EngineeringX

Exploring the safety of super-sized structures

Royal Academy of Engineering

bre

UCL

Lloyd's Register Foundation

Report of a workshop held on 11 May 2020

Hosted by the Royal Academy of Engineering in partnership with Lloyd's Register Foundation, University College London and BRE (Building Research Establishment)

Professor Jeremy Watson CBE FREng

Royal Academy of Engineering
Prince Philip House
3 Carlton House Terrace
London SW1Y 5DG
Tel: 020 7766 0600
www.raeng.org.uk
@RAEngNews

ISBN 978-1-909327-51-1

Contents

0

Foreword

Foreword by Dr Jan Przydatek

Dr Jan Przydatek
Director of Technologies, Lloyd's Register Foundation, and Board member of the Engineering X Safer Complex Systems Mission

In June 2017, Lloyd's Register Foundation (LRF) published its insight report on global safety challenges, an engagement with the community to understand where the community believed there were significant safety challenges. At face value these challenges appear diverse, covering a range of sectors, one of which was the safety of super-sized structures.

In this safety of super-sized structures workshop, the five sectors represented have critical roles to play in our daily lives. When safety is compromised in these structures, the social, societal and economic consequences can be high and have impacts that extend far beyond the structure involved.

When the findings and recommendations of this report are considered in the context of deeper dives into the other challenges identified in the 2017 insight report, it is striking how seemingly different challenges have common themes. This provides the opportunity for well-targeted interventions to have far-reaching impact.

Among these common themes is reimagining regulation, governance and management of what are essentially complex systems; a need for increased diversity of collaborative thinking that brings together the multiple disciplines and broader stakeholders involved throughout the life of assets; and lifelong education that builds people's competency to greater levels, enabling better decisions to be made.

1

Preface

1 Preface

Dame Judith Hackitt DBE FREng
Chair of the Engineering X
Safer Complex Systems Mission

Most of my career has been concerned with safety in some way or another, ranging from working in major hazard industries as a graduate engineer, chairing the Health and Safety Executive, championing process safety at the Institution of Chemical Engineers to the Independent Review of Building Regulations and Fire Safety in 2017. Throughout, two things have become increasingly clear:

- **Engineered solutions are becoming increasingly complex – bigger, taller, more integrated than ever before.**
- **Different engineering disciplines have developed their own set of tools and techniques to manage engineering safety with much less sharing of knowledge and learning than one would expect of a profession that is inherently collaborative.**

When I was invited to chair the 11 May workshop on the 'Safety of super-sized structures' I readily accepted because it is a subject of great interest to me and also has strong links to the important work that the Royal Academy of Engineering (the Academy) and LRF are engaged in under the Engineering X brand, seeking to explore and improve the safety of complex systems. Despite the thematic approach used for group discussion, I was struck most of all by the similarity of views that emerged from all of those groups.

Now, more than ever we need to promote interdisciplinary collaboration to address the issues that are challenging us in this area – including competency, socio-technical challenges, learning lessons, and sharing good practice among others.

The workshop also began to explore the type of regulatory frameworks required for increasingly complex and large projects and structures. There is a strong consensus that outcomes-based regulation, which places responsibility with the owner and risk creators, is most effective but also a recognition that with complexity comes a significant challenge in identifying that single point of responsibility and accountability.

The whole debate was rich with ideas and created a good deal of food for thought and further work. This report is a record of that discussion and the potential workstreams that may flow from it. We need to keep this rich seam of work going; we need to address the challenges we have identified; and we welcome further input from more people as we seek to extend this debate more globally.

Professor Jeremy Watson CBE FREng
BRE Chief Scientist and Engineer

It was a privilege to be asked by LRF to arrange a process to collect and report on thoughts, opinions and evidence from experts with experience of engineering sectors that deal with super-sized structures. With colleagues from the Academy, BRE and University College London (UCL), we evolved a workshop design, the outcomes of which are reported here.

There is clearly a need to move to an outcomes-based regulatory system, as this gives control to experts, whereas rules-based regulation has the danger of allowing people without engineering insight to provide design authority. Society should require a duty of care on the part of commissioners of super-sized structures, to ensure adequate competencies and accountabilities exist across the supply and delivery chains.

2

Executive summary

2 Executive summary

The workshop, which was held online and hosted by the Academy partnered with LRF, UCL and BRE, was attended by 33 participants and chaired by Dame Judith Hackitt DBE FREng. A plenary opening session featured brief context-setting addresses from five theme leaders, and guidance from the chair. In particular, Dame Judith pointed out the need to think across engineering disciplines and to identify generic factors that could inform safety across sectors.

Deliverables from the workshop (including this report) are intended to inform thinking about research needs, policy recommendations and practice guidance.

The five theme groups identified generic issues and cross-disciplinary concerns. It was clear that common challenges spanned socio-technical[1], economic, educational, and engineering domains from viewpoints including safety, risks, economics, competency, regulation, and governance. A key point was the need for programme teams to know who is responsible for the safety of a whole system.

Managing aging structures was a common theme, while the groups discussing geotechnics[2] and offshore made similar observations concerning the difficulty of assessing asset condition, and balancing safety with necessary renovation investment. Some assets, such as Victorian rail tunnels and tidal energy systems, have a useful life of more than 150 years. The workshop asked how can we assess and future-proof these structures, as well as the new infrastructure we are building today?

A further key generic outcome was the recognition that a review looking at competence is required across the entire engineering community. This must cover in-discipline and cross/multidisciplinary capabilities, including socio-technical considerations, particularly as they relate to systems views of safety.

Generic and cross-cutting challenges covered areas including:

- competency
- engineering
- socio-technical and behavioural
- economic
- regulatory and governance.

These considerations applied to all five of the theme groupings in different proportions. Engineering challenges featured strongly in the high-occupancy buildings, geotechnical and bridge structures groups, with comments including: *"There is little engineering research on low chance, high consequence events."*

At a meta-level[3], the challenges themselves need to be looked at through combinational lenses as well. For example, competency clearly influences the quality of decision-making in the other four challenge areas. Similarly, without effective regulation and governance, an environment of safety and quality cannot be created and maintained.

Socio-technical and behavioural factors were highlighted in the industrial complexes and processes groups, with comments including: *"There are often misunderstandings in perceived responsibilities"*; *"Reporting of accidents, incidents and near-misses down supply chains is incomplete."* A further important observation was that *"for megastructures and systems of increasing complexity we don't have a choice but to use outcome-based frameworks."* An important question from the high-occupancy buildings theme group was: *"How do we ensure that the people who are tasked to ensure safety, have the appropriate competence (and professionalism with appreciation of ethics)?"*.

