National Infrastructure Commission

Digitally Connected Infrastructure System Resilience

Literature Review (UCL)

August 2017

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

UCL ARUP

Literature Review: Content

Page

1 Introduction and Context 1

1.1 Purpose 1
1.2 Focus 1
1.3 Structure 2

2 Normal Accident Theory (NAT) Literature 3

2.1 Brief Overview of NAT 3
2.2 Significant Messages from NAT 7
2.3 Key concepts proposed by or used in NAT 9
2.4 Application of NAT to Infrastructure Systems 10

3 Learning from High Reliability Organisation (HRO), Systemic Resilience Studies, Infrastructure Interdependence and Systems Thinking 13

3.1 Overview of High Reliability Organising (HRO) 13
3.2 The Relationship between HRO and NAT 17
3.3 Resilience as a System Property 19
3.4 Infrastructure Interdependence 26
3.5 Infrastructure as a Complex Adaptive Systems 40
3.6 Summary of Best Practise Findings from Literature Review 45

4 Digitally Connected Infrastructure Systems' Resilience to Future Change 49

5 Key recommendations from Literature Review 51

5.1 Recommendation A: Apply LTS theory and CAS thinking to analyse digital transformation impacts and DCIS resilience 51
5.2 Recommendation B: Prioritise organisational paradigms and thinking tools to support Resilient Digital Transformation 52
5.3 Recommendation C: Make systemic resilience a core objective of DCIS planning 52
5.4 Recommendation D: Develop an interdependency toolkit for DCIS systemic resilience analysis 53
5.5 Recommendation E: Define DCIS explicitly in terms of interdependency with underlying infrastructure systems 53
5.6 Recommendation F: Adopt a more nuanced approach to NAT in Infrastructure Systems 54
5.7 Recommendation G: Adapt HRO to develop a set of HR Complex System principles 54
5.8 Recommendation H: Undertake research to assess application of Meadows (n.d.) to DCIS planning 54

6 Reference List 55

Tables

Table 1. Summary of terms to characterise complex and linear systems (Perrow, 2011:p88) 6
Table 2. Tight and Loose Coupling Tendencies (Perrow, 2011:p96) 6
Table 3. Terminology or Concepts from NAT 10
Table 4. High Reliability and Mindfulness and HRO Principles (adapted from Weick and Sutcliffe, 2007) 15
Table 5. HRO Principles (adapted from Weick and Sutcliffe, 2007) 16
Table 6. Competing Perspectives on Safety with Hazardous Technologies (reproduced from Sagan, 1995: P46) 18
Table 7. Components of Ecological Resilience and Significance for Infrastructure 22
Table 8 SES Attributes of a Dynamic System (Source: Walker et al. 2004) 23
Table 9. Four Abilities of a Resilient Built System (Source: Hollnagel, 2014) 24
Table 10. Strategic Resilience Challenges (adapted from Hamel and Valikanagas, 2003) 25
Table 11. Interdependency Dimensions Overview (adapted from Rinaldi et al. (2001). 30
Table 12. Infrastructure Interdependency Characterisation Checklist 37
Table 13 Summary Table of Literature Review Best Practise Findings – HRO 45
Table 14 Summary Table of Literature Review Best Practise Findings – Interdependence 46
Table 15. Summary Table of Literature Review Best Practise Findings – Systemic Resilience 47
Table 16. Summary Table of Literature Review Best Practise Findings – Systemic Perspectives 48

Figures

Figure 1. Interaction/Coupling Chart (Perrow, 2011:p97) 5
Figure 2. The NIAC Resilience Construct (Source: NIAC, 2010) 20
Figure 3. ENCORE Plus Resilience Framework (Source: Punzo et al., 2017) 21
Figure 4. Dimensions for Describing Infrastructure Interdependencies (Source: Rinaldi et al., 2001) 27
Figure 5. Examples of electric power infrastructure dependencies (Source: Rinaldi et al. 2001). 28
Figure 6. Examples of infrastructure interdependencies (Source: Rinaldi et al. 2001). 29
Figure 7. Interdependency Matrix applied to Interdependency between Sectors (Source: RAEng, 2011) 35
Figure 8. Interdependency Matrix in General Form (Source: Personal communication with Dr Neil Carhart, 2015) 35
Figure 9. Simplified version of Figure 8 for interdependence between two components (Source: Personal communication with Dr Neil Carhart, 2015) 36
Figure 10. Anytown Interdependency Ripple Diagram 39

Figure 11. Example of Systemic Interdependency Mapping for ICT Infrastructure (Source: Beckford Consulting, 2009) 40
Figure 12. Infrastructure Enables Society - Society Demands Outcomes - Infrastructure as CAS (Source: Beckford, 2013) 42

1 Introduction and Context

1.1 Purpose

This literature review was produced by Dr Tom Dolan, Senior Research Associate ICIF and UKCRIC, UCL on behalf of UCL and Arup for the National Infrastructure Commission.

The literature review presents and critiques key areas of academic literature relevant to four research questions on digitally connected infrastructure systems (DCIS) posed by the National Infrastructure Commission (NIC). The review provides additional context to support analysis, findings and recommendations presented in the main project report, and can be read as in conjunction with the report or as a standalone document.

Digitally Connected Infrastructure System (DCIS) Research Questions

1. What lessons can we learn from Normal Accident Theory (NAT) in order to exploit the benefits of digitally connected infrastructure systems (DCIS), whilst minimising the creation, and maximising awareness, of the potential for digitally enabled vulnerabilities?
2. How do we make digitally connected infrastructure systems (DCIS) more resilient and what current practices are used, for example in high reliability organisations?
3. How might the resilience of digitally connected infrastructure systems (DCIS) change over the next 10 to 30 years?
4. What key recommendations would we make to reduce the frequency of normal accidents in digitally connected infrastructure systems (DCIS), and for areas of further research?

1.2 Focus

The literature review is focused on:

i) Normal accident theory (NAT) and related literature (section 2),

ii) High reliability organisations (HRO) and related literature (section 3),

iii) Literature inspired by and building on either NAT and/or HRO in ways relevant to the above questions. (section 3)

iv) Interdisciplinary literature on the topics of resilience and systemic resilience (sections 3)

v) Conceptual literature on infrastructure interdependence and the significance of interdependence to NAT and systemic analysis

vi) Research literature relevant to NAT and HRO, drawn from disciplines independent of the safety literature of which NAT and HRO are a part.

Specifically, literature on systems, complex systems, complex adaptive systems and large technical systems

vii) Research literature from current UK and international interdisciplinary research into interdependent infrastructure systems (e.g. ICIF, iBUILD, ITRC, Mistral, UKCRIC, Liveable Cities) and international supporters of ISNGI (e.g. University of Wollongong SMART IF, TU Delft, IIASA, University Technology Sydney, University of Auckland. (sections 2, 3 and 4)

viii) Selected influential technical or government reports from non-academic sources. (sections 2 and 3)

1.3 Structure

For consistency with the main report, the literature review presented here has been divided into 5 sections. Section 1 provides context for the study and an overview of how the literature review is structured. Sections 2 and 3 introduce, outline and critique key concepts from relevant academic literature, and offer responses to questions 1 and 2. Sections 4 and 5 address questions 3 and 4 respectively, drawing on the literature in sections 2 and 3.

2 Normal Accident Theory (NAT) Literature

Introduction

This section of the literature review is focused on the question:

> *What lessons can we learn from Normal Accident Theory (NAT) in order to exploit the benefits of digitally connected infrastructure systems (DCIS), whilst minimising the creation, and maximising awareness, of the potential for digitally enabled vulnerabilities?*

The initial of focus of the review of NAT literature was to examine the question *Are digitally connected infrastructure systems (DCIS), as they develop, likely to make normal accidents inevitable?* However, following initial scoping, the question was re-framed to the above to broaden the scope of the study and identify transferable lessons for digitally connected infrastructure systems (DCIS) from NAT.

Section 2.1 provides an overview of Normal Accident Theory (NAT); section 2.2 presents key messages from NAT; section 2.3 collates important concepts or terminology connected to NAT (Table 3); section 2.4, applies NAT to address the above question(s).

2.1 Brief Overview of NAT

The work of Charles Perrow which led to his 1981 publication of *Normal Accidents living with high-risk technologies* (Perrow, 2011) was motivated by the possibility of improving the ways in which high-risk technologies are managed. Normal Accident Theory (NAT) identifies two system characteristics present in high-risk technologies [organisations or systems], and defines these as 'interactive complexity' and 'tight coupling'(Perrow, 2011).

> System Coupling – the components of a technology, organisation or system can be either loosely or tightly bound. Tight coupling is where *'processes happen very fast and can't be turned off, the parts cannot be isolated from other parts, or there is no other way to keep the production going safely.'*
>
> System Interactions - interactions between system components can either be linear or complex. Interactive complexity is where *'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; we call it the interactive complexity of the system.'*

NAT asserts that when these system characteristics are present in a technology the result is a *high-risk* technology, from which risk, regardless of the efficacy of conventional safety devices, can never be completely eliminated. NAT postulates that in these high-risk technologies, a specific type of accident is inevitable. The term Normal Accident (also system accident) refers to this type of accident. NAT

is the study of the emergence of *high-risk* in technologies, organisations and systems, or any situation where *tight coupling* and *interactive complexity* are possible.

In NAT, *high-risk* is characterised as the presence of both *interactive complexity* and *tight coupling*. In *high-risk* systems, the occurrence of normal accidents although uncommon, even rare, is an inevitable emergent property i.e. normal accidents are inevitable in any system that has the properties of complex interactivity and tight coupling. The emphasis on high-risk as an emergent property highlights that it is through interactions (interdependencies) that *high-risk* emerges. *High risk* is not, therefore, a property of any single component, rather the system as whole.

Explanation of the term Normal Accident

Perrow, (2011) explains his choice of the term 'Normal Accident' as follows:

"when we have interactive systems that are also tightly coupled, it is ***normal*** *for them to have this kind of [normal] accident, even though it is infrequent. It is* ***normal*** *not in the sense of being frequent or being expected – indeed, neither is true, which is why we are so baffled when by what went wrong [when a normal accident occurs]. It is* ***normal*** *in the sense that it is an inherent property of the system to occasionally experience this interaction [a normal accident]." (P8)* (Perrow, 2011)

Explanation of inevitability of Normal Accidents

In an Afterword to the second edition, Perrow (2011) provides further elaboration on why NAT concludes normal accidents are inevitable:

"let me review this more explicitly. Nothing is perfect, neither designs, equipment, procedures, operators, supplies, or the environment. Because we know this, we load our complex systems and safety devices in the forms of buffers, redundancies, circuit breakers, alarms, bells, and whistles. Small failures go on continuously in the system since nothing is perfect, but the safety devices and the cunning of designers, and the wit and experience the operating personnel, cope with them. Occasionally, however, two or more failures, none of them devastating in themselves in isolation, come together in unexpected ways and defeat the safety devices – the definition of 'normal accident' or system accident. If the system is also tightly coupled, these failures can cascade faster than any safety device operator can cope with them, or they can even be incomprehensible to those responsible for doing the coping. If the accident brings down a significant part of the system, and the system has catastrophic potential, we will have a catastrophe. That, in brief, is Normal Accident Theory" (Perrow, 2011)

Box 1. Explanation of term 'normal accidents'

In depth analysis of the two system characteristics 'interactive complexity' and 'tight coupling' that constitute *a high-risk* technology, organisations or systems is

essential to apply NAT in any specific context. To support this analysis, greater definition of the two system characteristics 'interactive complexity' and 'tight coupling' are provided Table 1 and Table 2. Furthermore, subsequent sections of this literature review outline how infrastructure interdependencies, a systemic perspective, the principles of systemic resilience and HRO can provide conceptual tools to support analysis.

Figure 1 demonstrates how comparative analysis of systems can be visualised using a 2x2 matrix to classify the current state of system interactions and system coupling.

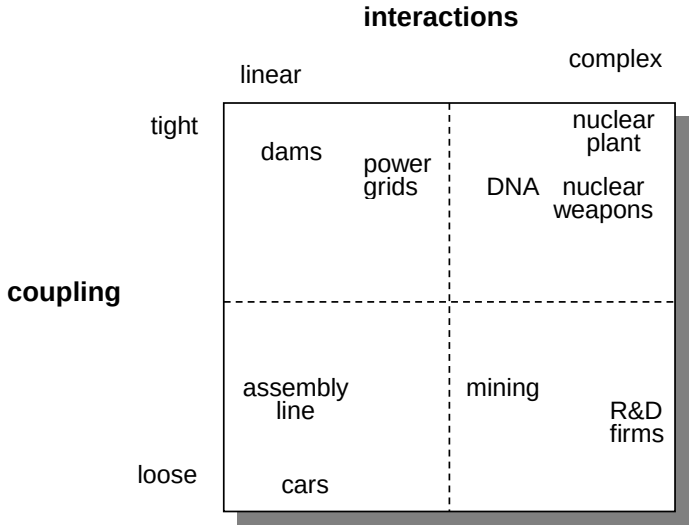

Figure 1. Interaction/Coupling Chart (Perrow, 2011:p97)

NB: Figure 1 is directly copied from Perrow (2011:p97), and the classifications shown are based on Charles Perrow's personal judgement of the state of various systems operating in the USA in 1984 (Normal Accidents was first published in 1984), and are therefore, neither definitive nor directly applicable to UK infrastructure systems in 2017.

The matrix is most effective, if populated collaboratively for the specific system under analysis. The process of populating Figure 1, facilitates discussion, enables interdisciplinary discussion of system characteristics, makes explicit assumptions about system coupling and interactions and identifies areas of uncertainty. It is most useful, therefore, to begin with a blank matrix, and approach population of the matrix as a collaborative learning exercise, to understand how experts from different infrastructure disciplines interpret the current state of infrastructure systems. An exercise to populate Figure 1, beginning with a blank matrix, for UK infrastructure systems in 2017, is recommended as an informative starting point for any subsequent analysis of the impacts of digitally connected infrastructure systems on systemic interactions and system coupling.

Characterising Interactions and Coupling States

Characterising Interactions

Linear interactions *are those in expected and familiar production or maintenance sequences, and those that are quite visible even if unplanned.*

Complex interactions *are those of unfamiliar sequences, or unplanned and unexpected sequences, and either not visible or not immediately comprehensible.*

Table 1. Summary of terms to characterise complex and linear systems (Perrow, 2011:p88)

Complex Systems	Linear Systems
Proximity	Spatial segregation
Common mode connections	Dedicated connections
Interconnected subsystems	Segregated subsystems
Feedback loops	Few feedback loops
Limited substitutions	Easy substitutions
Multiple and interacting controls	Single purpose, segregated controls
Indirect information	Direct information
Limited understanding	Extensive understanding

Characterising Coupling

Table 2. Tight and Loose Coupling Tendencies (Perrow, 2011:p96)

Tight Coupling	Loose Coupling
Not possible to delay processes	Possible to delay processes
Invariant sequences	Order of sequences can be changed
Only one methods to achieve the goal	Alternative methods to achieve goal are available
Little slack as possible in supplies, equipment, personnel	Slack in resources is possible
Buffers and redundancies must be deliberately designed into the system	Buffers and redundancies may fortuitously be available
Substitutions of supplies, equipment, personnel are limited and must be deliberately designed into the system	Substitutions may fortuitously be available

Box 2 Characterising Interaction and Coupling States

2.2 Significant Messages from NAT

The following headings are intended a synopsis of significant messages from NAT significant to the scope of this study on digitally connected infrastructure systems (DCIS).

Not all Accidents are Normal Accidents. NAT makes an important distinction between Normal (System) accidents, an inherent emergent (and often incomprehensible) property of *high-risk* systems (systems where interactive complexity and tight coupling are present) and component failure accidents. Component failure accidents, caused by the failure of a single component, rather than interactions between components need not be inevitable, can be anticipated, learnt from and prevented

'a component failure accident is the simple failure of one or more components, without any significant interaction of failures, it is the most common form of accident. Most of them could be prevented if we tried harder (Perrow, 2011: p355).

Normal Accidents are only inevitable in *high-risk* contexts. NAT defines the meaning of *high-risk* in terms of two system characteristics (interactive complexity and tight coupling). In systems where these characteristics are absent, normal accidents are not inevitable.

