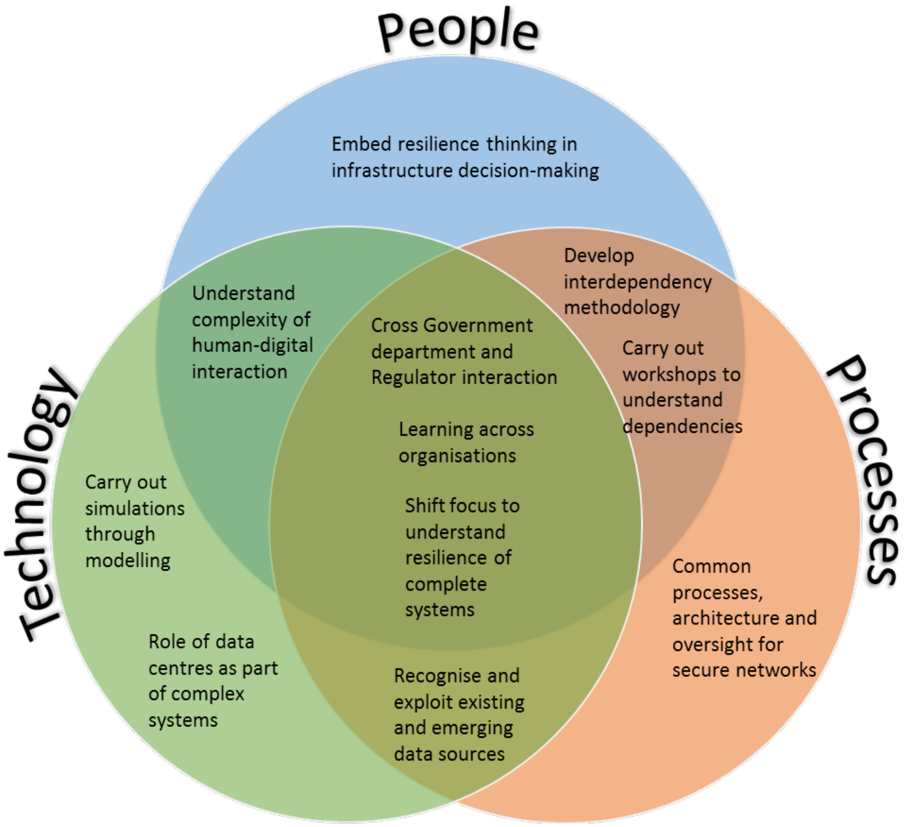

People
Technology
Processes
Embed resilience thinking in infrastructure decision-making
Understand complexity of human-digital interaction
Cross Government department and Regulator interaction
Develop interdependency methodology
Carry out workshops to understand dependencies
Learning across organisations
Shift focus to understand resilience of complete systems
Carry out simulations through modelling
Role of data centres as part of complex systems
Recognise and exploit existing and emerging data sources
Common processes, architecture and oversight for secure networks

Figure 7. Recommendations to increase the resilience of digitally-connected infrastructure systems

[1] UCL, 2017, CCCC17A21 Digitally Connected Infrastructure System Resilience Literature Review

[2] Arup, 2017, NIC Infrastructure and Digital Systems Resilience Industry Panel Workshop #1 Factual Report

[3] Arup, 2017, NIC Infrastructure and Digital Systems Resilience Industry Panel Workshop #2 Factual Report

[4] Pinsent Masons (2017) The evolution of Infratech. How technology is shaping the future of infrastructure.

[5] https://data.london.gov.uk/blog/integrating-infrastructure-data-publishing-a-first-version-of-the-london-infrastructure-map/

[6] Defra, 2013, Defra Open Data Strategy. https://www.gov.uk/government/publications/defra-open-data-strategy

[7] Sustainability First, 2017, accessed June 2017, Long-run resilience in the energy and water sectors. Discussion paper. http://www.sustainabilityfirst.org.uk/images/publications/new-pin/New-Pin_Long-run_resilience._Discussion_paper_-_FINAL.pdf

[8] Perrow, C., 2011, Normal Accidents: Living with High Risk Technologies.

[9] The Guardian, accessed June 2017, https://www.theguardian.com/business/2017/may/31/ba-it-shutdown-caused-by-uncontrolled-return-of-power-after-outage.