It was noted that safety issues can arise from a few common behavioural causes, including familiarity, lack of understanding of new technologies, and sheer complexity.

Economic influences were clear across all theme groups, with principles of ALARP (as low as reasonably practicable) being accepted in some sectors, but less so in others. In general, the need to properly understand the condition of structures so that pre-emptive measures could be applied before any failure was seen to be an important way to mitigate refurb/retrofit costs. Understanding the evolution of the condition of the structures – how they age – is therefore essential to address the economics of refurb/retrofit. Geotechnical and offshore group thinking brought environmental and societal cost/benefit into focus, as well as whole-life costs, such as decommissioning and waste disposal or re-use. The high-occupancy buildings group was concerned with *"the cost of compliance, the cost of systems (information, sensors, etc.) and of resource."*

The area of regulation and governance clearly has a central role to play in creating a societal environment for safe structures. Insights ranged from a *"national strategy and a plan is required (not a few random bits masquerading as a plan)"* to *"codes of practice and regulations are out of date, taking insufficient or no account of recent developments in materials/technology/understanding"*. Adversarial and blame cultures were mentioned, and *"the curse of procurement (lowest price) – part of the same downward spiral – cheapest price means less competent engineers means more reliance on recipe book codes means less innovation and poor design"*.

Key recommendations

- The engineering profession must address the varying levels of competence across sectors that work with super-sized structures. While more and more engineering programmes are becoming interdisciplinary, there is a need for greater sharing of knowledge and for research into new methodologies as systems and structures become more complex.

- Effective and immutable communication and sign-off[4] of safety-related information down supply and sub-contract chains must be mandated to enable effective management throughout the life cycle of complex structures.

- Outcomes-based regulation should be a focus of government policy, but this must be accompanied by new thinking to address complex ownership and operating models for structures and systems.

3

Introduction

3 Introduction

LRF is a registered charity. Its mission is, for the benefit of the community, to protect the safety of life and property, and to advance education, engineering-related research and public engagement.

LRF previously published an insight report on global safety challenges[5], which identified issues associated with the safety of super-sized structures. To better understand this challenge, including the identification of critical areas and knowledge gaps, and hence establish what practical steps can be taken to enhance the safety of these large structures and protect lives, a scoping workshop was held on 11 May 2020 that looked across various types of built environment infrastructure. Typical instances might be roads and railways[6], bridges, dams, tunnels, mega-buildings, ocean-going ships, and transport nodes. Many of these share contingent risks from, for example, external effects of extreme weather (such as flooding) and climate change, seismic disturbance, fire, terrorism, and inaccurate human perceptions of risks, as well as errors. Additional risks are associated with user ignorance and carelessness, insufficiency in competence[7], corporate policies and practices[8], inadequate mitigations, and so on. Discussion included public policy and corporate and personal behaviours[9] as well as technical matters. As well as sharing many risks, an important aspect that all super-sized structures have in common is the potential for extraordinary consequences in the event of failure[10]. With current trends including the quest for increased efficiency through the scale-up of projects, it is vitally important to look at the safety of super-sized structures, understand the overlaps and interdependencies of risk types, the factors that potentiate risk, and the responses and mitigations available through socio-technical interventions. Are safety considerations and interventions developing that track the scale-up of ever larger and more complex structures? While more sophisticated responses are becoming available through pervasive digital technologies that provide multidisciplinary design tools, clear lines of sight for accountability, operational monitoring and sophisticated analytics, it is not clear if progress in the safety sector is enabling its effective use in improving the safety of super-sized structures[11]. However, with the right channels of dissemination, it is anticipated that solutions from one sector may, by analogy, be helpful in others.

The 4S workshop brought together a group of experts to report on five theme groupings:

- **Industrial complexes and processes** (manufacturing and process industries)
- **Geotechnical structures** (dams, tunnels, bridges)
- **Engineered moving structures** (aircraft, ships)
- **Offshore structures** (oil platforms, wind farms)
- **High-occupancy buildings** (residential and commercial)