Normal Accidents are neither frequent nor expected. Normal Accidents are *normal* in the sense that they an inherent property of interactions in *high-risk* systems. NAT makes no explicit assertions about timescale.

The term normal accident, does not imply catastrophe is inevitable.

'It takes just the right combination of circumstances to produce a catastrophe, just as it takes right combination of inevitable errors to produce an accident.' ……it is hard to have a catastrophe; everything has to come together just right (or wrong). When it does we have negative synergy. Since catastrophes are rare, elites, I conclude, feel free to populate the earth with these kinds of risky [high-risk] systems.' (Perrow, 2011: p356-358)

Perrow observed that there are many more accidents in *high-risk* systems than there are catastrophes. NAT asserts that for a catastrophe to occur, a *high-risk* system must also have an additional system characteristic *'catastrophic potential'*. In such systems, a normal accident can manifest as a catastrophe. However, catastrophe is not the inevitable outcome of a normal accident in a system with *catastrophic potential*, timing and serendipity both have a large role to play. NAT explains this as follows: *Catastrophic potential is a system characteristic; it can be latent (present) in a system without having any impact in the day to day performance of the system.*

Risk cannot be completely eliminated from *High-Risk* Systems.

'Risk will never be eliminated from high-risk systems…. At the very least, however, we might stop blaming the wrong people and the wrong factors and stop trying to fix the system in ways that only make them riskier.' (P5) (Perrow, 2011)

In NAT inevitable is used to mean that the likelihood of a normal accident cannot be reduced to zero. NAT does not imply that the likelihood cannot be reduced, rather it states that under certain circumstances (those that characterise a *high-risk* system) risk cannot be completely eliminated and that efforts to do so will be unsuccessful. NAT does not undermine the case for investment in safety devices, but it does challenge the assumption that accidents can be achieved through technical fixes alone, and makes a case for better understanding of the characteristics of high-risk systems.

The study of system characteristics and interdependence is essential. NAT makes a compelling case for in depth analysis of those system characteristics that make a system *high-risk*

'it is possible to analyse the special [system] characteristics [complexity and coupling] and in doing so gain a much better understanding of why accidents occur in the systems, and why they always will. If we know that, then we are in a better position to argue that certain technology should be abandoned, and others, which we cannot abandon, because we have built so much of society around them, should be modified.' (p4) (Perrow, 2011)

Systems can be tightly coupled with 'exogenous' factors. NAT proposes the term 'Ecosystem accident' to describe *'an interaction of systems that were thought to be independent but are not because of [independence with] the larger ecology'*. The significance of this is that system interactions are much broader than the interaction between technical components, and include interactions with natural and societal process.

A systemic approach is required. Technological fixes, better organisation and improved system design are complimentary approaches to address high -risk systems. A focus solely on technological fixes is often insufficient and can have unforeseen impacts.

'it is particular important to evaluate technological fixes in the systems that we cannot or will not do without. Fixes, including safety devices, sometimes create new accidents, and quite often merely allow those in charge to run the system faster, or in worse weather, or with bigger explosives. Some technological fixes are error reducing – the jet engine is simpler and safer than the piston engine; photometer's are better than lead lines; three engines are better than two on an aeroplane; computers are more reliable than pneumatic controls. But other technological fixes are excuses for poor organisation or an attempt to compensate for poor system design.' (Perrow, 2011) (P 11)

Single Discrete failures cannot typically explain the cause of a normal accident.
'Accidents are not often caused by massive pipe breaks, wings coming off, or motors running amok. Patient accident reconstruction reveals the banality and triviality behind most catastrophes…. Discrete failures are expected and can be guarded against by backup systems. (Perrow, 2011) *(P9)*

Rather it is 'the *interactive nature of the world and it's tight coupling and interaction between multiple small failures* ['*the seemingly trivial mishaps which continuously abound in big systems]* (Perrow, 2011) *p8-9]* that often explain an accident.

During a normal accident events can be incomprehensible. The interactions **(**Interdependencies) that unfold during a normal accident are often comprehensible only in retrospect, and can be *incomprehensible for some critical period of time during a normal accident.* Consequently, action to address an accident during the event is difficult. Furthermore, *often although witnessed the significance of interdependencies is not believed prior to an event,* making pre-emptive action difficult.

Organisational Contradictions (*'organisational pushmepullyous')* abounds.
NAT identifies a tendency for organisations to try to go in opposite directions simultaneously (*'organisational pushmepullyous').* This characteristic makes the prioritisation of action to reduce normal accidents more than purely a technical problem.

2.3 Key concepts proposed by or used in NAT

Based on the above review, Table 3 provides a list of key terminology from the book Normal Accidents: Living with High Risk Technology(Perrow, 2011). Since initial publication in 1984, this has been cited by over 1000 academic publications, and a significant body of literature on NAT has emerged. This body of literature expands on, critiques, refines, challenges, extends and applies the concept of NAT and the terminology used in NAT.

The concepts in Table 3 have been used to inform this literature review and identify relevant papers from two groups of literature relevant to this project: (i) literature that directly builds on NAT, i.e. makes direct reference to NAT and (ii) complementary literature from independent disciplines that uses these or similar terms.

Table 3. Terminology or Concepts from NAT

Key Term/Concept from NAT
Normal and System Accidents
Component failure Accident
Accident typology
High-Risk Technologies, organisation, systems
High-Risk Organisations
High-Risk Systems
System characteristics
System properties
System coupling
Complex interactivity and complexity
Catastrophic potential
Negative synergy
Interdependence and incomprehensible and comprehensible
System and Complex and Linear and Esoteric and transformation (P14)
Interacting and small and multiple failures
Failure and Cascade and propagating and interactive and discrete
Human Factors (the cunning of designers, and the wit and experience the operating personnel to cope with the unexpected)
Organisational contradictions and organisational Pushmepullyous
Organisation of organisations
Risk assessment (p12) Risk perceptions (P9) erroneous worlds in their minds. Risk and shaman.
Safety culture and Near misses
Technological Fix
Safety Devices buffers, slack, redundancies, redundant paths, circuit breakers, alarms, bells, and whistles
System components
System design
Ecosystem accident
Reliability
Resilience

2.4 Application of NAT to Infrastructure Systems

What lessons can we learn from Normal Accident Theory (NAT) in order to exploit the benefits of digitally connected infrastructure systems, whilst minimising the creation, and maximising awareness, of the potential for digitally enabled vulnerabilities?

The initial of focus of the review of NAT literature was to examine the question *Are digitally connected infrastructure systems (DCIS), as they develop, likely to make normal accidents inevitable?* However, following initial scoping, the question was re-framed to the above to broaden the scope of the study and identify transferable lessons for digitally connected infrastructure systems (DCIS) from NAT.

Application of NAT to infrastructure systems gives rise to the following conclusions:

- Infrastructure systems, particularly digitally connected infrastructure systems, have the properties of *high risk* systems (complex interactivity and tight coupling);
- Therefore, any intervention in an infrastructure system that, intentionally or otherwise, increases the *complex interactivity* of, or *tightens coupling* between infrastructure system components and the broader socio-technical system (STS) within which infrastructure systems are embedded will increase the likelihood of a normal accident.
- Furthermore, any intervention that increases human reliance on a specific infrastructure system to enable the outcomes on which individuals, communities, organisations, societies, nations, international bodies, global humanity depend, then that intervention will also increase the likelihood of a normal accident.

Application of NAT specifically to digitally connected infrastructure systems (DCIS), gives rise to similar conclusions:

- Infrastructure systems, particularly digitally connected infrastructure systems, have the properties of *high risk* systems (complex interactivity and tight coupling);
- Unless the implementation of digitally connected infrastructure systems (DCIS) reduces complex interactivity and/or loosens system coupling, normal accidents will remain inevitable.
- Unless digitally connected infrastructure systems (DCIS) can be implemented in such a way as to reduce reliance on established infrastructure system, normal accidents will remain inevitable.
- As we become increasingly dependent on digitally connected infrastructure systems (DCIS) to enable the outcomes we expect infrastructure systems to deliver, or if use of digital connectivity tightens coupling or increase complex interactivity, the likelihood of normal accident occurring will increase.

In light of the literature review we concluded in response to the original question *Are digitally connected infrastructure systems, as they develop, likely to make normal accidents inevitable?* i) by definition normal accidents are inevitable in high-risk technologies, organisations and systems; and ii) infrastructure systems, particularly digitally connected infrastructure systems, have the properties of *high risk* systems (complex interactivity and tight coupling); then iii) an increase in the likelihood of normal accidents will logically follow.

However, broadening the question to examine what lessons can be learnt gives a different perspective, the key messages in section 2.1.2 become lessons for the way in which we consider digitally connected infrastructure systems, and i), ii) and iii) above become lessons about the state of current infrastructure systems and provide a compelling case for developing:

a) Greater understanding of the extent and characteristics of interdependencies within infrastructure systems and the broader Socio-technical system (STS);
b) Analysis of how a transition towards digitally connected infrastructure systems (DCIS) will create new interdependencies and impact on current interdependencies;
c) Analysis of the resilience of infrastructure systems to the emergent properties that occur as a result of any change in systemic interdependencies that might occur as established infrastructure systems are transformed into digitally connected infrastructure systems (DCIS)
d) Analysis of what impact HRO principles can have on reducing the likelihood of normal accidents in digitally connected infrastructure systems.

The literature review in section 3 has been developed with the above considerations in mind.

3 Learning from High Reliability Organisation (HRO), Systemic Resilience Studies, Infrastructure Interdependence and Systems Thinking

How do we make digitally connected infrastructure systems more resilient and what current practices are used, for example in high reliability organisations?

This section builds on findings from the review of NAT to address the above question. In particular, this section provides review and analysis of HRO, infrastructure interdependence, systemic resilience and systems thinking literature with a view to identifying best practise lessons related to the following:

- Whether best practise from HRO can be implemented in digitally connected infrastructure systems to either reduce (or prevent an increase in) complex interactivity, loosen system coupling, or reduce dependence on specific components of infrastructure systems and therefore reduce either the likelihood or impact of normal accidents. Particular emphasis will be given to understanding an ongoing tension between HRO theory and NAT, to interpret for infrastructure systems and DCIS whether the likelihood of normal accidents can be reliably reduced to zero.
- Potential methods, insights, tools and processes from the study of interdependence in infrastructure systems that can be applied to improve analysis and understanding of the NAT *high-risk* characteristics of complex interactivity and tight coupling in infrastructure systems and DCIS.
- Lessons from the interdisciplinary study and application of resilience in other contexts. In particular, which if any resilience models represent best practise transferable to understanding and improving resilience in the context of digitally connected infrastructure systems.
- Other transferable lessons from the field of systems thinking and systems engineering

3.1 Overview of High Reliability Organising (HRO)

"The hallmark of an HRO is not that it is error free, rather that an error does not disable it." (Weick and Sutcliffe, 2007)

"a High Reliability Organisation (HRO) is one capable of discovering and managing unexpected events, and sustaining reliable performance in the face of unexpected events" (Weick and Sutcliffe, 2007)

3.1.1 Introduction

High-Reliability.org (van Stralen, 2017) on the origin of High Reliability theory:

"High Reliability developed to make an organization stronger (Mercer) and for an individual to operate in uncertainty or under threat (van Stralen). People come together to create High Reliability (Weick, 1987) *in an organization designed for this (Roberts). It is the individual who acts but the organization must allow that action."* (van Stralen, 2017)

Additionally, van Stralen, (2017) outlines four organizational characteristics of the HRO that limit accidents or failures:

> *1. Prioritization of both safety and performance are shared goals across the organization;*
>
> *2. A "culture" of reliability (or, better, attitude toward reliability) that simultaneously decentralizes and centralizes operations allowing authority decisions to migrate toward lower ranking members;*
>
> *3. A learning organization that uses "trail-and-error" learning to change to the better following accidents, incidents, and, most important, near misses;*
>
> *4. A strategy of redundancy beyond technology but in behaviours such as one person stepping in when a task needs completion.*

When discussing the mix of strategies needed to achieve High Reliability in any given context, Malone and Woodhouse (quoted in Sagan, (1995: p27) state

"while the exact mix of strategies appropriate in a given case obviously depends on the nature the particular problem, the catastrophe aversion strategy outlined [in the above steps] should be applicable to virtually any risky technology."

(Malone and Woodhouse quoted in Sagan, (1995: p27)

Roberts (quoted in *Sagan, 1995: P27)* further emphasises HRO is a transferable approach applicable in all organisational contexts, and is most needed in any context where failure must be completely avoided.

"most of the characteristics identified [in high reliability organisations] should operate in most organisations that require advanced technologies and in which the cost of error is so great that it needs to be avoided altogether."

(Roberts quoted in Sagan, (1995: p27)

An additional key insight from HRO is the important distinction between the organisational structures needed for an efficient organisation – one capable of delivering reliable performance in a stable context, and those required for a High Reliability Organisation (HRO) – one capable of reliable performance in the face of unexpected events (unstable external context). This insight is consistent with Hollings (1996) differentiation between Ecological and Engineering Resilience and the *'tension between managing for efficiency and managing for resilience*' reported by participants in a resilience engineering study undertaken by Lloyds Register Foundation (2015).

Efficient organizations are vulnerable to disruptive external events because their success is rooted in the unvarying repetition and/or reproduction of actions or patterns of activity, and the assumption that operating conditions will remain within a stable range. An HRO, by contrast, recognises that because unexpected events will happen, and that *"for a system to remain reliable, it must somehow handle unforeseen situations in ways that forestall unintended consequences…."* ...therefore system reliability i.e. *'whether the system, in the global sense, works appropriately; not only individual components or sub systems'* not efficiency should be the primary goal of the organisation.

3.1.2 HRO Principles

Managing the Unexpected: Resilient Performance in an Age of Uncertainty, (Weick and Sutcliffe, 2007) provides a review of scholarship on high reliability organisation (HRO), and synthesises earlier HRO literature (Weick and Sutcliffe, 2006; Laporte and Consolini, 1991; La Porte, 1996; Weick, 1987; Weick, 2004) to argue that a High Reliability Organisation (HRO) - *one capable of discovering and managing unexpected events, and sustaining reliable performance in the face of unexpected events* – must create a '*mindful infrastructure'* [organisational structure], that embodies the following five principles:

(i) Preoccupation with failure [of all sizes]
(ii) Reluctance to simplify operations
(iii) Sensitivity to operations,
(iv) Commitment to resilience
(v) Underspecification of structures/ deference to expertise

The outcome of adherence to these principles is an HRO, and a significant reduction to the risk of serious accidents and catastrophes. Whether HRO can eliminate risk completely is a source of tension between NAT and HRO proponents (section 3.2 provides further details). Table 4 and Table 5 summarise key HRO concepts:

Table 4. High Reliability and Mindfulness and HRO Principles (adapted from Weick and Sutcliffe, 2007)

Idea	Overview
High Reliability	Reliability is a result of interactions within the system and interdependencies between the system and external environment. It is therefore a system characteristic or emergent property of how the system operates. High reliability should therefore be seen as *an overall goal of the system and whether the system, in the global sense, works appropriately; not only individual components or sub systems.*
Mindfulness	Mindfulness is less about decision making (a traditional focus of organizational theory and accident prevention), and more about inquiry and interpretation grounded in capabilities for action. Furthermore, mindfulness in HROs is not activated solely by novelty [the unexpected], but rather is a persistent mindset that admits the possibility that any "familiar" event is known imperfectly and is capable of novelty [the unexpected]. This ongoing wariness is expressed in active, continuous revisiting and revision of assumptions, rather than in hesitant action.