[10] BBC News, accessed July 2017, http://www.bbc.co.uk/news/technology-40367628

[11] Amazon Web Services, 2017, accessed 9 June 2016, Summary of the Amazon S3 Service Disruption in the Northern Virginia (US-EAST-1) Region https://aws.amazon.com/message/41926/

[12] Storage OS, Surviving an AWS outage: Multi-Region Storage, accessed July 2017, https://storageos.com/surviving-an-aws-outage-multi-region-storage/

[13] Cabinet Office, 2016 Summary of the 2015-16 Sector Resilience Plans https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/526351/2015_16_summary_of_the_srp.pdf

[14] BBC, 2017, accessed May 2017, Ransomware and the NHS – the inquest begins, Rory Cellan-Jones http://www.bbc.co.uk/news/technology-39917278

[15] CNN, 2017, accessed May 2017, http://money.cnn.com/2017/05/13/technology/ransomware-attack-who-got-hurt

[16] Royal Academy of Engineering, 2016, Living Without Electricity, http://www.raeng.org.uk/publications/reports/living-without-electricity

[17] National Infrastructure Advisory Council, 2010, A framework for establishing critical infrastructure resilience goals: Final report and recommendations from the Council, October 19, 2010. https://www.dhs.gov/xlibrary/assets/niac/niac-a-framework-for-establishing-critical-infrastructure-resilience-goals-2010-10-19.pdf

[18] Weick, K.E., Sutcliffe, K.M., 2007, Managing the Unexpected: Resilient Performance in an Age of Uncertainty, 2nd Revised edition edition. ed. John Wiley & Sons, San Francisco

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

[20] Chartered Institute of Ergonomics & Human Factors, Defence Homepage, accessed July 2017, http://www.ergonomics.org.uk/defence/

[21] 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

[22] Civil Aviation Authority, 2017, accessed July 2017, Human Factors, http://www.caa.co.uk/Safety-initiatives-and-resources/Working-with-industry/Human-factors/Human-factors/

[23] Chappin, EJL & van der Lei, T, 2014, Adaptation of interconnected infrastructures to climate change: A socio-technical systems perspective. Utilities Policy. 31: 10-17.

[24] British Standards Institute, 2010, Risk management – risk assessment techniques BS EN 31010:2010

[25] Hoffman, D. & Frese, M. (Eds), 2011, Errors in Organizations. Taylor & Francis

[26] 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

[27] Hollnagel, E., 2014, Resilience engineering and the built environment. Build. Res. Inf. 42, 221-8

[28] Lloyds Register Foundation, 2015, Foresight Review of Resilience Engineering: Designing for the expected and unexpected. Lloyds Register Foundation, London.

[29] ITRC Mistral, Data and Analytics Facility for National Infrastructure (DAFNI) Launch: http://www.itrc.org.uk/dafni-data-and-analytics-facility-for-national-infrastructure/dafni-launch/#.WYBzIIjyvmE

[30] 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).

[31] 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.

[32] 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.

[33] Hogan, M., 2013, Anytown Final Report.pdf. London resilience, London.

[34] Rinaldi, S.M., Peerenboom, J.P., Kelly, T.K., 2001, Identifying, understanding, and analyzing critical infrastructure interdependencies. IEEE Control Syst. Mag. 21, 11–25

[35] Vespignani, A., 2010, Complex networks: The fragility of interdependency. Nature 464, 984–5.

[36] Boin, A., McConnell, A., 2007, Preparing for critical infrastructure breakdowns: The limits of crisis management and the need for resilience. J. Contingencies Crisis Manag. 15, 50–59.

[37] National Infrastructure Commission, 2016, Technology Study Call for Evidence. https://www.nic.org.uk/wp-content/uploads/Technology-Study-Call-for-Evidence-Accessible.pdf

[38] Council for Science and Technology, 2009, A National Infrastructure for the 21st Century. http://webarchive.nationalarchives.gov.uk/+/http:/www.cst.gov.uk/reports/files/national-infrastructure-report.pdf

[39] 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

[40] National Infrastructure Commission, 2017, The impact of technological change on future infrastructure supply and demand. https://www.nic.org.uk/wp-content/uploads/2905991-NIC-TECHNICAL-v0_5-ACCESSIBLE.pdf

[41] Digital Railway, accessed July 2017, Homepage, http://digitalrailway.co.uk/

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

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

[44] 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

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

[46] 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

[47] Parliamentary Office of Science and Technology, 2014, Big and Open Data in Transport. House of Parliament, POSTNOTE, Number 472, July 2014.

[48] ICE (2017) State of the Nation 2017: Digital Transformation

[49] Parliamentary Office of Science and Technology, 2014, Big Data: An Overview. House of Parliament, POSTNOTE, Number 468, July 2014.

[50] https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/consultancy/deloitte-uk-network-rail.pdf

[51]Smart Water Network, accessed July 2017, Homepage, https://www.swan-forum.com/resources/what-is-a-swn/