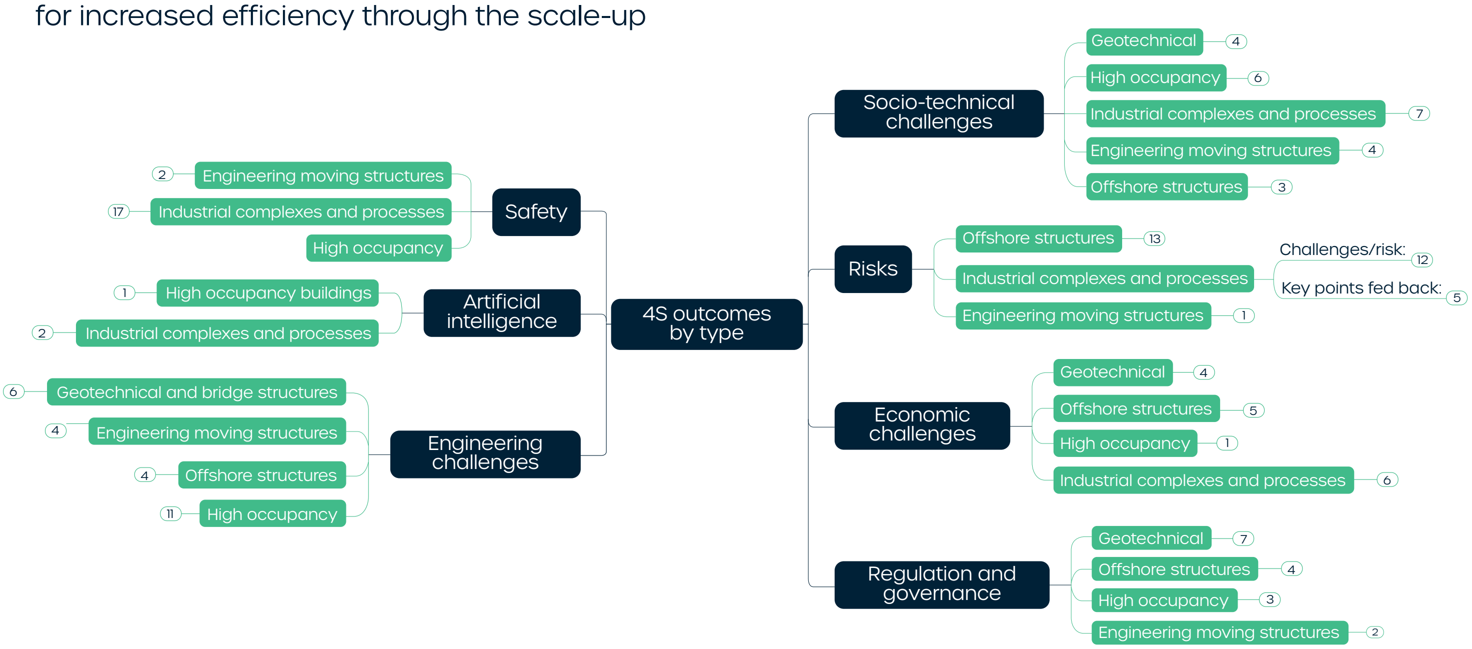

Figure 1: A mind map provides a useful structure to visualise the common and cross-cutting safety issues that span these themes.

4

Competencies

4 Competencies

Competency needs to be addressed under a specific heading because it was a common theme across all discussions and was highlighted as particularly important for super-sized structures.

There was debate about whether existing professional engineering registration (CEng) was adequate to address the needs of contemporary engineering and its frequent requirement to take a cross- and multidisciplinary viewpoint. This conversation extended to considering the ethical reasoning that engineers need to practice. *"Are engineering degree courses covering ethics in a relevant and practical way?"*[12]

"The Institution of Chemical Engineers has created a separate qualification called 'Professional Process Safety Engineer[13]' as it was felt that additional competencies were required beyond CEng. This was eight years ago but could it be something other PEIs[14] could introduce?"

Different organisational models exist for PEIs[15] around the world and it would be valuable to understand how this influences the effectiveness of skills development, knowledge sharing and collaboration.

When considering competency, we need to consider a number of factors: skills; training at professional and craft levels; knowledge gaps where research may be needed; and ethical considerations. Competency is critically important to super-sized structures and is more than just knowledge; it also encompasses a series of attributes that are strongly related to the nature of the professional activity.

Skills and competence gaps must be addressed to move from anecdotal examples to design frameworks that promote better and inherently safer system outcomes. There is an important tie in here to the work of the Engineering X Safer Complex Systems work[16].

The workshop noted that: *"construction and operation phases require different skillsets yet are inextricably linked."*

Without relevant skills and experience, the same tools and techniques used to design and create safety strategies for smaller structures may be inappropriately applied to super-sized and more complex projects, with no conscious sense of the risks introduced.

Competency is critically important to super-sized structures and is more than just knowledge; it also encompasses a series of attributes that are strongly related to the nature of the professional activity.

This underlines the fact that education is vital at all levels from further education to higher education and beyond. There is a real need to upskill and reskill, requiring up-to-date readiness of courses and institutions. *"Keep the importance of engineering at forefront; nurture a talent pipeline."*

Ensuring we have access to the right knowledge is vital – do we know where structures (for example offshore) are situated? A shared understanding of what already exists and a planning framework are needed.

There are also research questions, such as how to evacuate from super-sized structures – for example tall buildings and ships – and can we safely adapt and repurpose super-sized structures? Gaps exist in both the research and practice spaces. These may be gaps in translation, where relevant research has yielded insightful results, but these have not been adopted as engineering practice.

Commissioners of super-sized structures have an ethical duty of care to ensure that their designers, engineers and constructors have the necessary competencies and up-to-date skills to ensure safety that is adequate to the type, cross-disciplinarity and complexity of a project. This currently varies across sectors, where aerospace may be considered at one extreme and high-occupancy buildings at the other. One workshop attendee remarked: *"There is widespread incompetence and self-interest – particularly concerning residential buildings."*

There needs to be significant consequences for responsible professional individuals who do not support safety with diligence. *"There are Issues of liability and to what extent people can be held liable. To what extent can the professions take action?"*

Education is vital at all levels from further education to higher education and beyond. There is a real need to upskill and reskill, requiring up-to-date readiness of courses and institutions. *"Keep the importance of engineering at forefront; nurture a talent pipeline."*

Commissioners of super-sized structures have an ethical duty of care to ensure that their designers, engineers and constructors have the necessary competencies and up-to-date skills to ensure safety that is adequate to the type, cross-disciplinarity and complexity of a project.

5

Engineering challenges

5 Engineering challenges

Engineering challenges differ across types of super-sized structures, but common themes can be identified. All the challenges need to take account of decarbonisation, both from the point of view of embodied carbon (in the renovation process) and operational carbon impact in use.

The challenges identified in the workshop do not represent a complete set, but they do exemplify some key concerns. They ranged from incomplete knowledge of structural condition, through the challenge of complexity, the need to consider interdependencies and unintended consequences, resilience, flexibility and adaptability, to longevity and legacy.

For undocumented, aging structures of all kinds there is a significant challenge in understanding their structure and condition[17]. Standardised assessment protocols vary in quality, coverage and depth according to sector and type[18]. Assessment must take account of degradation processes, their rate (often a function of operating environment) and degree of visibility[19]. Most failures occur in structures not in use (probably because of a lack of condition knowledge). For structures in use, failures often occur because design limits are exceeded, or because 'design intent' is lost in later (cost) engineering[20] exercises[21].

Complexity can be the enemy of safety, and modern digital design techniques can lead to over-specification in terms of complexity, rather than addressing the purely 'necessary'. Digital tools can also hide design assumptions being made, and this opacity can hinder or mislead human oversight[22]. Complexity can yield systems that are 'brittle' – that lack resilience and fault-tolerance. Similarly, simulation can give false confidence in the safety of systems, when for example a real-world event falls outside the scope of the simulation, or when a rare and unanticipated combination of external stimuli occurs. The workshop concluded that simulation cannot replace testing but that there is a need to develop new methods to assess and manage complexity.

When conducting engineering design and analysis, it is vital to understand system boundaries. In other words, the parts of the structure whose operation or failure influences other parts[23]. For example, in high-occupancy buildings, issues of progressive collapse, fire spread, etc. result from the interactions between sub-systems of the building, whose safety needs to be considered as a whole.

The development of operational concepts is important, so that the safety and operation of a system can be maintained under both normal and partial failure conditions[24]. This must be applied at the start of a design, should reflect assumptions and be kept current throughout the design/build/use life cycle.