Table 5. HRO Principles (adapted from Weick and Sutcliffe, 2007)

HRO Principles of/Processes for Mindfulness	
Principle	**Brief Overview**
Preoccupation with failure [of all sizes]	A fundamental reluctance among higher management to put decision or action frameworks in place that are not sensitive to the possibilities of analytic error. Effective HROs observe a preoccupation with failure in at least three ways: by treating any and all failures as windows on the health of the system, by a thorough analysis of near failures (near misses), and by focusing on the liabilities of success (what vulnerabilities do successfully processes create) HROs act as if there is no such thing as a localized failure and suspect, instead, that causal chains that produced the failure are long and wind deep inside the system.
Reluctance to simplify operations	HROs recognise the instinctive tendency to simplify and the potential danger of this. Simplifications, (variously referred to as worldviews, frameworks, or mindsets) used to handle complex tasks by simplifying the manner in which the current situation is interpreted, allow members to ignore data and keep going (normalise unexpected data/events) (Turner, 1978). Simplifications are potentially dangerous for HROs because they limit both the precautions people take and the number of undesired consequences they envision; increase the likelihood of eventual surprise; allow anomalies to accumulate; intuitions to be disregarded, and undesired consequences to grow more serious.
Sensititivity to operations,	HROs pay serious attention to ongoing operations and are aware of the imperfections in these activities. HROs strive to make ongoing assessments and continual updates of the actual state of operations rather than assuming all is as it is expected to be.
Commitment to resilience	Effective HROs tend to develop both anticipation and resilience in the sense defined by Wildavsky (1991, p. 77). **Anticipation** refers to the "prediction and prevention of potential dangers before damage is done," whereas **Resilience** refers to the "capacity to cope with unanticipated dangers after they have become manifest, learning to bounce back [furthermore] Resilience is not only about bouncing back from errors, it is also about coping with surprises in the moment. Resilience is NOT simply the capability to absorb change and still persist. [it is more dynamic] … The best HROs don't wait for an error to strike before responding to it. Rather, they prepare for inevitable surprises "by expanding general knowledge and technical facility, and generalized command over resources" (Wildavsky, 1991, p. 221)
Underspecification of structures / deference to expertise	Do not assume that the highest-ranking individual possesses the greatest expertise or experience situation at hand. During troubled times, shift leadership role to the person or team system the greatest expertise and experience to deal with the problem at hand. Provide them with the empowerment they need to take time effective action.

Importantly, the five HRO principles (Table 5) are not a menu of options. An HRO must implement them all. A failure in implementing any one of these principles, undermines the capability of an organisation to achieve high reliability, and therefore '*the capability of an organisation to discover, manage and sustain resilient performance in the face unexpected events.'* (Weick and Sutcliffe, 2007)

To further emphasise the significance of this point, Weick and Sutcliffe (2007), emphasise the importance of implementing all HRO principles, by stating observable characteristics of an organisation in violation of HRO principles. These characteristics provide a rapid diagnosis tool to assess whether an organisation is truly an HRO.

"When these 5 Principles [Table 5] *are violated, people fall back on practises that: (i) deny small failures, (ii) accept simple diagnoses, (iii) take frontline operations for granted, (iv) overlook capabilities for resilience, and (v) defer to authorities rather than experts."* (Weick and Sutcliffe, 2007)

Therefore, if any of these characteristics are observed in an organisation (or system), it is a symptom that the organisation (or system) is not achieving high reliability. Furthermore, if an HRO observes even a single symptom a complete review of all organisational practice is needed, not just the specific HRO principle to which it relates, before the organisation can be regarded as an HRO. A symptom allowed to remain unchallenged typically becomes accepted and normalised. In such situations, normal accidents will remain inevitable.

Weick and Sutcliffe (2007), provide a series of detailed case studies of how catastrophes could have been prevented by adherence to HRO principles, and which of the HRO principles could have prevented the failure. Depending on the perspective of the analyst, these case studies can either be interpreted as: a) demonstrable evidence that HRO principles if perfectly implemented can prevent all accidents; or b) it is not possible to implement HRO principles with 100% certainty 100% of the time, therefore although HRO principles can decrease the likelihood of normal accidents, normal accidents remain inevitable in certain *high-risk* contexts. The relationship between HRO and NAT is explored in more detail in Table 6.

3.2 The Relationship between HRO and NAT

As illustrated in the above quote by Roberts (quoted in *Sagan, 1995: p27)*, high reliability organisation (HRO) is most needed when the high-risk system conditions identified by NAT ('*interactive complexity'* and '*tight coupling')* are present. However, whether implementation of HRO principles, can eliminate normal accidents remains an unresolved issue. A proponent of HRO would answer yes, whereas a proponent of an NAT would counter that a certain type of accident (normal accidents) will always remain inevitable in *high-risk* systems. Table 6 reproduced from analysis by Sagan (1995) analyses tension between the two schools of thought.

Table 6. Competing Perspectives on Safety with Hazardous Technologies (reproduced from Sagan, 1995: P46)

High Reliability Organisation Theory	Normal Accident Theory
Accidents can be prevented through good organisational design and management.	Accidents are inevitable in complex and tightly coupled systems
Safety is the priority organisational objective.	Safety is one of a number of competing objectives
Redundancy enhances safety: duplication and overlap can make a "reliable system out of unreliable parts."	Redundancy often causes accidents: it increases interactive complexity and opaqueness and encourages risk-taking.
Decentralised decision-making is needed to permit prompt and flexible field-level responses to surprises.	Organisational contradictions: decentralisation is needed for complexity, but centralisation is needed but tightly coupled systems.
A "culture of reliability" will enhance safety by encouraging uniform and appropriate responses by field level operators."	The military model of intense discipline, socialisation, and isolation is incompatible democratic values.
Continuous operations, training, and simulations can create and maintain high reliability operations.	Organisations cannot train to unimagined, highly dangerous, politically unpalatable operations.
Trial and error learning from accidents can be effective, and can be supplemented by anticipation and simulations.	Denial of responsibility, faulty reporting, and reconstruction of history cripples learning efforts.

On a practical level for this study, we recommend that HRO be interpreted as a form of good practice capable of increasing the reliability of a high-risk systems, rather than a panacea to eliminate normal accidents. By definition, normal accidents are inevitable in certain *high-risk* systems. Therefore, the aspiration of HRO must be to reduce normal accident risk to near zero, and reduce the scale of impact when such accidents occur. HRO, therefore, provides a useful starting point for planning how to increase the reliability of any digitally connected infrastructure systems.

Shrivastava et al. (2009) and (Leveson, 2011) are amongst those critics who suggest the tension between NAT and HRO perspectives is over-stated because the principles of HRO (Table 5) can all be characterised as actions to address one or both of the high-risk characteristics dimensions (coupling and interactions) identified by NAT.

"Despite differing motivations – HRT [HRO] *looks for organizational factors and processes that contribute to reliability, and NAT focuses on organizational properties that lead to accidents – we believe that both theories have similar*

implications for practice. NAT implies that organizations can lower the statistical probability of systems accidents (but never lower it to zero) by reducing their complexity and loosening the coupling amongst their subsystems. We argue that the initiatives identified by HRT [HRO] *– strategic concern for safety and safe design, redundancy, simultaneous centralization and decentralization, training, organizational learning, and mindfulness* [see Table 5] *– can all be construed as attempts to either directly or indirectly address the challenges posed by complex interactions and tight coupling, the very dimensions central to NAT."* (Shrivastava et al., 2009: p1365)

3.3 Resilience as a System Property

The need for infrastructure practitioners and policymakers to develop a deeper understanding of systemic resilience and the potential value of targeted investment in infrastructure system resilience, rather than solely retaining a narrow focus on cost and efficiency is widely acknowledged.

Dolan *et al* (2016) undertook analysis of how the term Resilience has been applied by a range of disciplines to describe an emergent property of different systems[1] and identified the following key messages:

- Resilience is a multi-dimensional concept and as such is difficult to define. Common across disciplinary perspectives are the concepts that: (i) resilience is a property of a system that emerges from the interaction between (interdependence of) system components; (ii) a resilient system has certain abilities or characteristics.
- All human activity (including construction and operation of infrastructure) takes place in the context of the broader system of which it is a part. It follows any infrastructure asset, sub-sector or sector is only as resilient as the least resilient component of the supply chains or other infrastructure on which it depends. Therefore, it is not possible (or at least very difficult) to be resilient without being systemic.
- In order to be resilient, any action(s) to increase efficiency or optimise a system must be evaluated in the context of potential changes to the system (sudden and gradual) that might affect the ability to preserve existence of function. Explicitly acknowledging and maintaining awareness of broader external factors during problem framing and solution selection, is therefore, an essential element of the resilience approach.
- 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

[1] Perspectives considered include: ecological systems (Holling, 1973), social systems (Adger, 2000), socio-ecological systems (Folke, 2006; Walker et al., 2004), psychological systems (Ong et al, 2006), communities (McAslan, 2010) dynamic and intentional systems (a category that includes built systems such as infrastructure (Hollnagel, 2014, 2011), and business systems (Hamel and Valikangas, 2003)

performance after a failure event, impedes an organisation's ability to be resilient.

Key ideas and frameworks from ecological, socio-ecological system (SES), Resilience Engineering and strategic engineering perspectives are outlined in sections 3.3.1 – 3.3.4.

3.3.1 Frameworks for Systemic Resilience

Two conceptual frameworks, from the systemic resilience literature, are included here (Figure 2 and Figure 3) to provide a visual illustration of important aspects of systemic resilience. These models have been chosen as relevant to this study because they emphasise that resilience is a dynamic and emergent property of systems and requires continuous dynamic action, rather than a one-off response.

The model of resilience favoured by the UK Cabinet Office in Keeping the Country Running: Natural Hazards and Infrastructure (Cabinet Office, 2011) and used to communicate resilience for the purposes of producing sector resilience plans (Cabinet Office, 2016) is not included here, because it fails to emphasis the dynamic and emergent nature of resilience, or communicate the need for coherent dynamic system-wide action rather than sectoral planning.

Figure 2 produced by The National Infrastructure Advisory Council[2] (NIAC, 2010) illustrates the need for a dynamic approach and continuous action for systemic resilience. It emphasises two components as central to the development of systemic resilience for built systems (i) '*people, plans, processes and procedure'* and to (ii) '*Infrastructure and assets'*, and outlines 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), as well as providing succinct explanations of each ability.

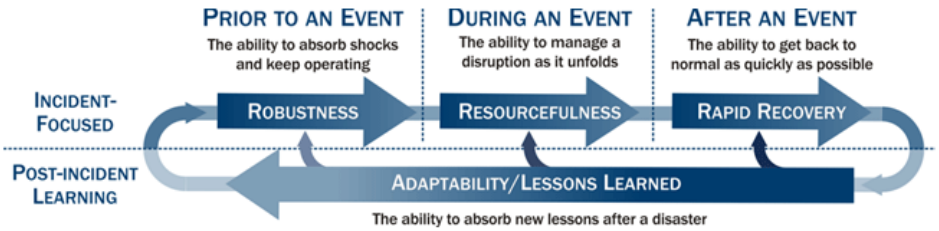

Figure 2. The NIAC Resilience Construct (Source: NIAC, 2010)

Figure 3 is The ENCORE Network Framework for Resilience, and is part of ongoing research into systemic risk and resilience in complex engineered system (CES). Figure 3 captures the dynamic characteristic of systemic resilience, and the

[2] NB: The National Infrastructure Advisory Council (NIAC) is a body created by the American President and Secretary of Homeland Security to provide advice on the security of the critical infrastructure sectors and their information systems. The NIAC is composed of members from across private industry, academia, and state and local government and is appointed by the President. See https://www.dhs.gov/national-infrastructure-advisory-council for more details.

need for continuous action to manage emergent system properties. Figure 3 remains a work in progress, the ENCORE team aim to refine the model to illustrate the significant role complexity science has to play in achieving systemic resilience.

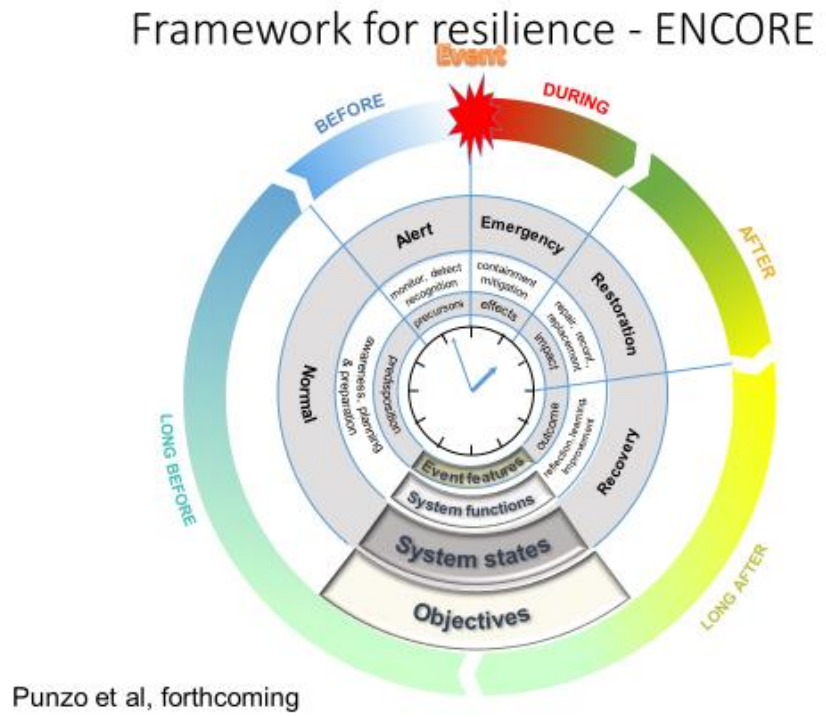

Figure 3. ENCORE Plus Resilience Framework (Source: Punzo et al., 2017)

However, despite the strengths of Figure 2 and Figure 3, a need remains for a conceptual model that makes explicit that the recovery phase can under some circumstance be an opportunity to restore not just to a prior state, but to restore in a way that addresses all vulnerabilities observed in the system prior to the failure, rather than solely the vulnerabilities believed to have caused the failure. The adaptation cycle in Ecology (Walker *et al.*, 2004), illustrates the restoration opportunity, but requires adaptation for use in this context.

3.3.2 Ecological and Socio-Ecological System Resilience

In Ecology, Holling (1973) pioneered the use of the term resilience to describe a system property, and Walker *et al.* (2004) defined 4 resilience components for ecological systems. Table 7 (reproduced from Dolan *et al.*, 2016) gives these definitions and offers interpretation of the significance of these to infrastructure systems including digitally connected infrastructure systems.

Table 7. Components of Ecological Resilience and Significance for Infrastructure

Resilience Component + Definition[i]	Significance to Infrastructure System
Latitude: the maximum amount a system can be changed before losing its ability to recover (before crossing a threshold which, if breached, makes recovery difficult or impossible).	Knowledge of the operating conditions for which the infrastructure was designed is important, as is analysis of consequences of operation outside of that range.
Resistance: the ease or difficulty of changing the system; how "resistant" it is to being changed.	Knowledge of the factors that make an infrastructure either resistant or vulnerable to change creates an opportunity for pro-active management prior to an infrastructure failure event.
Precariousness: how close the current state of the system is to a limit or "threshold."	Continuous information on how close current operating conditions are to the upper or lower bound of specified operating conditions provides an actionable resistance diagnostic.
Panarchy: because of cross-scale interactions, the resilience of a system at a particular focal scale will depend on the influences from states and dynamics at scales above and below. For example, external oppressive politics, invasions, market shifts, or global climate change can trigger local surprises and regime shifts.	An infrastructure asset is only as resilient as the least reliable component of the supply chains on which it depends. Therefore, it is not possible (or at least very difficult) to be resilient without being systemic. More broadly, knowledge of the extent to which infrastructure is dependent on a stable external context is needed to create strategies which reduce vulnerability to contextual change.
	Left column from (Walker et al., 2004)

In the study of Socio-ecological systems (SES), systems which Folke (2006) describes as "*characterised by non-linear dynamics, thresholds, uncertainty, surprise, gradual change, rapid change, and a range of spatial and temporal scales"*

Resilience is best understood as, one of three tightly coupled and complementary attributes of a dynamic system the other two being adaptability and transformability (Walker *et al.*, 2004). The significance of each is outlined in Table 8.

Table 8 SES Attributes of a Dynamic System (Source: Walker et al. 2004)

Attribute	Significance
Resilience	the capacity of a system to absorb disturbance and reorganize while undergoing change so as to still retain essentially the same function, structure, identity, and feedbacks
Adaptability	the collective capacity of the human actors in the system to manage resilience and is strongly linked to the ability to intentionally manipulate the four components of Resilience
Transformability	the capacity to create a fundamentally new system when the old is untenable

This emphasis on the attributes of system dynamics, illustrates that from an SES perspective understanding (i) the current state of these attributes (ii) the potential impacts on infrastructure performance if these attributes were to change, (iii) the underlying causes of change to these attributes, (iv) the factors that inhibit the ability of a system to reorganise (v) how these attributes can be managed to mitigate risk and create opportunities to increase resilience, are all important parts of developing systemic resilience.