Complexity can be the enemy of safety, and modern digital design techniques can lead to over-specification in terms of complexity, rather than addressing the purely 'necessary'.

With clients involved throughout the design process rather than just at the beginning – a trend in current practice – the ability to adapt to changing requirements is important[25]. Maintaining clear visibility of safety implications through this process may be complicated but is vital.

Some super-sized assets like offshore structures and dams have very long life expectations. Comments included: *"we should be able to apply monitoring and assessment technologies to reduce costs while maintaining structural integrity"*, and *"how can we safely keep structures in operation longer?"* Concerning end of life, one discussion noted *"we need to think through from beginning to end. We have missed the opportunity with offshore structures, such as wind farms. Thinking of disposal, we are left with some of the same problems as 'old energy'"*.

If up-rated super-sized structures (such as wind turbines) are to replace and use the previous generation's infrastructure (for example foundations), overdesign for futureproofing (with consequent cost) may be inevitable. *"When undocumented infrastructure is inherited, how can fitness for purpose be assessed with safety in mind?"*.

Evacuation

A common engineering question with very large structures is how do you rapidly and safely get people out of them in an emergency? Current practice is weak and ad hoc in terms of how such systems work. Innovation and shared thinking are needed across various types of structure. Density of usage is another complicating factor, requiring innovation around changes of scale.

With clients involved throughout the design process rather than just at the beginning – a trend in current practice – the ability to adapt to changing requirements is important[25]. Maintaining clear visibility of safety implications through this process may be complicated but is vital.

Instrumentation and condition monitoring

The availability of affordable instrumentation and condition monitoring components and systems provides a route to risk mitigation in many super-sized structure applications. Immediate benefits can be realised in infrastructure and building monitoring, both in terms of detecting precursor conditions that might lead to the compromise of safety, and in preventative maintenance, with its benefits of reducing operating costs and improving asset availability. Emerging trends towards the development of 'Digital Twins' for engineered systems should lead to agile and cost-effective condition monitoring for performance and safety. However, comparison with a digital model may be inadvisable as a primary means of detecting unsafe conditions.

Types of safety issue and residual risks

Three clear categories of safety issues were identified in the workshop:

1. Those long-known, that may have been forgotten about, or where 'familiarity breeds contempt'.
2. Those introduced through the adoption of new technologies, where inadequate education or experience exists.
3. Those too complex for any one individual to understand.

Environmental conditions are changing with climate and human development, so long-lived structures must be future-proofed against emerging conditions, which may be far beyond the original design factors. Monitoring and analysis can provide a measure of the remaining safety margins.

Monitoring and managing residual risk is important, but leading indicators[26] and similar are needed. It is increasingly easy to be overwhelmed with data, and a key skill is to convert this into reliable and useable information. In the future, artificial intelligence and machine learning are likely to play a role in this, reducing human cognitive burdens. It is vital to understand residual risk when design and engineering assessment is complete, as is the need to monitor and manage residual risk throughout an asset's life cycle, balanced by understanding it in the context of use.

Environmental conditions are changing with climate and human development, so long-lived structures must be future-proofed against emerging conditions, which may be far beyond the original design factors. Monitoring and analysis can provide a measure of the remaining safety margins.

6

Socio-technical challenges

6 Socio-technical challenges

Behaviour combined with technology presents generic challenges that vary in degree across sectoral applications, *"understanding how people will actually use/interact with the infrastructure is important (infrastructure itself can be an agent for behaviour change)"*.

It is important to take stakeholder and user perceptions into account. *"It is all the more important to learn from people using the facilities, and feed that learning into processes."*

For safe design and operation, it is important to understand how people will interact with a structure (for example a high-occupancy building) and use it, noting that modes of use (and renovation) may compromise the safety of what has been delivered. This must be understood to ensure that safety is maintained over the (long) life of the asset. The comment was made *"this is not looked at in a holistic way. How do alterations or works done for maintenance alter the performance of the building eg to fire?"*.

Several pivotal considerations apply when considering corporate and personal behaviours. The workshop discussions included incentivisation, factors affecting accident reporting and information sharing.

The practicalities of safety versus profit must be considered. This suggests that incentives may be needed. *"There is a tendency to retreat into prescriptive regulations, which is not the way to go, and doesn't provide incentives."* Negative perceptions of safety measures were noted in the workshop: *"the idea that safety results in downtime and therefore slowing down and reducing organisational profitability for shareholders and investors."*

A 'no blame' culture is vital in corporate practice to encourage accident and 'near miss' reporting. A workshop attendee also noted: *"accidents incubate – they are rarely sudden and unexpected to everyone."*

There is a need for shared and open data in the management of existing structures. How can communities of users be built on- or off-site? Candidate information sources include Earth observation and remote sensing technologies. *"These structures are for the public; how do we make the public more aware of them."* London 2012 was seen as a successful project. *"One of the key enablers was that 'several eyes were looking at and reviewing projects'. This is not the case in residential building projects."*

Systems integration

Problems can arise when design and engineering tasks are divided and allocated to different organisations. This has been the norm for civil engineering programmes. The culture of design, engineer, cost reduction, construct, and snag creates a one-dimensional chain of activity (horizontal), while the practice of prime, subcontract and sub-sub-contracting creates stratification in the vertical[27]. Clear lines of sight for design intent, particularly as they relate to safety, are essential, but documentation transfers and sign-offs remain in many cases, obscure and unreliable[28]. *"Understanding the importance of system boundaries is important to any safety assessment, as those boundaries affect both the initial design and change management."*

Standards and codes of construction

A challenge results from the rapidly growing demand for, and hence construction of, high-occupancy buildings in developing (and developed) countries where there is either a lack of local building codes, or where there is adoption, appropriate or otherwise, of codes from elsewhere. A general lack of regulation leads to lax and potentially unsafe practices. Corporate behavioural issues therefore need to be addressed, the workshop revealed a view that *"data on real-time performance of a building should be shared with others (for example in nearby buildings). The idea that this data and so on is proprietary is inappropriate, when they affect nearby areas. This is especially important in an urban environment"*.

A 'no blame' culture is vital in corporate practice to encourage accident and 'near miss' reporting. A workshop attendee also noted: *"accidents incubate – they are rarely sudden and unexpected to everyone."*

Perception of risk

High-consequence, low-probability hazards pose both social and physical science challenges. The understanding of, and response to, such risk is difficult, particularly where large investments may be needed to reduce or mitigate it[29]. The statistics and science of this type of risk are also hard; there may be very little experimental evidence to model or predict likelihoods[30].

Tensioned against the view of inadequate risk understanding was opinion concerning risk aversion: *"we have become very risk averse (contractual interfaces, professional indemnity, blame culture: Category 3 checks are often a stumbling block to innovation)."*

Managing and adapting to change

Many super-sized structures are subject to change and adaptation. Industrial manufacturing processes are a good example of this. Safety cases, FMEAs[31] and so on must therefore be dynamic, which gives rise to questions of change control, document maintenance, and notification of affected users. *"Continuous improvements and continuous changes to the environment, for example business, logistics and economics, change the safety context too."*

Incremental changes typical of industrial applications can give rise to safety analyses not tracking the functional or structural changes to a plant[32]: *"processes get incrementally changed until one final change leads to a system that is not fully understood, and the safety of the system is compromised"*.

Chemical engineering may be ahead of other disciplines regarding methodologies for assessing and managing safety risk in complex systems/processes. How can learning from all domains be pooled, adapted and shared throughout all disciplines?

Change control is a common requirement in all design processes. Historically, manual drawing controls came before automation was possible through computer-aided design. Now, more sophisticated processes are required for dealing with software changes, with better adoption of best practices for dealing with them. *"Not sure there are really good practices. There is an assumption that following good practices (standards) will give low and well-defined failure rates; this is not true. The best we can do with software for modern systems with hundreds of thousands or even millions of lines of code is to reduce the probability of failure – not eliminate it. Maybe a better approach is looking at assumptions and uncertainties and monitoring against the assumptions that cannot be validated prior to operation."*

Incremental changes typical of industrial applications can give rise to safety analyses not tracking the functional or structural changes to a plant[32]: *"processes get incrementally changed until one final change leads to a system that is not fully understood, and the safety of the system is compromised".*

Chemical engineering may be ahead of other disciplines regarding methodologies for assessing and managing safety risk in complex systems/processes. How can learning from all domains be pooled, adapted and shared throughout all disciplines?

7

Economic challenges

7 Economic challenges

Across all sectors and applications, it was recognised that economic pressures have required operators to cut costs and try to get as much lifetime and use as possible, out of assets they already possess. For geotechnical and other structures, this has often led to use beyond the end of design life, and to the deferral of renovation, requiring 'down rating' in some cases. There are tensions to be dealt with between affordability, service availability, customer experience and safety. *"Finance needs to be available when needed, for example for preventative rather than reactive maintenance, when the need is identified – and we need compelling business cases for that."*

Several considerations were discussed in the workshop and its syndicates, among these; understanding whole-life costs; the economic impacts of decommissioning; non-monetised benefits; and issues around how cost-driven decision-making influences business cases.

Although architects and designers often claim that they understand whole-life costs, workshop attendees felt this was not always the case, and that 'as designed' was rarely found to match 'in use' performance. There is a role for methods to assure performance, to be applied in many cases.

Whole-life cost estimation needs to anticipate renovation and changes in use that require retrofit. Principles behind the 'Circular Economy'[33] may provide tools for thinking about whole-life costing.

Whole-life costing must include decommissioning, and the associated expense can be high, such as for nuclear power stations and offshore structures. Special safety considerations usually apply in decommissioning. *"Must factor in cost of decommissioning and disposal." "End of life has often not been wrapped into project cost. There are safety consequences, and poor economic models."*

Whole-life costing must include decommissioning, and the associated expense can be high, such as for nuclear power stations and offshore structures. Special safety considerations usually apply in decommissioning.

When considering super-sized structures, some benefits and costs may not be directly financial, although their indirect effects are often monetisable. Carbon emission is an example; construction is a major contributor to CO2 release with concrete manufacture being a significant part of this[34]. Carbon cost budgets are split into embodied (that created in construction) and operational. For buildings, the latter may be many times the embodied carbon over the lifetime of the asset. This contrasts with, for example rail tracks, where the converse may be true. *"We need to take account of environmental and societal benefits in cost/benefit analysis."*

The non-monetised value of assets can be made visible if a systems view is taken in business case development. This may require the external boundary of the systems value analysis to extend beyond that of the developer into the lessee domain or into the local or national community. Health, wellbeing and productivity are examples of benefits that are not directly financial. Obviously, productivity is itself of financial value to a lessee, and health and wellbeing directly save cost to the NHS.

Cost engineering is a typical step in the design/engineering/construction workflow for super-sized structures. It is frequently applied after architecture/design and first-pass engineering steps. This often carries the risk of a loss of original design intent concerning both safety and functional features. *"There is a curse of procurement (lowest price). This contributes to a downward spiral – cheapest price means less competent engineers means more reliance on recipe book codes means less innovation and poor design."* The availability of a clear line of sight down the workflow chain, with immutable safety signoffs, must reduce the risk of losing design intent.

Making a business case for safety was seen (by the industrial complexes and processes group) to have similar difficulties to planning for investment in resilience: *"very hard case to make for continued investment/budget, as money only seems to flow when there has been a failure."* Moreover, a view was expressed that managing safety results in asset downtime, thereby reducing productivity and profitability. *"Finance needs to be available when needed (for example for preventive rather than reactive maintenance, when the need is identified)'."* This view suggests that a regulatory framework that takes a systems view and is supported by standards and competency frameworks is necessary to ensure appropriate corporate behaviours.

The non-monetised value of assets can be made visible if a systems view is taken in business case development. This may require the external boundary of the systems value analysis to extend beyond that of the developer into the lessee domain or into the local or national community.

A regulatory framework that takes a systems view and is supported by standards and competency frameworks is necessary to ensure appropriate corporate behaviours.