Many of these principles are applicable to understanding the resilience of infrastructure systems and DCIS. Furthermore, there are close parallels between these and the principles of HRO. However, the potential for lessons from ecology and SES to be applied to adapt HRO for application in systems rather than organisations needs further research, as does the application of these lessons to improve NAT analysis of system coupling and interaction.

3.3.2.1 Conflict between Efficiency and Resilience – Insight from Ecological Resilience

In later work, Holling (1996) made a distinction between Ecological resilience as concerned with enabling *'existence'* of function in a changing context, whereas engineering resilience focuses on the *'efficiency'* of function in a stable context. It follows from Holling (1996):

- Engineering resilience assumes stable external conditions. Under such conditions it is intuitive to optimise for efficient performance within the stable range.

- Ecological Resilience assumes external conditions are subject to gradual change and occasional shocks. Under such conditions maintaining delivery of desired outcomes in the presence of external disruption (often beyond direct control of those affected) becomes of greater significance than achieving efficient delivery.

The two concepts are nested and mutually complementary, and serve to illustrate that decisions justified on the grounds of efficiency (or any narrow decision criterion) are likely to proceed, whilst tacitly assuming the stability of the external

environment. Therefore, efficiency driven decisions, if not to undermine systemic resilience must be grounded in deep understanding of the systemic context in which they are implemented. This distinction between ecological and engineering resilience has the power to explain the observed tension between managing infrastructure systems for efficiency and managing infrastructure systems for resilience reported by both HRO theorists and by infrastructure practitioners involved with resilience work led by the Lloyds Register Foundation (2015).

3.3.3 Resilience Engineering and Dynamic and Intentional Systems

Resilience Engineering is a field of study concerned with the resilience of built systems (including interdependent infrastructure systems). Hollnagel (2014) 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. These abilities to address the actual, the critical, the factual and the potential, are also described by Hollnagel as the abilities to respond, monitor, learn and anticipate (brackets in Table 9).

Table 9. Four Abilities of a Resilient Built System (Source: Hollnagel, 2014)

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.

Lay et al. (2015) provides a case study of these abilities in action. Furthermore, these abilities are closely linked with the frameworks shown in Figure 2 and Figure 3 of this review.

A Foresight review of Resilience Engineering: Designing for the expected and unexpected (Lloyds Register Foundation, 2015), provides further insight from Resilience Engineering. One finding of particular relevance to this study is that all infrastructure sectors independently identified *'tension between management for resilience and management for efficiency'* (P20-27) when asked to identify governance, organisational and system drivers which provide systemic resilience

challenges. This finding reinforces the idea that systemic resilience is an emergent system property, that cannot be managed solely at sector level, or by engineering interventions.

3.3.4 Strategic Resilience

Hamel and Valikangas (2003) propose that to be strategically resilient, an organisation needs to address four challenges. Table 10 interprets these challenges.

Table 10. Strategic Resilience Challenges (adapted from Hamel and Valikanagas, 2003)

Challenge	Explanation
Conquer Denial	Be deeply conscious of external change. Recognise that in a dynamic environment change is more likely than stability. Look to the future and continuously consider how change will affect the organisation. Operate in the world 'as-is', not the world as you would like it to be.
Value Variety	Embrace ideas from all levels of the organisation (not just those in positions of influence). Measure success on a portfolio basis. Encourage small scale experiments and do not punish those behind failed experiments. Recognise that variety is insurance against vulnerability and can support continual adaptation of your organisational strategy.
Liberate Resources	Do not overcommit resources to just one strategy. If an existing strategy appears not to be working, recognise that costs already sunk on that strategy are lost. Make resources available to a portfolio of strategies to increase organisational adaptability.
Embrace Paradox	Recognise that the long term value of a systemic exploration of strategic options is as valuable or more valuable than maximising short term efficiency. Recognise that you will get the behaviour you reward, therefore structure your organisational values and remuneration strategy with resilience objectives in mind.

3.4 Infrastructure Interdependence

3.4.1 Section Overview: The significance of 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) referred to by NAT (Box 2). Improved understanding of system characteristics, can in turn contribute to improved understanding of what the impact of digitally connected infrastructure systems (DCIS) might be on the likelihood or expected scale of a normal accident.

Digitally connected infrastructure systems (DCIS) will on the one hand increase complex interactivity and tighten coupling, whilst simultaneously enabling an infrastructure system to perform in ways more closely aligned to the outcomes we now expect. Therefore, trade-offs between system performance and risk will need to be made when managing infrastructure systems.

Systemic interdependency analysis can support decisions related to such trade-offs. The work by Rinaldi et al. (2001), presented below provides an invaluable starting point for this, and the extension in Table 12 (Carhart and Rosenberg, 2016: 50) a framework for more in-depth analysis. However, further work is needed to make these concepts more widely known and to develop a set of practical examples framed in terms of Figure 4 and Table 12 that practitioners and policy makers involved with infrastructure systems can readily understand and draw learning from.

The IP&MF (Rosenberg et al., 2014) 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. This could be used to provide a more systemic perspective on infrastructure system interdependence, and the degree to which Normal accidents are already inevitable in any system and the impact of any project (or targeted change to the system). Such projects will increasingly be linked to digitally connected infrastructure systems (DCIS), therefore work to tailor the IP&MF specifically to digitally connected infrastructure system (DCIS) is needed.

Additionally, exercises, such as those used by Engineering the Future (Figure 7) and Anytown (Figure 10) 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 (DCIS) is needed to analyse the impacts of digitally connected infrastructure systems on NAT risk and systemic resilience.

3.4.2 Literature on The Study of Interdependency

3.4.2.1 Rinaldi (Rinaldi et al., 2001)

The notion that our nation's critical infrastructures are highly interconnected and mutually dependent in complex ways, both physically and through a host of information and communications technologies (so-called "cyber based systems"), is more than an abstract, theoretical concept. As shown by the 1998 failure of the Galaxy 4 telecommunications satellite, the prolonged power crisis in California, and many other recent infrastructure disruptions, what happens to one infrastructure can directly and indirectly affect other infrastructures, impact large geographic regions, and send ripples throughout the national and global economy.(Rinaldi et al., 2001)

In a highly cited paper Rinaldi et al. (2001), introduced a conceptual framework (Figure 4) to improve analysis and increase understanding of interdependencies (*the interconnections and mutual dependencies* referred to in the above quote). This conceptual framework (Figure 4), and evidence that infrastructure is in practise an interdependent system-of-systems, best analysed as a complex adaptive system (CAS), have inspired much subsequent research into understanding, identifying, communicating, modelling, raising the profile of, and planning for infrastructure interdependencies.

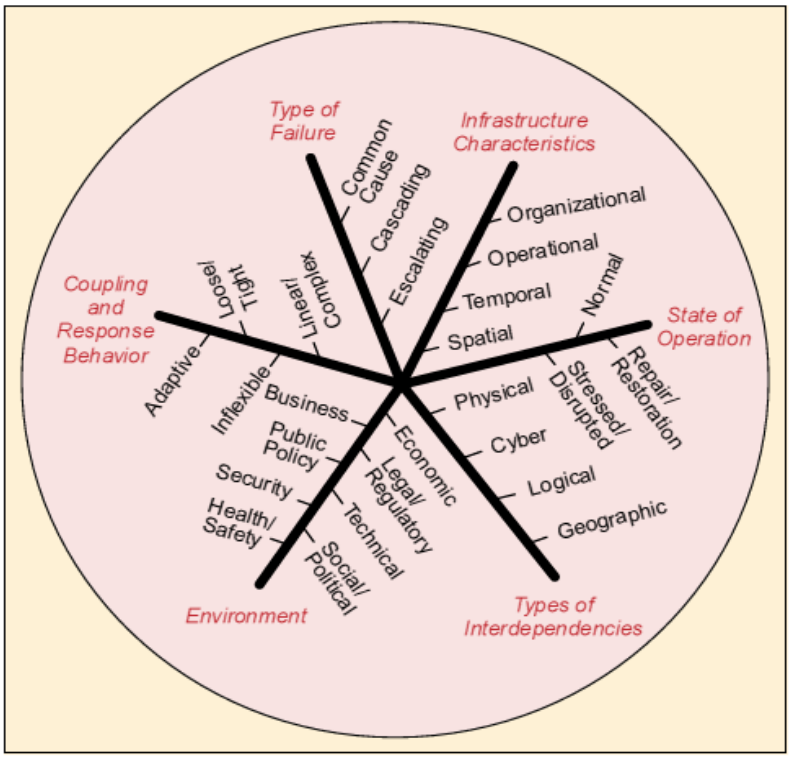

Figure 4. Dimensions for Describing Infrastructure Interdependencies (Source: Rinaldi et al., 2001)

Further explanation of the six interdependence dimensions, and interpretation of their significance to NAT is provided in Table 11 and details of notable work that has refined these in section 3.4.2.

Dependency or interdependency – a simple but important distinction

Although not explicit in the dimensions of Figure 4, it is important to elaborate on, and illustrate, the distinction made by Rinaldi et al. (2001) between the linear concept of dependency (Figure 5) and the more complex concept of interdependency (Figure 6). This distinction is significant to NAT because it mirrors the interaction spectrum (linear- complex) used by NAT in Figure 1.

Figure 5 illustrates dependency, defined by Rinaldi *et al.* (2001) as '*a linkage or connection between two infrastructures, through which the state of one infrastructure influences or is correlated to the state of the other'* by mapping the inputs, supplied by (or via) other infrastructures, on which electric power depends. Dependency relationships have a clear directionality [much like a supply chain] between a *supported* infrastructure, and the other systems or *supporting* infrastructures, without which the *supported* infrastructure cannot function.

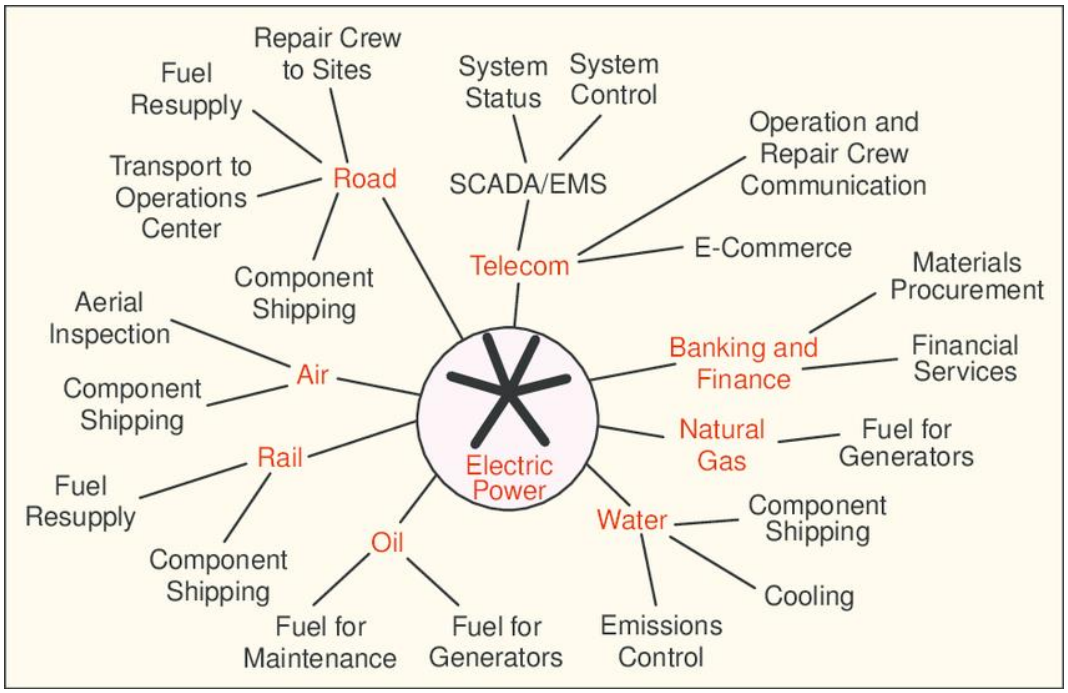

Figure 5. Examples of electric power infrastructure dependencies (Source: Rinaldi et al. 2001).

By contrast Figure 6 maps both the inputs electric power receives from, and the outputs electric power supplies to other infrastructure systems in order to illustrate **interdependency**.

Rinaldi *et al.* (2001), define interdependence as *the bidirectional [mutual dependence] relationship between two infrastructures through which the state of each infrastructure influences or is correlated to the state of the other. More generally, infrastructures are interdependent when each is dependent on the other*.'

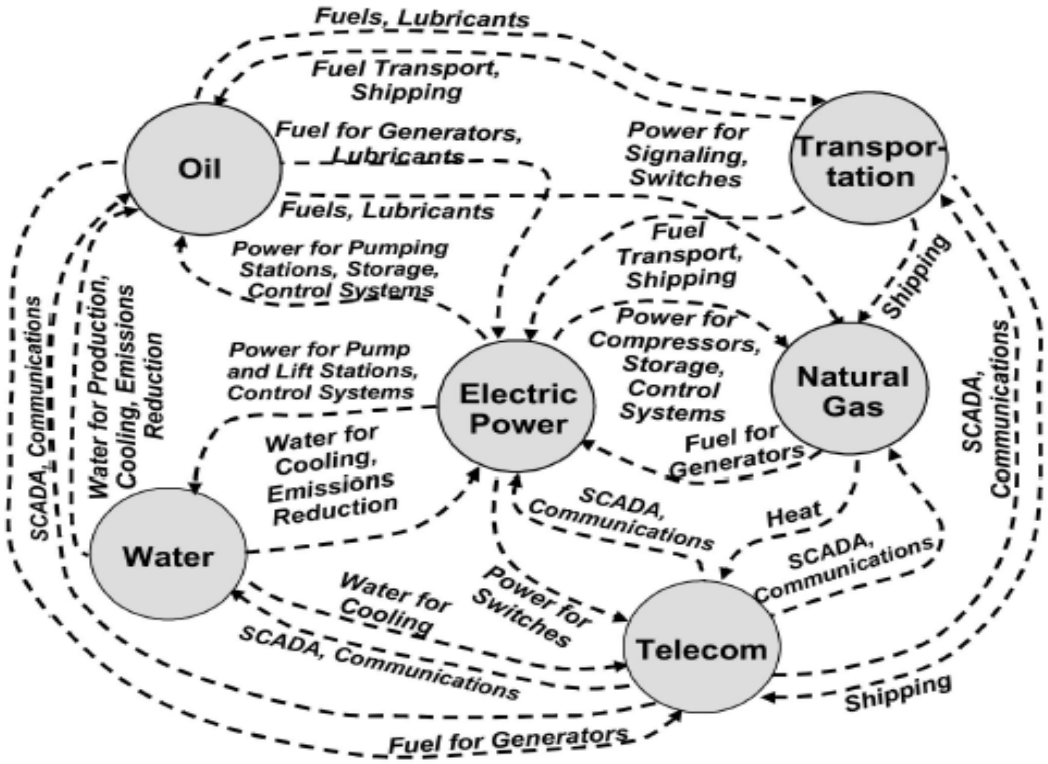

Figure 6. Examples of infrastructure interdependencies (Source: Rinaldi et al. 2001).

Figure 6, through the relatively simple example of electric power demonstrates that in practise infrastructure systems are interdependent and connected at many points and through many mechanisms. Because these interdependencies among infrastructures dramatically increase the overall complexity of the system of systems, a compelling argument can be made that interdependencies give rise to interactive complexity. Therefore, a framework to understand interdependence characteristics, their causes and characteristics, is a framework capable of offering insight into both the root causes of interactive complexity and how tightly coupled interdependent systems are likely to be. Therefore, interdependence is a vital lens to analyse NAT and the principles of HRO in Infrastructure systems and DCIS.

Rinaldi *et al.* (2001) elaborate further on the interdependent relationships illustrated in Figure 6**Error! Reference source not found.** to justify why holistic nalysis of complex interdependencies within the infrastructure system of systems has greater value than, and must be prioritised over, the conceptually more simple analysis of linear dependencies.

'These complex relationships are characterized by multiple connections among infrastructures, feedback and feedforward paths, and intricate, branching topologies. The connections create an intricate web that, depending on the characteristics of its linkages, can transmit shocks throughout broad swaths of an economy and across multiple infrastructures. It is clearly impossible to adequately analyze or understand the behavior of a given infrastructure in isolation from the environment or other infrastructures. Rather, we must consider multiple interconnected infrastructures and their interdependencies

in a holistic manner.' Rinaldi et al. (2001).