8

Regulation and governance

8 Regulation and governance

There is clearly a role for government regulation, standards and governance in promoting the safety of super-sized structures. These necessarily apply differently across sectoral applications, but there are cross-cutting elements that can inform a culture of better practice. A voiced view was that *"there is a need to move to an outcome-based regulatory system rather than a rules-based system"*, and *"outcome-based regulation gives control to experts, whereas rules-based regulation can allow people who only know those rules to consult"*. The link to competency was also noted in the workshop: *"need to have regulatory frameworks complemented with competency frameworks to enable them."*

Systems thinking was also recommended for regulation and governance: *"working out regulation in silos won't solve this, we need a systematic approach."*

Compliance, reporting and international frameworks

Historically, compliance with building codes and regulations has been poorly policed in the UK[35]. Some regulations and codes of practice are considered out of date. Electronic technologies, including for example blockchain[36], can be expected to make compliance transparent and much easier to audit, together with providing immutability, and clear lines of sight down the design, engineering, construction, operation, and maintenance timeline. *"There need to be significant consequences for individuals who neglect safety. There are issues of liability – to what extent can people be held liable? To what extent can the professions take action?"*

The professional engineer (or more generally, a competent person) is often a missing figure in checking the implementation phase of projects. *"Where are the engineers in the building control departments of local councils/authorities? Clearly, there are major implications for safety. It comes down to thinking that engineers do not have specialist and valued skills. It costs less to employ non-engineers to conduct the inspections …"*

Confidential reporting of structural safety (CROSS) is not disseminated to the level it should be. *"In the aviation industry near misses are openly reported and shared, and sanctions can be applied. One problem is that CROSS has no 'teeth' associated with it and cannot sanction actors."*

Regulation needs to be applied in a manner similar to space or Antarctic exploration, with international frameworks or conventions that set out principles of shared development. *"More international cooperation is needed, using engineering as well as human rights and environmental principles. Currently there is a gap in governance."*

"There need to be significant consequences for individuals who neglect safety. There are issues of liability – to what extent can people be held liable? To what extent can the professions take action?"

Regulation needs to be applied in a manner similar to space or Antarctic exploration, with international frameworks or conventions that set out principles of shared development.

9

Research questions

9 Research questions

Many of the challenges associated with understanding and improving the safety of super-sized structures are concerned with practices, competencies and transferring 'what works' between sectors.

However, some key questions remain that create an agenda for research:

- What socio-technical understanding and developments are necessary to move to an outcomes-based regulatory system?
- How can low occurrence, high safety consequence 'Black Swan' events, be better modelled, predicted and mitigated?
- How can aging materials and their changing functional properties be characterised?
- How can probabilistic approaches inform an understanding of imperfections across behavioural and physical domains?
- How can artificial intelligence (AI) and machine learning be used to augment pervasive sensing to yield early detection of hazard precursor conditions?
- Can AI be used to provide automated design assistance to ensure safety matters are not overlooked?
- What leading indicators can be identified for managing and reducing residual risk?
- What are the key current and emerging socio-technical knowledge gaps?

10

Safety-promoting enablers

10 Safety-promoting enablers

Role of digital technologies

As in many sectors, digital technologies play a central role in all stages of the design, engineering, construction, and use of super-sized structures.

Many of these provide opportunities to improve safety, including:

- computer-aided design (CAD)
- modelling and simulation at all levels
- building information modelling (BIM) – the management of design and construction information down supply and delivery chains
- four-dimensional modelling and Digital Built Britain (merging real-time and static CAD information)
- smart facilities management dashboards
- Blockchain[37] – providing immutability of documents and signoffs
- monitoring via wired and Internet of Things (IoT) sensors
- safety, condition feedback and notification via user and occupant smartphone apps
- analytics, locally and cloud based.

Digital enablers are diverse and rapidly evolving. They include pervasive sensing of structures, which enables condition monitoring and preventative maintenance. These will increasingly use local and cloud-based analytics to infer asset condition.

IoT devices have made sensing and instrumentation of physical structures practical and affordable. IoT devices typically embody sensors in combination with computing and communications. They link in sub-networks to local or wide-area networks that route information to analytical systems, typically with a minimum of (or no) external wiring.

As device and installation costs become negligible compared with the capital cost of an asset, the benefits of installing large numbers of sensors can be realised. This can allow ‘spatial oversampling’, which gives system resilience and can improve confidence in readings.

Once a suitable number of relevant types of sensors are in place (for example strain gauges, thermocouples and humidity sensors) on an asset (super-sized or not), and they are connected to an analytical system (such as the cloud), it is possible to monitor function and safety at a system level. Moreover, conditions that are precursors to failure or unsafe states can be detected through the fusion of early warning signals before a real hazard materialises.

AI has a role in learning normal sensor signal patterns, so that anomalies that may be indicative of unsafe states can be detected. Hazard mitigation itself may become a real-time automatic response from AI, in addition to notifying a human supervisor (an example is automatic braking in autonomous vehicles). Lloyd’s Register Foundation-funded work is currently under way at the Alan Turing Institute (ATI) on the role of AI in safety.

Digital enablers are diverse and rapidly evolving. They include pervasive sensing of structures, which enables condition monitoring and preventative maintenance. These will increasingly use local and cloud-based analytics to infer asset condition.

AI has a role in learning normal sensor signal patterns, so that anomalies that may be indicative of unsafe states can be detected. Hazard mitigation itself may become a real-time automatic response from AI, in addition to notifying a human supervisor (an example is automatic braking in autonomous vehicles).

Tools and training

Traditional methods of safety and fault-consequence analysis include FMEA and Fault Tree Analysis. In super-sized structures, systems approaches are needed to augment these methods. Analysis boundaries must be carefully examined to ensure that the safety sensitivity of the structure and its sub-systems to external and internal events is below an acceptable level. Conversely, potential modes of failure of the structure must be shown not to cascade into its supporting infrastructure.

The effective use of safety and fault-consequence tools requires professional training that develops technical and behavioural insights coupled with ethical mindedness. As tools and structures evolve with time, professional training must be refreshed through CPD[38]. The need for proven competence cannot be overemphasised, and registration with a professional body associated with the relevant domain of engineering should be mandatory for signatories of safety cases.

Outcomes-based regulation requires a level of competence beyond that needed for rules-based compliance. Developed training programmes as part of engineering degree courses are indicated to promote this competence.

Policy

Government policy and public sector procurement have powerful roles to play in promoting the safe design and operation of super-sized structures. Several options exist for promoting desired outcomes. Non-mandatory standards developed through industry and stakeholder consultation can be adopted and, if necessary, adapted as technologies and markets evolve. Standards are based on widespread agreement among a broad cross section of relevant actors including industrial supply chains, PEIs and RTOs[39]. Process and product standards can address barriers to the market and, where needed, prevent the dominance of technologies and products that cause environmental or societal harm. They can also promote supply chain collaboration. Furthermore, government can set procurement rules for public sector projects that require compliance with relevant standards, to promote desired behaviours and outcomes. When the practicalities of adoption have been established, a third option is to enforce through regulation, either against standards or performance-based design outcomes.

The effective use of safety and fault-consequence tools requires professional training that develops technical and behavioural insights coupled with ethical mindedness.

Outcomes-based regulation requires a level of competence beyond that needed for rules-based compliance. Developed training programmes as part of engineering degree courses are indicated to promote this competence.

11

Generic factors

11 Generic Factors

Workshop discussions in the plenary and syndicate sessions highlighted certain generic factors, common to safety engineering across all sectors. It was widely agreed that 'systems thinking', which properly considers the design and influence perimeters of super-sized structures and includes consideration of interdependencies and unintended consequences of failure, was a fundamental requirement.

Understanding the boundaries (spatial, temporal, and behavioural/social) of the system is vital to maximise safety. Complexity is a further factor that can make safety engineering difficult for super-sized structures. Considering large structures in construction and use using the three 'lenses' of temporal extent, spatial extent and complexity may be useful in reasoning about risks and safety.

As a consequence of systems thinking in engineering, interdependencies between parts of the system under consideration, as well as those more loosely associated with it, can be revealed and understood. Some interdependencies may be synergistic, but others can reduce safety and introduce the possibility of cascade failures in associated systems.

Balancing 'Net Zero' with cost and safety

New paradigms and methodologies will be required to 'square the circle' in balancing affordability with green credentials while ensuring that safety is not compromised.

Poorly engineered systems, or those that began with a sound design but were compromised by cost engineering that did not take account of the original design intent, can lead to unintended consequences ranging from non-critical performance shortfalls to life-threatening scenarios. An example given in the workshop was dynamic clash between trains and bridges – as tolerances become tighter, train kinematic envelopes can intersect with structure boundaries. Good systems thinking at all phases of project development should be used to monitor for unintended consequences.

Other points of discussion included the need to refocus on education and training for safety engineering, and the importance of tracking emerging technologies and their possibly unanticipated technical and social consequences.

Delegates felt that formal teaching at technical and university levels was currently weak in safety engineering. A requirement for formal training in this might be made a determining factor in engineering registration.

Safety contexts are dynamic. They are changing as a result of the environment, technological development, business conditions, economics, and evolving supply chains.

Safety contexts are dynamic. They are changing as a result of the environment, technological development, business conditions, economics, and evolving supply chains.

12

Use-case examples

12 Use-case examples

Ageing structures

In February 1974 the collapse of a school roof beam at the John Cass School, Stepney[40], gave rise to concern over the use of high alumina cement (HAC). This near-tragedy sparked off the current industry position on the material. HAC differs from Portland cement, being composed of calcium aluminates rather than calcium silicates. Its rapid strength development made it popular from 1950 to 1970. However, mineralogical 'conversion' processes can, under appropriate environmental conditions, cause reductions in concrete strength and increased vulnerability to chemical attack.

HAC concrete was essentially banned for use as new structural concrete in the UK following well publicised collapses in the 1970s. However, further analysis may indicate that the primary causes of these collapses were poor construction details or chemical attack. Most HAC concrete in the UK went into precast beams, and perhaps 50,000 buildings with such beams remain successfully in service in the UK.

Loss of design intent

The Piper-Alpha rig was a large fixed platform in the North Sea. An explosion and resulting oil and gas fires destroyed Piper Alpha on 6 July 1988, killing 167 people[41].

During the late 1970s, works were carried out to enable the platform to meet gas export requirements. After completion, Piper Alpha operated in 'phase 2 mode', with a Gas Conservation Module (GCM). From the end of 1980 until July 1988 this was its operating state. Significant construction, maintenance and upgrade works were planned for the late 1980s and by July 1988, the rig was undergoing major reconstruction, including the change-out of the GCM unit. Hence the rig was returned to its initial phase 1 mode (operating without a GCM unit). Despite a complex work schedule, operators decided to continue operating the platform in phase 1 mode throughout this period and not shut it down as had been originally planned. Planning and controls that were put in place were thought to be adequate. Piper continued to export oil at just under 120,000 barrels per day and to export Tartan gas at some 33 million cubic feet (930 thousand cubic metres) per day at standard conditions during this period until the catastrophic events of 6 July 1988.

Misuse

The Chernobyl nuclear accident occurred on 26 April 1986, at Chernobyl (Ukraine) Nuclear Power Plant, No. 4 reactor. The worst nuclear disaster in history, it was caused by a flawed reactor design that was operated with inadequately trained personnel. Within three months of the disaster, the accident killed 30 operators and firefighters[42].

On 25 April 1986, prior to a routine shutdown, the reactor crew at Chernobyl 4 prepared for a test to determine how long turbines would spin and supply power to the main circulating pumps following a loss of electrical power. A similar test had been carried out at Chernobyl the previous year, but the power from the turbines fell too rapidly, so new voltage regulator designs were to be tested.

A series of operator actions, including disabling automatic shutdown mechanisms, preceded the attempted test early on 26 April. By the time a dangerous state was perceived, and the operator moved to shut down the reactor, it was in an extremely unstable condition. A design flaw in the control rods resulted in a huge power surge as the rods were inserted into the reactor. This led to a steam explosion, the disassembly of the reactor, and the ejection of more than 1,200 tonnes of highly radioactive material. The explosion and fires released at least 5% of the radioactive reactor core into the environment.

13

Concluding remarks

13 Concluding remarks

Many of the safety challenges posed by the design, engineering, construction, maintenance, and use of super-sized structures are common to structures of more conventional scale. However, extremes of physical size combined with extended lifetimes (during which maintenance and refurbishment are inevitable) coupled with sheer complexity, put safety engineering challenges on a different level.

New practices and tools are needed to address this three-dimensional picture. As the responsible team is likely to be distributed across knowledge and supply chains that will change over time, clear immutable and enduring evidence is required of design intent, as well as engineering information relating to the current asset condition coupled with its design evolution post-commissioning and snagging, through maintenance and renovation.