Dimensions for Describing Infrastructure Interdependencies

As outlined above the six dimensions in Figure 4 (Rinaldi *et al.*, 2001) are of direct significance to the remit of this study and the application of NAT and HRO to the analysis of infrastructure systems resilience and the resilience of digitally connected infrastructure systems. Each of these dimensions is outlined in Table 11 below.

Table 11. Interdependency Dimensions Overview (adapted from Rinaldi et al. (2001).

Dimension	Description
Coupling and Response Behaviour	When defining this dimension, Rinaldi et al (2001: P19) makes direct reference to NAT. The dimension is focused on the two system characteristics, Coupling and Interaction, which if tight and complex respectively, create the type of high-risk system in which NAT predicts Normal Accidents are inevitable. This dimension, demonstrates that interdependent infrastructure systems fit the definition of high-risk systems referred to in NAT. Therefore, implying normal accidents are inevitable in interdependent infrastructure systems. Rinaldi provides clarity on the use of the concepts in NAT in relation to infrastructure systems. On coupling: *In sum, tight and loose coupling refer to the relative degree of interdependency among the infrastructures.* Rinaldi et al (2001: 19) On interactions The concept of '*coupling order'* illustrates that interdependencies can be direct (1st order) or indirect through one or more intervening infrastructures (2nd, 3rd, …. nth order). Furthermore, the concept provides terminology to enable more detailed analysis and increased understanding of the *incomprehensible interactions* referred to by NAT. *In these real-world examples, disturbances rippled through and across the interconnected infrastructures and created nth-order effects.* Rinaldi et al (2001: 20)
Environment	This dimension emphasises the breadth of infrastructure system interdependence. Interdependence stretches far beyond the interaction of technical or engineered components with one another, to include interactions with and between those elements that comprise the broader context in which an infrastructure is embedded. This dimension is aligned with the systemic concepts of infrastructure as a complex adaptive system (CAS), or infrastructure as part of a socio-technical-system, or infrastructure as a large technical system (LTS) (NB: see section 3.5 of this reviewer for further details).

	The dimension makes explicit that system performance can, therefore, be affected positively or negatively by changes (intentional or otherwise) to any component of the environment in which they are embedded.
'**State of Operations'**	*The state of operation of an infrastructure can be thought of as a continuum that exhibits different behaviors during* ***normal operating condition****s (which can vary from peak to off-peak conditions), during times of* ***severe stress or disruption****, or during times when* ***repair and restoration activities*** *are under way. At any point in the continuum, the state of operation is a function of the interrelated factors and system conditions depicted [by the interdependency dimension in Fig. 4].* Rinaldi et al (2001) The mutual independence between state of operations and the other 5 interdependence dimensions is closely aligned to the HRO principle *Sensitivity to operations,* and the need for this principle to be mindfully observed in interdependent infrastructure systems if HRO is to reduce the inevitability of normal accidents. Furthermore, the dimension demonstrates that in an interdependent system, the assumption that the actual system performance is perfectly aligned with predicted or expected performance, must regularly be reviewed.
'Types of Failure'	*Interdependencies increase the risk of failures or disruptions in multiple infrastructures, as the power crisis in California has demonstrated. The subtle feedback loops and complex topologies created by interdependencies can initiate and propagate disturbances in a variety of ways that are unusual and difficult to foresee.* Rinaldi et al (2001) In terms evocative of the distinction made in NAT between Normal Accidents and single component failures, Rinaldi makes the distinction between (i) *interdependence-related disruptions* and (ii) disruptions confined to a single infrastructure. Three types of *interdependence-related disruptions* are identified, how each would occur is described below. Significantly, Rinaldi observes that *interdependence-related disruptions* can only occur if propagated via interdependencies from an initial disruption to a single infrastructure. *interdependence-related disruptions* are therefore, failures to confine disruptions of type (ii) **A cascading failure** occurs when a disruption in one infrastructure causes the failure of a component in a second infrastructure, which subsequently causes a disruption in the second infrastructure. **An escalating failure** occurs when an existing disruption in one infrastructure exacerbates an independent disruption of a second infrastructure, generally in the form of increasing the severity or the time for recovery or restoration of the second failure **A common cause failure** occurs when two or more infrastructure networks are disrupted at the same time: components within each

<table>
<tr><td></td><td>network fail because of some common cause. Components from multiple infrastructure networks could be affected simultaneously, either because the components occupy the same physical space (a geographic interdependency) or because the root problem is widespread
(e.g., a natural disaster, such as an earthquake or flood, or a man-made disaster, such as a terrorist act).

Arguably, Rinaldi can be paraphrased as ‘In interdependent infrastructure system-of-systems (those where interdependencies are present) interdependence-related disruptions are possible, and these types of failure can be thought of as different types of normal accident, because all require interdependence (or complex interactivity) to occur.</td></tr>
<tr><td>‘Types of Interdependence’</td><td>While acknowledging that all interdependencies are contextually unique, through this dimension, Rinaldi proposes that there is enough commonality between interdependencies that it is possible to classify all interdependencies into one of four broad types.

<table>
<tr><th>Type</th><th>Description</th></tr>
<tr><td>Physical</td><td>Two infrastructures are physically interdependent if the state of each is dependent on the material output(s) of the other.</td></tr>
<tr><td>Cyber</td><td>An infrastructure has a cyber interdependency if its state depends on information transmitted through the information infrastructure.</td></tr>
<tr><td>Geographical</td><td>Infrastructures are geographically interdependent if a local environmental event can create state changes in all of them.</td></tr>
<tr><td>Logical Interdependency (none of the above)</td><td>Two infrastructures are logically interdependent if the state of each depends on the state of the other via a mechanism that is not a physical, cyber, or geographic connection.</td></tr>
</table>

This dimension in particular has inspired much subsequent analysis</td></tr>
<tr><td>Infrastructure Characteristics</td><td>All infrastructure systems have a unique combination of Organisational, Operational, Temporal and Spatial characteristics which need to be considered when evaluating infrastructure system behaviour, performance and by all decision making processes.

In the quote below Rinaldi elaborates further, refers briefly to each characteristic, and supports the assertion that infrastructure is a complex adaptive system (CAS)

“All of the aforementioned critical infrastructures have one property in common they are all complex collections of interacting components in which change often occurs as a result of learning processes; that is, they are complex adaptive systems (CASs) [14]. Seen from this perspective, which has important benefits for modelling and analysis, each component of an infrastructure constitutes a small part of the intricate web that forms the overall infrastructure [spatial characteristics]. All components are</td></tr>
</table>

	influenced by past experiences. For example, electric transformers slowly degrade from overuse, and natural gas pipes age over time [temporal characteristics]. *And many components are individually capable of learning from past experiences and adapting to future expectations, such as operating personnel who try to improve their performance and real-time computer systems that adjust electric generator outputs to meet varying power loads* [operational characteristics]. *From a CAS perspective, infrastructures are more than just an aggregation of their components* [organisational characteristics]. *Typically, as large sets of components are brought together and interact with one another, synergies emerge. Consider the emergence of reliable electric power delivery from a collection of well-placed electric generators, transformers, transmission lines, and related components. Simply aggregating the components in an ad hoc fashion will not ensure reliable electricity supplies. Only the careful creation of an intricate set of services will yield a system that reliably and continuously supplies electricity. This additional complexity exhibited by a system as a whole, beyond the simple sum of its parts, is called emergent behaviour and is a hallmark of CASs"* Rinaldi et al (2001: 13)

3.4.3 Tools for identifying and understanding Interdependency in infrastructure Systems

Rinaldi et al (2001), in particular Figure 4, has inspired much subsequent research. This section gives an overview of selected conceptual tools for the analysis of interdependence in infrastructure systems and DCIS. These tools are relevant to this study, to improve understanding of the interaction and coupling impacts of digitally connected infrastructure systems, and therefore their impact on the likelihood of normal accidents and systemic resilience.

For reasons of brevity, this study has excluded quantitative modelling approaches that have been undertaken subsequent the publication of Figure 4. Future work to assess the suitability of these models to assess the study questions is required.

The Interdependency Planning and Management Framework (IP&MF)

At the core of the proposed [IP&MF] framework is a strategic set of systems thinking principles, processes and tools which aim to drive infrastructure proposers and delivery teams to look for a) beneficial interdependencies with other infrastructure and policies (synergies), and b) problematic dependencies (systemic vulnerabilities or conflicts) to be managed. (Rosenberg et al., 2014)

Commissioned as part of HM Treasury work to develop supplementary guidance for the Green Book on processes to Value Infrastructure Spend (HM Treasury, 2015), The Interdependency Planning and Management Framework (IP&MF) (Rosenberg et al., 2014) outlines a systemic approach to make planning for interdependencies an explicit part of any infrastructure project. It offers a practical and structured approach, for the identification, analysis and subsequent management of interdependency issues in infrastructure systems. The approach draws on established system thinking principles, and is structured around three

groups of activities: (i) problem structuring; (ii) measurement and appraisal; and (iii) creating stakeholder understanding.

The IP&MF is directly applicable to analysis of the interdependency impacts of increased implementation of digitally connected infrastructure systems (DCIS), and therefore analysis of how digitally connected infrastructure systems (DCIS) impact the NAT characteristics of system interactions and coupling behaviour.

The Interdependence Matrix

The interdependence matrix is an output from the IP&MF (Rosenberg et al., 2014; Rosenberg and Carhart, 2014) and Engineering the Futures work (RAEng, 2011). It can be applied to capture and categorise infrastructure interdependencies on a range of scales. The example shown in Figure 7 is from (RAEng, 2011) and shows analysis of interdependencies between infrastructure sectors. Figure 8 shows the interdependence matrix in a general form. Figure 8 could be used to analyse interdependencies between any infrastructure system and digital communications infrastructure systems (DCIS), or to analyse the ways in which digital connectivity creates and changes interdependencies between different infrastructure systems. Figure 9 shows a greater resolution suitable to examine interdependence between two specific components. The version of Figure 9 shown focuses only ‘interdependence type’ relationships between two elements, but could also be used as a framework for analysis using the infrastructure interdependence categorisation checklist (Table 12) for a more complete characterisation of any interdependence relationship.

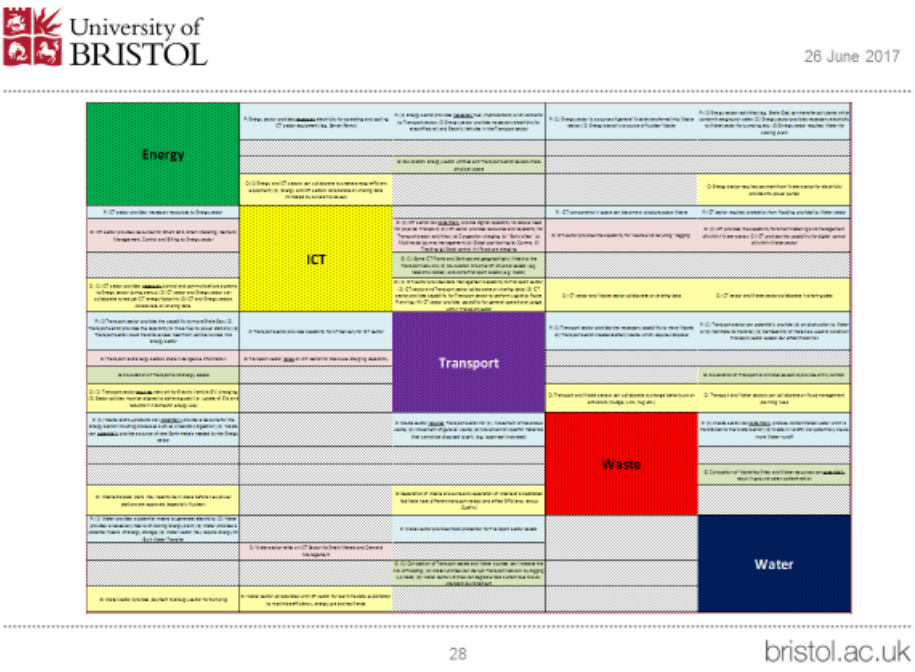

Figure 7. Interdependency Matrix applied to Interdependency between Sectors (Source: RAEng, 2011)

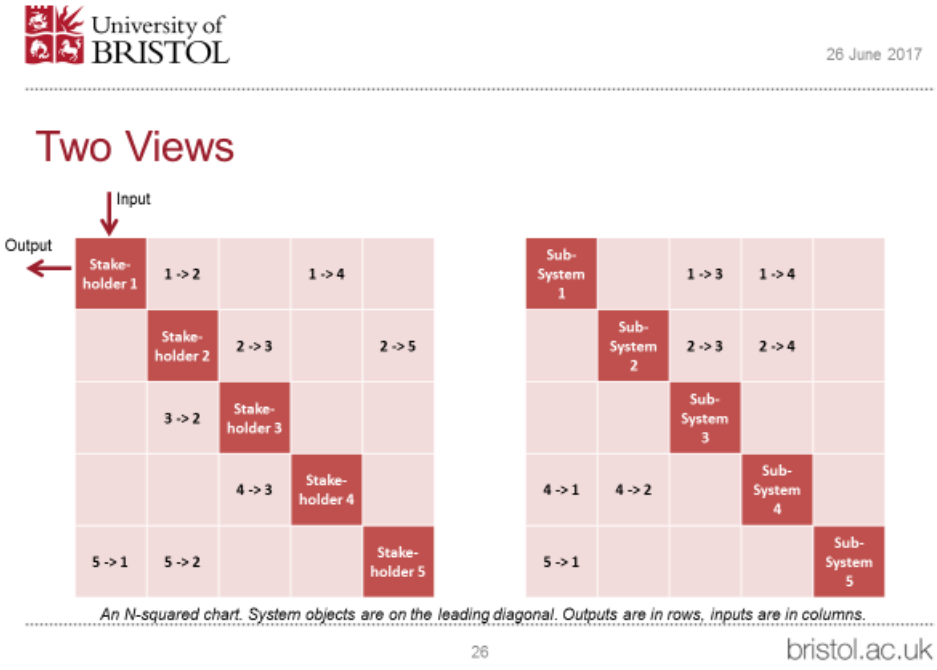

Figure 8. Interdependency Matrix in General Form (Source: Personal communication with Dr Neil Carhart, 2015)

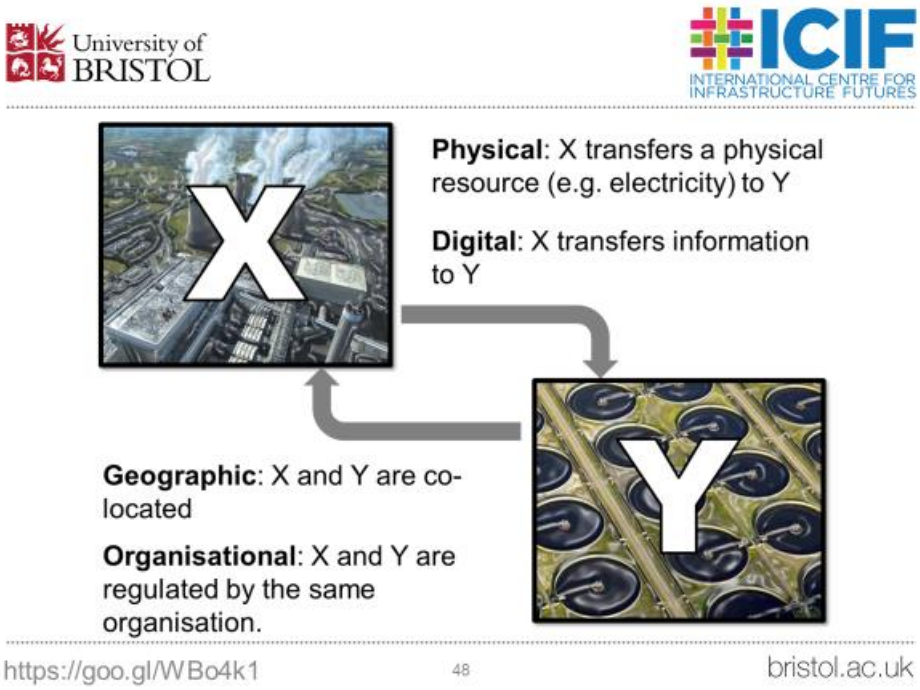

Figure 9. Simplified version of Figure 8 for interdependence between two components (Source: Personal communication with Dr Neil Carhart, 2015)

Using the Interdependence Matrix

To use the interdependence matrix shown in Figures 7, 8 and 9, follow the steps below.

Step 1 – Populate the diagonal with the infrastructure sectors, sub-sectors, stakeholders or other category that are under analysis. For example, in Figure 7 the diagonal is populated with the infrastructure sectors Energy, ICT, Transport, Waste and Water).

Step 2 - Input dependencies and interdependencies between diagonal cells into the appropriate matrix cells: (i) if a sector is dependent on an input from another sector record that in the vertical column, (ii) if a sector produces an output on which another sector depends record that in the horizontal column. For example, in Figure 8 the cell labelled 2>3 lists inputs from stakeholder 2 on which stakeholder 3 is dependent, and the cell labelled 3>2 lists inputs from stakeholder 3 on which stakeholder 2 is dependent.

Step 3 - Classify the dependencies identified using an interdependence classification system. For example, Figures 7 and 9, both use the classification used in Figure 9 and taken from the IP&MF. For more in-depth analysis, use a more detailed classification system such as that presented in Table 12.

Step 4 – Identify direct (first order) interdependencies. Sectors are directly interdependent where both relevant cells are populated, for example in Figure 8, stakeholder 2 and 3 are interdependent because both cells 2>3 and 3>2 are populated.

Step 5 – Identify indirect (higher order) interdependencies. For example, in Figure 8 stakeholder 4 and stakeholder 2 have a second order interdependency because although not directly connected, they are connected through Stakeholder 3. Stakeholder 2 is dependent on stakeholder 3, who is in turn dependent on stakeholder 4.

Infrastructure Interdependence Characterisation Checklist

Drawing on many of those sources listed above and their experience in compiling the IP&MF (Rosenberg et al., 2014; Carhart and Rosenberg, 2015.) Carhart and Rosenberg (2016:50) extend the *interdependence type* and *infrastructure characteristics* and *response behaviour* dimensions from Figure 4 into an infrastructure interdependency characterisation checklist (Table 12) (ref p50). This provides a set of terminology that can be utilised to characterise the interdependencies in any *high-risk* system and enable deeper understanding of the interaction and coupling behaviour in infrastructure system or DCIS. For the purposes of this study the column 'link to Figure 4 dimension' has been added to Table 12.

Table 12. Infrastructure Interdependency Characterisation Checklist

Characterisation	Description	Possible States	Link to Figure 4 Dimensions*
DIRECTIONALITY	*Whether the reliance of one element on another is mutual*	Bi-directional	An interdependent relationship (Fig 6)
		Non-reciprocal	A dependent relationship (Fig 5)
ORDER*	*Whether the relationship is direct or via an intermediary.*	First Order	A concept mentioned by Rinaldi, but not explicit in Fig. 4. The terms illustrate interdependencies can be direct, or Indirect via one, two or more intermediaries. Examples can be seen in Fig. 6
		Second Order	
		Higher Order	
COUPLING	*Whether the effects of the relationship are felt closely in time and space or not.*	Loose	Response and Coupling behaviour
		Tight	
LOCATION*	*Whether the element of interest provides or receives a resource.*	Upstream	Not explicit in Figure 4. Extension of the spatial component of the infrastructure characteristics dimension
		Downstream	
TYPE	*The nature of the relationship, spatially or in terms of resource flow.*	Physical	A refinement of Interdependency type dimension
		Digital	
		Geographic	
		Organisational	
INTERACTION TYPE	*The degree of co-operation and structure of the relationship.*	Competition	Not explicit in Figure 4. Either a new dimension or an extension of the response and coupling behaviour dimension
		Symbiosis	
		Integration	
		Spill Over	
FUNCTIONALITY	*Whether the relationship is an integral part of the function of the elements or not.*	Functional	Not explicit in Figure 4. An additional component of the Response and Coupling behaviour dimension
		Non-Functional	
NECESSITY*		Necessary	

	Whether the relationship is unavoidable or required, or whether there is flexibility.	Optional	Not explicit in Figure 4. An additional component of the Response and Coupling behaviour dimension
OUTCOME*	*Whether the effect of the relationship on the element of interest in positive or negative.*	Benefit	Not explicit in Figure 4, Interdependency can be an opportunity, rather than always a risk
		Dis-benefit	
LIFE-CYCLE IMPACT STAGE	*The phase of the project during which the effects of the relationship are relevant.*	Planning	Extension of the temporal component of the infrastructure characteristics dimension
		Construction	
		Operation	
		End of Life	
		Scenario	
GEOGRAPHIC SCALE	*The spatial distribution of the relationship or its effects.*	Project	Extension of the spatial component of the infrastructure characteristics dimension
		Local	
		National	
		International	
SECTORAL SCALE	*Whether the relationship is contained within one infrastructure sector or not.*	Intra-Sector	Extension of the organisational component of the infrastructure characteristics dimension
		Inter-Sector	

Workshop Approaches

The Anytown Project led by The London Resilience Partnership[3] has developed ripple diagrams such as Figure 10 to capture findings from interdependence workshops with front line emergency response professionals. The workshops attempt to gauge what *interdependence-related disruptions* are likely to occur in other infrastructure sectors (see labels in grey Figure 10) if any failure in a critical infrastructure sector were to occur. Each segment of the diagram captures how the incident unfolds in a different sector or element of the infrastructure system-of-systems. Each layer of the diagram represents a greater time from the initial

[3] NB: on behalf of the Mayor of London, Greater London Authority, Local Authorities and London Fire Brigade, The London Resilience Partnership coordinates institutions and communities to prevent, handle, recover and learn from disruption, and adapt to change; to ensure London survives and prospers. The Partnership brings together over 170 organisations who each have specific responsibilities for preparing for and responding to emergencies. In addition the partnership is growing to include organisations and communities of all types to help ensure a holistic approach is taken. See https://www.london.gov.uk/about-us/organisations-we-work/london-prepared for more information.

incident to chart how the disruption would develop if the initial incident remained unresolved.

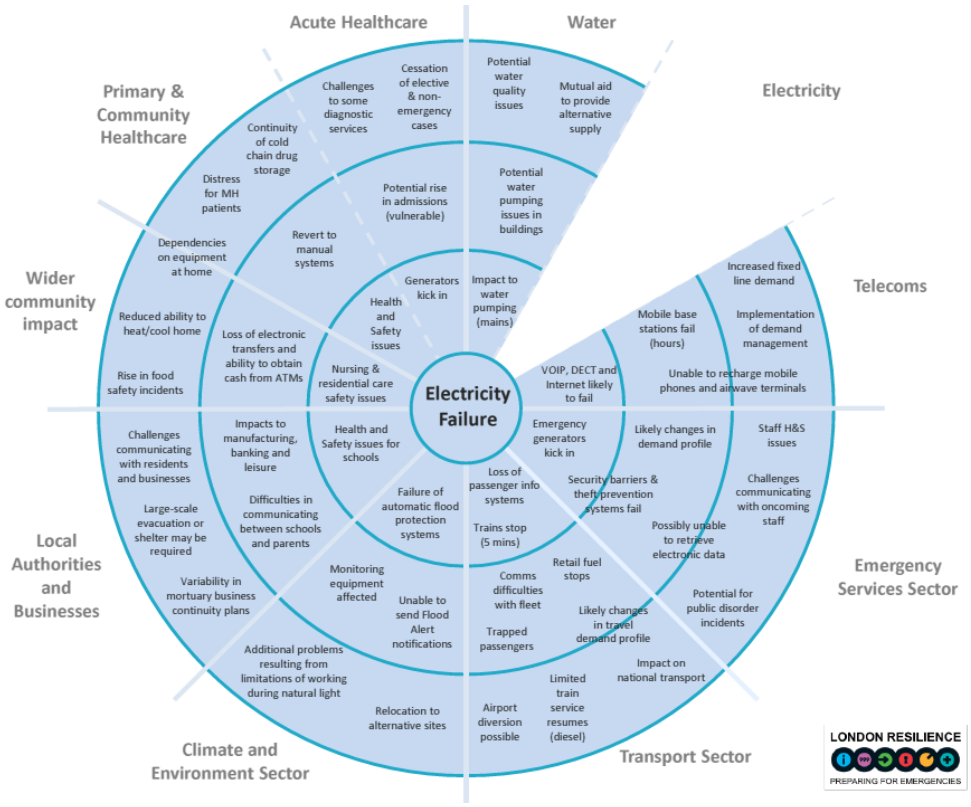

Figure 10. Anytown Interdependency Ripple Diagram

To date the Anytown Project have conducted at least 4 workshops to examine impacts of gas, telecoms, water and power failure. Figure 10 illustrates findings from the power failure workshop, a report of findings and methodology are available (Hogan, 2013). NB: although the report is dated 2013, at time of writing the Anytown project remains active and most recently hosted a workshop on 3rd July 2017.

From the perspective of this study a workshop that combines the terminology from Figure 4 and Table 12, with the IP&MF methodology, Interdependence Matrix and Anytown Ripple Diagrams, to specifically explore the impacts of Digitally Connected Infrastructure System interdependency and failure impacts is suggested as a next step to extend this work.

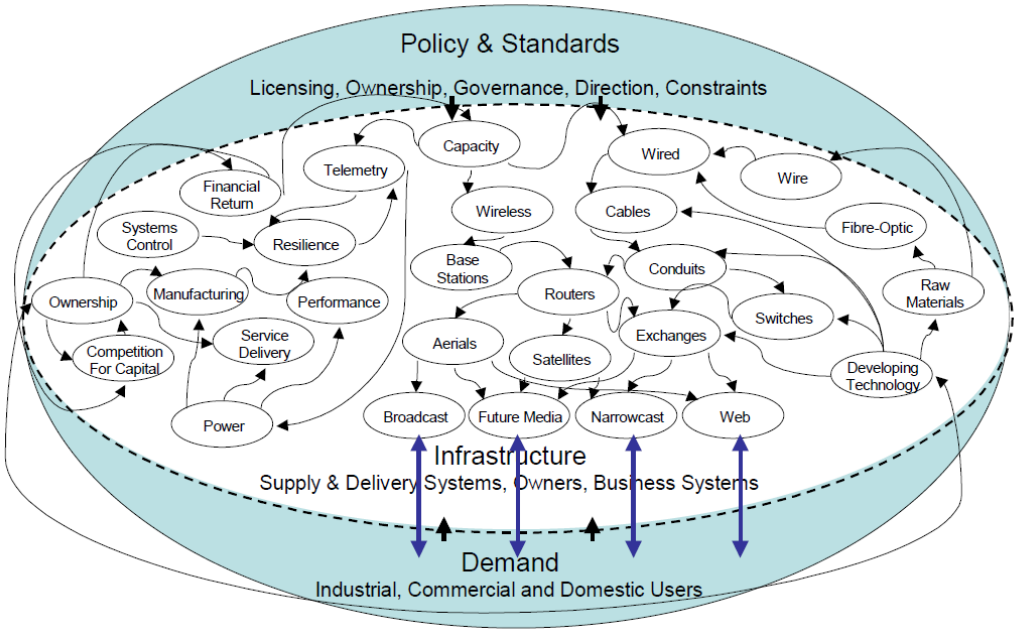

Figure 11. Example of Systemic Interdependency Mapping for ICT Infrastructure (Source: Beckford Consulting, 2009)

Comprehensive mapping of systemic interdependencies of UK infrastructure systems (similar to Figure 11) was undertaken for all infrastructure sectors as part of a series of workshops hosted in 2009. Figure 11 maps interdependencies within ICT infrastructure. Similar mapping and analysis is available for all infrastructure sectors (Beckford Consulting, 2009)

3.5 Infrastructure as a Complex Adaptive Systems

3.5.1 Overview of Systems and Complex Systems

Elliott et al. (2007) in a report written for the Royal Academy of Engineering, provide an explanation of what is meant by the terms System, emergent properties and complex system

- A **system** is a set of parts which, when combined, have qualities that are not present in any of the parts themselves.
- **Emergent properties** Those qualities of the system, that are not present in any of the parts themselves.

- **Complex system** are systems in which the parts interact with each other and with the outside world in many ways – the relationships between the parts determine how the system behaves.

A system is closed and independent of the outside world, a complex system is open and interdependent with the outside world.

Elliott et al. (2007), recommend six principles to provide a pervasive framework for understanding the challenges of [infrastructure system decision making as] a system design problem and for educating engineers to tackle those challenges:

1 Debate, define, revise and pursue the purpose
2 Think holistic
3 Follow a systematic procedure
4 Be creative
5 Take account of the people
6 Manage the project and the relationships.

The h*igh-risk* technologies referred to in NAT, are systems because they have emergent properties from the interaction of the parts. Moreover, they are complex systems because when in operation, they become part of a broader socio-technical system (STS) comprising not just the high-risk technology but also the context in which they are embedded.

Based on the same reasoning, the High Reliability Organisation (HRO) is also a system. HRO recognises that organisations become complex systems if they are deeply interdependent with the broader STS within which they are embedded. In this context, HRO is effectively a suite of interventions intended to reduce coupling, the complexity of interactions and lessen dependence on specific interactions in organisations.

3.5.2 Complex adaptive systems

In the case of infrastructure systems, Rinaldi et al (2001) illustrates that infrastructure is not just a complex system but rather a complex adaptive system (CAS). Where a complex adaptive system is a complex system capable of undergoing evolution.

> *"A CAS can be defined as containing a large number of agents which interact, learn and most crucially, adapt to changes in their selection environment in order to improve their future survival chances (Holland, 2006)."*

In an ITRC working Paper Infrastructure as a CAS (Oughton, and Tyler., 2013) provide evidence to demonstrate that the infrastructure system of systems is a CAS and therefore conclude:

"*we need to Reframe our Thinking of Infrastructure systems…by utilising concepts drawn from Complex Adaptive Systems (CAS) theory. [CAS] can help recognise the interdependencies that exist between supply and demand, between infrastructure sectors, and how the agents of national infrastructure systems tend to adapt and co-evolve over time…[the need for CAS] perspectives is illustrated with a case-study example of Information Communications Technologies (ICT) infrastructure, for which the complex adaptive Lens is found to be particularly amenable."*

This observation is particularly pertinent to this study because if introducing digital connectivity into already established infrastructure systems to create digitally connected infrastructure systems (DCIS) increases the adaptive potential of a CAS or transforms a complex system into a CAS, then digitally connected infrastructure systems (DCIS) will require a further shift in how we think about and make decisions related to infrastructure systems. Collectively, we already struggle to manage emergent properties in infrastructure decision making processes, managing and planning for emergent co-evolution in infrastructure systems will be harder still.

In recognition that infrastructure is a complex system and often a CAS, Beckford (2013) provides a practical overview of the range of systems engineering and systems thinking methods applicable to the management of infrastructure systems. Figure 12 represents the co-evolution between the provision of infrastructure systems and the demands of the socio-technical systems (STS) in which they are embedded. Infrastructure services and elements of society are shown as emergent properties of the infrastructure systems that enable them, but demand for infrastructure systems is in turn shaped by societal expectations which feedback as demand for infrastructure systems capable of enabling the outcomes society expects. In short, as the provision of infrastructure systems makes new outcomes possible, societal expectations normalise demand for these outcomes.

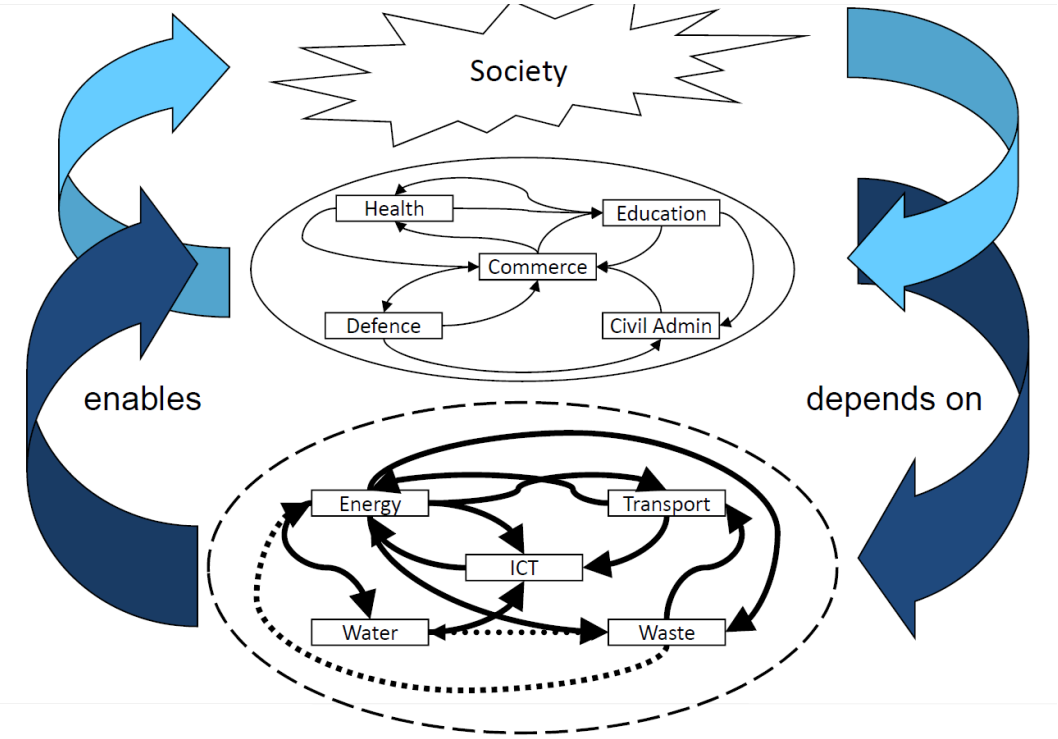

Figure 12. Infrastructure Enables Society - Society Demands Outcomes - Infrastructure as CAS (Source: Beckford, 2013)

Furthermore, in the Intelligent Organisation (Beckford, 2016) Beckford suggests that IT [and digital connectivity] are simply an enabling system. The significance

being that if the implementation of digitally connected infrastructure systems is coupled with organisational paradigms and thinking tools, to purposefully convert data into meaningful information [information is *data which has been filtered, integrated, assimilated, aggregated and contextualised to enable decisions* (Silver, 2012 quoted in Beckford p1]. Digitally connected infrastructure systems can enable improved knowledge of actual system performance, and facilitate an improved capability for systemic decision making. Conversely, if this is not the case, there is no guarantee that the improved capability for data collection enabled by digitally connected infrastructure systems will improve the quality of decision making.

From the perspective of managing complex systems, Donella Meadows article Leverage Points Places to Intervene in a System (Meadows, n.d.) requires further analysis as a tool for targetted DCIS implementation.

3.5.3 Large Technical Systems

In influential work on The Evolution of Large Technical Systems Hughes (1987), developed a number of terms directly relevant to analysis of the impacts of digital transformation in infrastructure systems – the evolution of infrastructure systems into digitally connected infrastructure systems. Specifically

i) The concept of infrastructure as a collection of Large Technical Systems (LTS) that have since their inception evolved in response to changing patterns of demand and expectations placed on them, and will continue to evolve in response to future changes.

ii) The proposal that the mechanism by which evolution takes place is through the 'rafting' of technical fixes onto the established LTS.

iii) LTS evolution is typically a response to 'reverse salients' or a pre-emptive adoption of forward salients.

In a paper highly applicable to this study, Egan (2007) provides further insight into the significance of each of the above

i) Infrastructure as LTS:
Many modern technologies have evolved into large and complex technical systems: 'spatially extended and functionally integrated socio-technical networks' such as electrical power, railroad, and telephone systems (Hughes, 1987: 11). These systems create vast efficiencies that have allowed for shifts in lifestyle and work especially in industrialized countries. The LTS will have developed through a planned, or more likely unplanned, 'rafting' together of many different systems, each relying on the next for efficiency, stability and effectiveness.

ii) Rafting as the mechanism of LTS and infrastructure system evolution
Rafting', as it is used here, refers to the joining of different elements to achieve a purpose usually unrelated to the purpose of each of the individual elements. Much like a raft made of many different foraged pieces of flotsam all lashed together with bailing wire, each of which contributes to the overall buoyancy of the watercraft, but none of which was designed specifically for flotation, a LTS is

composed of many different technical and organizational elements each of which contributes to the overall function of the system, but few of which were designed to serve a larger system.

iii) Reverse and Forward Salients as drivers of LTS evolution

Reverse salients are voids in the system that emerge as large technical systems expand. Reverse salient require socio-technical fixes to address them, and adapt the system, if not addressed reverse salient may lead to system transformation…A socio-technial fix in response to a Reverse salient, is a response that alleviates a known constraint on LTS growth.

Forward Salients are needs in the LTS, that only becomes obvious after the socio-technical fix has been applied. New technologies can serve as forward salients. Rather than providing a socio-technical fix to system vulnerabilities. Technlogy as a Forward salient is where a new technology development makes LTS growth possible….. The World Wide Web is an example of a 'forward salient' technology for which there was little need – and which was thus not critical – until it was created; as its uses became more varied and widespread, it also grew increasingly critical.

Furthermore, Egan (2007) makes explicit why i-iii are significant by citing the world wide web, Wi-Fi wireless broadband internet, ATM machines, credit cards, spreadsheet software, database technology, email, portable email devices, fibre optic cable, satellite communication systems, video-conferencing, GPS network, google as examples of digitally enabled technologies that have rafted onto established infrastructure systems to improve the performance, and in so doing drive digital transformation from infrastructure systems to digitally connected infrastructure systems (DCIS).

Moreover, Egan (2007) builds on i-iii with a number of observations/cautionary tales applicable to the study of the impact any LTS evolution may have on system interactions, coupling and reliability (summarised below) and develops two approaches (the criticality Spectrum and a consequence-based characterization of criticality) to aid those who rely on new technologies to anticipate the vulnerabilities they create (see Egan, 2007, figure 1, Table 1, and Appendix 1).

- If used to address a reverse salient or forward salient it is possible for a technology to become critical, and for the LTS to become exposed to vulnerabilities inherent in these technologies used as socio-technical fixes.
- Typically, the socio-technical 'fixes' used to enable LTS growth are technologies or services that are not fully tested before they are implemented, and if successful can become critical support elements of critical systems despite being untested
- The consequences of systemic failure can be magnified by the type and complexity of the socio-technical systems of which they are a part.
- Increasing usage and reliance on emerging technologies creates vulnerabilities to the shortcomings of those technologies, especially where they have not been fully tested.

3.6 Summary of Best Practise Findings from Literature Review

Tables Table 13 -16 provide a summary of best practise findings relevant to this study from the HRO (Table 13), systemic resilience (Table 15), infrastructure interdependence (Table 14), and systemic perspectives (Table 16) sections of the literature review (sections 3.1 -3.5).

Table 13 Summary Table of Literature Review Best Practise Findings – HRO

		Best Practise Concept	Section
HRO	H1	High reliability should be an aspirational goal, a clearly stated priority, and at the heart of decision making processes and operations.	Table 4, Table 5
	H2	High reliability is created by people, enabled by supportive organisational structures. The right people and organisational culture are needed to achieve High reliability	Section 3.1.1 Figure 2
	H3	The principles of HRO (Table 7) can be characterised as actions to address one or both of the high-risk characteristics (coupling and interactions) identified by NAT.	Section 3.2
	H4	HRO is a useful starting point for planning how to increase the reliability of any digitally connected infrastructure systems. However, HRO is not a panacea, it cannot eliminate normal accidents, but It can reduce the likelihood (therefore frequency) and impacts of normal accidents.	Section 3.1.2
	H5	HRO principles, like any intervention in a complex system can unintentionally increase complex interactivity or tighten system coupling. Therefore, HRO can have unintended consequences that increase normal accident likelihood.	Table 5 Table 6
	H6	Achieving High reliability is not a single, one-off action. HRO is not a menu of options, rather HRO requires full implementation of HRO principles as a suite of purposeful interventions that are continuously implemented, monitored and refined.	Section 3.1.2
	H7	There is a trade-off between managing for an efficient system and managing for high reliability.	Section 3.1.1 Table 7
	H8	HRO is focused on organisations. Implementing HRO principles in a complex or complex adaptive system where competing priorities abound, may not be feasible. HRO needs to be adapted for use in complex adaptive systems	Sections 2.2 Section 3.1.1 Section 3.5 Table 7
	H9	High reliability (like systemic resilience) is a mindset (it requires mindful implementation of principles). Symptoms of mindlessness are warning signs that must not be ignored or normalised	Section 3.1.2 Table 6 Table 7

Table 14 Summary Table of Literature Review Best Practise Findings – Interdependence

		Best Practise Concept	Section
Interdependence	I1	Interdependency offers a conceptual framework and terminology to better differentiate between: Digital technology; digital infrastructure; infrastructure systems; and digitally connected infrastructure systems in terms of the interactions (interdependencies) that characterise them. Whereas digital infrastructure (ICE, 2017) refers to communications infrastructure – both fixed (broadband) and wireless (mobile) assets and systems – (Infrastructure that enable digital connectivity and the use of digital technologies) Digitally connected infrastructure system (DCIS) refers to any infrastructure system that has one or more cyber interdependence (Table 11) or digital interdependence (Table 12) with a digital technology or the digital communications infrastructure. Digital transformation as used in ICE (2017) refers to a process of transformation from an infrastructure system independent of digital infrastructure to one increasingly functionally interdependent with digital infrastructure i.e. a digitally communicated infrastructure systems (DCIS).	Interdependence dimensions Figure 4 Table 11 Table 13 Interdependence characterisation checklist Table 12 Figure 5 Figure 6
	I2	Interdependency offers a conceptual framework, terminology and a set of conceptual tools/methods to analyse the high-risk system characteristics (coupling and interactions) identified by NAT.	Interdependence dimensions Figure 4 Table 11 Table 13 Interdependence characterisation checklist Table 12 The Interdependence Matrix Figure 7 Figure 8 Figure 9 Interdependency Ripple Diagram Figure 10 Systemic Interdependency Mapping Figure 11
	I3	A conceptual framework to differentiate between (i) *interdependence-related disruptions* (Normal accidents) and (ii) disruptions confined to a single infrastructure (component failure accidents). A three-part classification of different types of *interdependence-related disruptions* (cascading failure, escalating failure, common cause failure).	
	I4	A set of conceptual tools and terminology to better understand current infrastructure system characteristics: (i) prior to assessing systemic needs; (ii) with a view to understanding systemic impacts of pipeline projects; (iii) with a view to understanding systemic impacts of all special study and NIA recommendations	
	I5	A conceptual framework applicable to all infrastructure sectors that can be used to analyse systemic root causes, and identify systemic challenges and opportunities common across sectors.	
	I6	A set of conceptual tools and terminology to improve analysis of systemic resilience and reliability and the impact of digital transformation (or any other change to the system) on systemic resilience.	

Table 15. Summary Table of Literature Review Best Practise Findings – Systemic Resilience

Best Practise Concept			Section
Systemic Resilience	R1	Resilience is a property of a system that emerges from the interaction between (interdependence of) system components.	Section 3.3 Section 3.4 Section 3.5
	R2	Systemic resilience requires the systemic characteristics (abilities/capabilities) outlined in Table 9, or the characteristics of a dynamic system Table 8	Section 3.3 Table 8 Table 9
	R3	To sustain systemic resilience requires a dynamic approach to all phases of the resilience cycle , in order to develop, maintain, enhance the above abilities/ capabilities (Table 9)	Section 3.3.1 Figure 2 Figure 3 Table 8 Table 9
	R4	It is not possible (or at least very difficult) to be systemically resilient without evaluating the systemic impacts of sectoral decision making processes.	Section 3.3
	R5	Efficiency and systemic resilience, can be conflicting objectives. In order to be resilient, any action(s) to increase efficiency or optimise a system must not trade-off against the resilient system abilities.	Section 3.1.1, section 3.3, section 3.3.1.2
	R6	In infrastructure systems, systemic resilience requires regular evaluation and review of interdependencies and may require a regular strategic re-evaluation of desired function(s)/outcome(s); business models; mode of delivery; system performance; asset condition. 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 a systems ability to pro-actively adapt to systemic vulnerabilities	Section 3.3 Table 10 Table 12 Figure 2 Figure 3
	R7	The resilience of a digitally connected infrastructure system cannot be considered in isolation from the resilience of the underlying infrastructure system. Digitally connected infrastructure system resilience is a function of: (I) pre-existing vulnerabilities within the underlying infrastructure system; (ii) vulnerabilities within the digital technologies enabling the digital connectivity, and (iii) new vulnerabilities from the creation of new interdependencies between the digital technology and infrastructure system that comprise the digitally connected infrastructure system	Section 3.3 Section 3.4 Section 3.5.3

Table 16. Summary Table of Literature Review Best Practise Findings – Systemic Perspectives

Best Practise Concept			Section
Systemic Perspectives	S1	**Emergent properties** - those qualities of the system, that are not present in any of the parts themselves - are a reality in infrastructure systems, and can be positive (opportunities) or negative (vulnerabilities). If NAT were framed in terms of emergent properties, it can be communicated as the following: (i) emergent properties are inevitable in interactive systems; (ii) some (not all) of these properties will be, to varying extents, negative. Therefore (iii) normal accidents (referring to negative emergent properties) are inevitable in interactive systems.	Section 2.2, Section 3.3, Section 3.4, Section 3.5.1, Section 3.5.2, Section 3.5.3
	S2	Socio-technical fixes are insufficient, emergent systemic problems require systemic understanding and collaborative responses[4]. Digitally connected infrastructure systems cannot be expected to address underlying systemic vulnerabilities	
	S3	Large Technical system (LTS) theory postulates that established infrastructure systems evolve with time in response to selection pressures (which LTS theory calls reverse and forward salients). Digital transformation can be interpreted as the latest stage in LTS evolution, and therefore, likely to follow a predictable mechanism in which digital technologies are 'rafted' onto mature infrastructure as 'socio-technical fixes' in response to selection pressures.	Section 3.5.3
	S4	Digital transformation is therefore a response to, and may to a large extent be constrained by, the current state of infrastructure systems. Therefore: (i) the future path of digital connected infrastructure systems, (ii) their systemic resilience, (iii) reliability or (iv) vulnerability to normal accidents cannot be meaningfully evaluated in isolation from a deep understanding of current infrastructure systems.	Section 3.5.3
	S5	At this early stage in the digital transformation, many digital technologies can be identified as drivers of LTS evolution. Examples are given in section 3.5.3 and in greater detail in Egan (2007)	Section 3.5.3
	S6	We need to Reframe our Thinking of Infrastructure systems …by utilising concepts drawn from Complex Adaptive Systems (CAS) theory.	Section 3.5 Figure 12
	S7	Information is data filtered, integrated, assimilated, aggregated and contextualised to enable decision making. Organisational paradigms and thinking tools, to purposefully convert data into meaningful information are needed if the potential of digitally connected infrastructure systems is to be realised.	Section 3.5.2

[4] "System problems are shared problems: they are caused by no one party in isolation, and can be solved by no one party in isolation. System problems emerge as a consequence of interaction between system components – including the political, social and economic context in which they are embedded – and are best managed collaboratively."
Dolan, T. and Cosgrave, E. (2016). Aligning systemic infrastructure decisions with social outcomes *Civil Engineering*, 169 (4), 147. doi: 10.1680/jcien.2016.169.4.147

4 Digitally Connected Infrastructure Systems' Resilience to Future Change

How might the resilience of digitally connected infrastructure systems change over the next 10 to 30 years?

In 2009, the Council for Science and Technology (CST) 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" (CST, 2009)

Other than the above quote which illustrates a trend of decreasing resilience, no additional literature is presented in this section. The answer to this question draws on literature presented in sections 2 and 3 of this document. In particular, this section draws predominantly on findings presented in Sections 2.2, 2.4 and the summary tables Table 13, Table 14, Table 15, Table 16 presented in section 3.6

With particular reference to points:

- **R7** (Table 15) - The resilience of a digitally connected infrastructure system cannot be considered in isolation from the resilience of the underlying infrastructure system. Digitally connected infrastructure system resilience is a function of: (I) pre-existing vulnerabilities within the underlying infrastructure system; (ii) vulnerabilities within the digital technologies enabling the digital connectivity, and (iii) new vulnerabilities from the creation of new interdependencies between the digital technology and infrastructure system that comprise the digitally connected infrastructure system
- **S2** (Table 16) established infrastructure systems evolve with time in response to selection pressures (which LTS theory calls reverse and forward salients).
- **S3** (Table 16) Digitally connected infrastructure systems cannot be expected to address underlying systemic vulnerabilities in the infrastructure systems they connect
- **S4** (Table 16) Digital transformation is a response to, and to a large extent be constrained by, the current state of infrastructure systems. Therefore: (i) the future path of digital connected infrastructure systems, (ii) their systemic resilience, (iii) reliability or (iv) vulnerability to normal accidents be meaningfully evaluated in isolation from deep understanding of current infrastructure systems
- **R4** (Table 15) It is not possible (or at least very difficult) to be systemically resilient without evaluating the systemic impacts of sectoral decision making processes.

- **R5** (Table 15) Efficiency and systemic resilience, can be conflicting objectives. In order to be resilient, any action(s) to increase efficiency or optimise a system must not trade-off against the resilient system abilities
- **H7** (Table 13) There is a trade-off between managing for an efficient system and managing for high reliability.
- **Section 2.4** Conclusions for digitally connected infrastructure systems from analysis of NAT

Evidence from the literature review supports the conclusion that digitally connected infrastructure systems are unlikely to have a positive impact on inherent vulnerabilities already present in underlying infrastructure systems. Additionally, digital transformation is likely to introduce new vulnerabilities into infrastructure system, and increase both interactive complexity and tighten system coupling.

Therefore, the trend of declining systemic resilience identified by CST (2009) should be expected to continue as we undergo digital transformation towards a world where all infrastructure systems are digitally connected infrastructure systems. It follows, the resilience of digitally connected infrastructure systems (which cannot be analysed in isolation) will over the next 10 to 30 years continue to diminish.

However, implementation of best practise identified in in Sections 2.2, 2.4 and the summary tables Table 13, Table 14, Table 15, Table 16 offers a significant opportunity to explicitly prioritise systemic resilience and other system problems in all infrastructure planning, delivery and operations as part of the digital transformation, and address this trend. Specific recommendations to integrate systemic resilience into core objectives and improve the impact of digital transformation on systemic resilience are presented in Section 5.

Rather than focus on seeking to identify the specific digital technologies that will be predominant in future digitally connected infrastructure systems over the next 10-30 years, this response has focused on the resilience and system parts of the question. This focus is justified, by making reference to points R1, S1 on resilience being an emergent system property, a consequence of interactions rather than a characteristic of any specific component. Points R7 and S4 on systemic resilience of digitally connected infrastructure systems being closely connected to the resilience of the original infrastructure systems which have evolved through digital transformation into digitally connected infrastructure systems. We do however acknowledge that some analysis of the precise digital technologies that will be in place 10-30 years from now would be a useful complement to the recommendations from the literature review, but such analysis should not be the starting point to address this question.

5 Key recommendations from Literature Review

What key recommendations would we make to reduce the frequency of normal accidents, and for areas of further research?

Based on this literature review, eight recommendations (A-H) are listed below. Further details of each recommendation are provided in sections 5.1 - 5.8

A. Apply LTS theory and CAS thinking to analyse digital transformation impacts and DCIS resilience

B. Prioritise organisational paradigms and thinking tools to support Resilient Digital Transformation

C. Make systemic resilience a core objective of DCIS decision making and implementation.

D. Develop an interdependency toolkit for DCIS resilience analysis

E. Define DCIS explicitly in terms of interdependency with underlying infrastructure systems

F. Adopt a more nuanced approach to understanding of Normal accidents

G. Adapt HRO to develop a set of HR complex System principles

H. Undertake research to assess application of Meadows (n.d.)[5] to DCIS planning

5.1 Recommendation A: Apply LTS theory and CAS thinking to analyse digital transformation impacts and DCIS resilience

Points R7 (Table 15) and S2, S3, S4, S5 and S6 (Table 16) of this study identified LTS theory as a practical perspective for analysis of digital transformation and DCIS resilience.

Additional research to review the full body of literature on LTS and develop a conceptual framework to analyse DCIS resilience using LTS theory is recommended.

[5] Meadows, D., n.d. Leverage Points: Places to Intervene in a System. Acad. Syst. Change.

5.2 Recommendation B: Prioritise organisational paradigms and thinking tools to support Resilient Digital Transformation

This recommendation is in direct response to conclusions in section 4 and builds on point **S7** (Table 16).

Information is *'data which has been filtered, integrated, assimilated, aggregated and contextualised to enable decisions'* (Silver 2012 quoted in Beckford p1).

In order to fully exploit the potential of the greatly enhanced data collection capabilities made possible by DCIS, organisational paradigms and thinking tools, that purposefully convert data into meaningful information are needed.

If adopted such tools will enable DCIS to provide a source of meaningful insight into system interdependencies, actual system performance, the likelihood and expected impact of normal accidents (emergent system properties) and other properties that underpin systemic resilience. Insights which in turn can be used as meaningful inputs into both: (i) Real-time operating decisions and (ii) strategic systemic decision making processes, in particular the National Infrastructure Assessment (NIA), National Infrastructure Commission special studies and the National Infrastructure Development Plan.

Additional research to review current approaches and develop organisational paradigms and thinking tools to enable DCIS to provide the information needed to improve systemic resilience and alleviate system vulnerabilities is recommended.

5.3 Recommendation C: Make systemic resilience a core objective of DCIS planning

This study identified the need to pro-actively address normal accidents and improve systemic resilience of infrastructure systems. It is recommended, based on justification provided in points R5 (Table 15), R1 (Table 15), S1 (Table 16) of this study, that systemic resilience is integrated into the core objectives for all NIC work. Systemic resilience requires either equal weighting with efficiency in decision-making processes, or action to ensure that systemic resilience impacts are made explicit during decision-making processes.

The following actions are recommended:

- Adopt the resilience cycle (Figure 2) as a communication tool to emphasise the importance of a dynamic approach to resilience planning
- Make assessment of the potential impacts on systemic resilience an explicit consideration in all decision-making processes. Consider basing this assessment on an evaluation of the abilities of a resilient system (Table 9)
- Make the type of review proposed in R6 (Table 15) an explicit component of future NIA methodology.

- Commit to evaluate all future recommendations arising from the NIA and NIC special studies in terms of impact on systemic resilience.
- Work with partners in other relevant bodies to develop a commitment to evaluate projects in terms of impact on systemic resilience prior to inclusion in the infrastructure pipeline.
- Champion the need for a similar systemic resilience impact evaluation for projects already listed in the infrastructure pipeline and recommendations already made in NIC special studies.
- Commission further research as detailed in recommendation D

5.4 Recommendation D: Develop an interdependency toolkit for DCIS systemic resilience analysis

Interdependence analysis potentially enables greater understanding of the root causes of infrastructure system resilience, vulnerabilities, performance and other systemic challenges.

Commission further research to: (a) develop an interdependency toolkit from the approaches identified in this study (see Table 14), and (b) establish a set of practical process to apply the interdependence toolkit to support analysis of: the interdependencies that enable DCIS; possible options to minimise new vulnerabilities create when implementing DCIS; the root causes of systemic resilience and vulnerabilities in DCIS and the underlying infrastructure systems of which they are a part.

NB: the focus of this research could be on repurposing/tailoring the IP&MF for this application, or may require a development of a new approach specifically for the proposed analysis.

5.5 Recommendation E: Define DCIS explicitly in terms of interdependency with underlying infrastructure systems

Interdependency offers a conceptual framework and terminology to better differentiate between the closely related terms: Digital technology; digital infrastructure; infrastructure systems; and digitally connected infrastructure systems in terms of the interactions (interdependencies) that characterise them. The provision of clear consistent definitions agreed by all infrastructure practitioners and linked to the concept of infrastructure interdependence, is recommended as an action to support greater clarity of discussion around the impacts of digital transformation.

NB: The definitions of digital transformation, digital delivery, digital infrastructure provided in the recent ICE state of the nation report (ICE, 2017) and the concept digitally connected infrastructure system used in this review are recommended as a starting point for this work.

5.6 Recommendation F: Adopt a more nuanced approach to NAT in Infrastructure Systems

The key points made in sections 2.2 and 2.4, demonstrate that NAT can provide a useful lens to analyse emergent system properties. In the context of infrastructure systems, the term normal accident is applicable to any emergent property of the infrastructure system. It follows, system problems such as local air quality, managing flood risk, congestion can all be interpreted as normal accidents.

Further research to develop a process to analyse these types of systemic infrastructure challenges from an NAT, interdependence and systemic resilience perspective is recommended.

5.7 Recommendation G: Adapt HRO to develop a set of HR Complex System principles

The concept of high reliability should be given a similar status to systemic resilience as a core objective for NIC work (Recommendation C). Specifically, achieving high reliability should either be given equal weighting with efficiency in decision-making processes, or ensure that impacts on the 'high reliability' of a system are made explicit during decision-making processes.

At present HRO principles are focused primarily on organisations and will require refinement if they are to be fully applicable to interdependent infrastructure systems (points H2, H8 in Table 14). This is a significant challenge because HRO principles require full implementation if high reliability is to be achieved.

Therefore, further research is needed to (i) investigate the applicability of HRO principles to interdependent infrastructure systems and DCIS is recommended; (ii) adapt HRO principles as necessary based on the findings of (i) is recommended.

5.8 Recommendation H: Undertake research to assess application of Meadows (n.d.) to DCIS planning

Further research to assess how insight from Donnella Meadows work Leverage Points: Places to Intervene in a System[6], can be applied to tailor approaches to DCIS implementation that minimise impacts on systemic resilience and the likelihood of normal accidents is recommended.

[6] Meadows, D., n.d. Leverage Points: Places to Intervene in a System. Acad. Syst. Change.

6 Reference List

A Framework for Establishing Critical Infrastructure Resilience Goals, 2010. . National Infrastructure Advisory Council, USA.

Adger, W.N., 2000. Social and ecological resilience: are they related? Prog. Hum. Geogr. 24, 347–364. doi:10.1191/030913200701540465

Beckford, J., 2016. The intelligent organisation: realising the value of information. Routledge, Taylor & Group, Abingdon, Oxon ; New York, NY.

Beckford, J., 2013. Systems Engineering: Necessary but not sufficient for 21st Century Infrastructure. Beckford Consulting.

Beckford Consulting, 2009. An Overview of Systemic Interdependencies of the UK National Infrastructure. Available at: Beckford Consulting http://beckfordconsulting.com/wp-content/uploads/2008/10/Modernising-National-Infrastructure-Draft-2009.pdf.

Cabinet Office, 2016. Sector resilience plans - GOV.UK [WWW Document]. Sect. Resil. Plans. URL https://www.gov.uk/government/collections/sector-resilience-plans (accessed 6.23.17).

Cabinet Office, 2011. Keeping the Country Running: Natural Hazards and Infrastructure: A guide to improving the resilience of critical infrastructure and essential services. UK Cabinet Office, London.

Carhart, N., Rosenberg, G., 2016. Towards a Common Language of Infrastructure Interdependency. Int. J. Complex. Appl. Sci. Technol. 1, 35–60. doi:DOI: http://dx.doi.org/10.1504/IJCAST.2016.10002359

Carhart, N., Rosenberg, G., 2015. Towards a Common Language of Infrastructure Interdependency, in: Dolan, T., Collins, B. (Eds.), International Symposium for Next Generation Infrastructure Conference Proceedings, ISNGI. Presented at the ISNGI 2014, UCL STEaPP, London, p. 5. doi:10.14324/20141455020

Egan, M.J., 2007. Anticipating future vulnerability: Defining characteristics of increasingly critical infrastructure-like systems. J. Contingencies Crisis Manag. 15, 4–17. doi:10.1111/j.1468-5973.2007.00500.x

Elliott, C., Deasley, P., Royal Academy of Engineering (Great Britain), Working Party on Integrated System Design, 2007. Creating systems that work: principles of engineering systems for the 21st century. Royal Academy of Engineering, London.

Folke, C., 2006. Resilience: The emergence of a perspective for social–ecological systems analyses. Glob. Environ. Change 16, 253–267. doi:10.1016/j.gloenvcha.2006.04.002

Hamel, G., Valikangas, L., 2003. The quest for resilience. Harv. Bus. Rev. 81, 52–+.

HM Treasury, 2015. Valuing Infrastructure Spend: Supplementary guidance to the Green Book (OGL No. PU1798), The Green Book. HM Treasury, London.

Hogan, M., 2013. Anytown Final Report.pdf. London resilience, London.

Hollnagel, E., 2014. Resilience engineering and the built environment. Build. Res. Inf. 42, 221–228. doi:10.1080/09613218.2014.862607

Hollnagel, E. (Ed.), 2011. Resilience engineering in practice: a guidebook, Ashgate studies in resilience engineering. Ashgate, Farnham, Surrey, England ; Burlington, VT.

Hughes, T. P., 1987. The Evolution of Large Technological Systems, in: The Social Construction of Technological Systems: New Directions in the History and Sociology of Technology. MIT Press, Cambridge, Massachusetts, p. 1–82.

ICE, 2017. State of the Nation 2017: Digital Transformation. ICE, London.

La Porte, T.R., 1996. High reliability organizations: Unlikely, demanding and at risk. J. Contingencies Crisis Manag. 4, 60–71.

Laporte, T.R., Consolini, P.M., 1991. Working in practice but not in theory: Theoretical challenges of "high-reliability organizations." J. Public Adm. Res. Theory 1, 19–48.

Lay, E., Branlat, M., Woods, Z., 2015. A practitioner's experiences operationalizing Resilience Engineering. Reliab. Eng. Syst. Saf. 141, 63–73. doi:10.1016/j.ress.2015.03.015

Leveson, N.G., 2011. Applying systems thinking to analyze and learn from events. Saf. Sci. 49, 55–64. doi:10.1016/j.ssci.2009.12.021

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

McAslan, A., 2010. Community Resilience Understanding the Concept and its Application. Torrens Resilience Institute, Adelaide, Australia, http://torrensresilience.org/origins-of-the-term.

Meadows, D., n.d. Leverage Points: Places to Intervene in a System. Acad. Syst. Change.

Oughton, E., Tyler, P., 2013. Infrastructure as a Complex Adaptive System.

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

Rinaldi, S.M., Peerenboom, J.P., Kelly, T.K., 2001. Identifying, understanding, and analyzing critical infrastructure interdependencies. IEEE Control Syst. Mag. 21, 11–25. doi:10.1109/37.969131

Rosenberg, G., Carhart, N., 2014. Review of Potential Infrastructure Interdependencies in Support of Proposed Route HS2 Phase 2 Consultation. International Centre for Infrastructure Futures, London. doi:10.14324/20141455383

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.

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.

Sagan, S.D., 1995. The Limits of Safety: Organizations, Accidents, and Nuclear Weapons. Princeton University Press.

Shrivastava, S., Sonpar, K., Pazzaglia, F., 2009. Normal accident theory versus high reliability theory: A resolution and call for an open systems view of accidents. Hum. Relat. 62, 1357–1390. doi:10.1177/0018726709339117

van Stralen, D., 2017. HRO Models | High Reliability Organizations [WWW Document]. URL http://high-reliability.org/High-Reliability-Organizations (accessed 6.22.17).

Walker, B., Hollin, C.S., Carpenter, S.R., Kinzig, A., 2004. Resilience, adaptability and transformability in social-ecological systems. Ecol. Soc. 9, 5.

Weick, K.E., 2004. Normal accident theory as frame, link, and provocation. Organ. Environ. 17, 27–31. doi:10.1177/1086026603262031

Weick, K.E., 1987. Organizational Culture as a Source of High Reliability. Calif. Manage. Rev. 29, 112–127. doi:10.2307/41165243

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.

Weick, K.E., Sutcliffe, K.M., 2006. Mindfulness and the quality of organizational attention. Organ. Sci. 17, 514–524. doi:10.1287/orsc.1060.0196

IN PRESS

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

Dolan, T., Jude, S., Varga, L., Quinn, A. and Neil Carhart, N. (2016) Infrastructure Resilience: a multi-disciplinary perspective (advanced copy). In: Dolan, T and Collins, B, (eds.) ICIF White Paper Collection (in Press), UCL Press, London, UK. Available online at: www.icif.ac.uk