It is notable how much of the thinking that emerged in this workshop overlaps with that of the Engineering X programme – and maps onto all four of its workstreams:

- Safer Complex Systems
- Safer End of Engineered Life
- Engineering Skills Where They Are Most Needed
- Transforming Systems Through Partnership

It is therefore recommended that following further review and discussion of the specifics identified in this report that any follow-on work should be merged into that of the Engineering X programme. Super-sized structures are the ideal example where an outcomes-based regulatory system is necessary. These are extended-life, complex systems of critical societal importance where the analysis of safety needs to be extremely precise and detailed. Failure of super-sized structures will lead to major consequences in the short term (life loss and damage), but also in the long term (time for recovery and resilience). These are not only physical consequences but also economic, societal and political. Thus, all these variables need to be considered when addressing safety. Not only is there no prescriptive solution for the design, implementation and management of these structures, but their complexity demands that the analysis of safety be done with extreme rigour and by individuals with demonstrated competencies and up-to-date skills. Furthermore, this analysis will evolve over time during the long period in which many structural reconfigurations, changes of use, and implementations of new technologies are possible. The required skills are therefore trans-disciplinary and must embrace an understanding of present and new technologies as well as the economic and socio-political context. To enable an outcomes-based analysis of safety it is necessary to have an adequate regulatory structure as well as competent professionals. The skills of these professionals are unique; thus, a new pedagogy needs to be developed as well as the correct certification process. The regulatory structure, the professional skills, the training programmes to attain them, and the nature of the certification process that will enable an outcomes-based approach for super-sized structures are necessary and currently do not exist. Research is necessary to define the path towards achieving this outcomes-based approach.

14

Annex A – Recommendations

14 Annex A – Recommendations

1. Research is needed into understanding low occurrence, high consequence events that impose risks on engineered structures, particularly high-occupancy buildings and geotechnical and bridge constructions.
2. The Engineering Council and PEIs must consider the competencies required of registrants for CEng. Competencies need to be fit for contemporary purpose, including the practical considerations around cross-disciplinary working, and a sound appreciation of ethics in engineering practice.
3. A mind map provides useful structure to visualise possible recommendations.

15

Annex B – Participant list

15 Annex B – Participant list

Participant list

Dame Judith Hackitt DBE FREng (Chair)
Professor Jeremy Watson CBE FREng, BRE and UCL
Professor José Torero Cullen, UCL
Professor Bridget Eickhoff FREng, Rail Safety and Standards Board
Professor Kelvin Higgins FREng, Geotechnical Consulting Group LLP
Professor Lord Robert Mair CBE FREng FRS, University of Cambridge
Tim Chapman FREng, Arup
Lila Tachtsi FREng, Highways England
Professor Dracos Vassalos FREng, University of Strathclyde
Professor Jeom-Kee Paik FREng, Pusan National University and UCL
Professor Chris Binnie FREng, Independent Consultant
Professor John McDermid OBE FREng, University of York
Emeritus Professor David Blockley FREng, University of Bristol
Professor Mark Girolami FRSE, University of Cambridge
Professor Rod Muttram FREng, Independent Consultant
Dr Carolyn Griffiths FREng, UK Rail Accident Investigation Branch
Professor Luke Bisby, University of Edinburgh
Professor Grunde Jomaas, University of Edinburgh
Professor Tiziana Rossetto, UCL
Professor William Powrie FREng, University of Southampton
Professor Joanna Chataway, UCL
Professor Nick Buenfeld FREng, Imperial College London
Professor Andrew Curran, Health and Safety Executive
Dr Debbie Smith OBE, BRE Global
Dr Deborah Pullen MBE, BRE Trust
Professor Liz Varga, UCL
Sir Geoff Mulgan CBE, UCL
Vara Suntharalingam, HS2
Dr Jan Przydatek, Lloyd's Register Foundation
Gbenga Olugbodi, Lloyd's Register
Georgia Bateman, PhD student
Alastair Shipman, PhD student
He-in Cheong, PhD student
Iulia Manole, PhD student

Royal Academy of Engineering staff

Dr Shabana Haque OBE
Shelley Stromdale
Dr Philippa Westbury

UCL/BRE

Sue Green

References

[1] Areas where social and behavioural factors and technical systems must be considered together

[2] The science and engineering of soil and rock mechanics

[3] A level of description that more abstractly describes lower-level specific elements

[4] Lines of authorisation that are clear, traceable and auditable

[5] Lloyd's Register Foundation, Insight report on global safety challenges, Challenges facing the safety community, Copyright ©Lloyd's Register Foundation and Nesta, 2017.

[6] Chen, W., 2007. Analysis of Rail Transit Project Selection Bias with an Incentive Approach. Planning Theory, 6(1), pp.69-94.

[7] Barry, Brock E., and Joseph R. Herkert. 2014. "Engineering Ethics." In Cambridge Handbook of Engineering Education Research, edited by Aditya Johri and Barbara M. Olds, 673–692. New York, NY, USA: Cambridge University Press.

[8] Bero, Bridget, and Alana Kuhlman. 2011. "Teaching Ethics to Engineers: Ethical Decision Making Parallels the Engineering Design Process." Science & Engineering Ethics 17 (3):597–605.

[9] Lester, D. and Torero, J.L., Using megaproject performance outcomes to enhance decision-making behaviours in civil engineering graduates, Construction Economics and Building, 19, 1, 2019.

[10] Flyvbjerg, B., 2009. Survival of the Unfittest: Why the Worst Infrastructure Gets Built – And What We Can Do About It. Oxford Review of Economic Policy, 25(3), pp.344-67.

[11] Flyvbjerg, B., 2014. What You Should Know About Megaprojects and Why: An Overview. Project Management Journal, 45(2), pp.6-19.

[12] Barry, Brock E., and Joseph R. Herkert. 2014. Engineering Ethics. In Cambridge Handbook of Engineering Education Research, edited by Aditya Johri and Barbara M. Olds, 673–692. New York, NY, USA: Cambridge University Press.

[13] www.icheme.org/membership/professional-registrations/ppse/

[14] Professional engineering institutions

[15] G. L. Downey, J. Lucena and C. Mitcham, Engineering Ethics and Engineering Identities: Crossing National Borders, Chapter 5, in Springer International Publishing Switzerland, 2015, S.H. Christensen et al. (eds.), Engineering Identities, Epistemologies and Values, Philosophy of Engineering and Technology, 21, 2015.

[16] www.raeng.org.uk/global/international-partnerships/engineering-x/safer-complex-systems

[17] Corotis, R.B. (2009). Societal issues in adopting life-cycle concepts within the political system. Structure and Infrastructure Engineering, 5, 59–65.

[18] Bruce R. Ellingwood & Ji Yun Lee (2016) Life cycle performance goals for civil infrastructure: intergenerational risk-informed decisions, Structure and Infrastructure Engineering, 12:7, 822-829.

[19] Biondini, F., Bontempi, F., Frangopol, D.M., & Malerba, P. (2006). Probabilistic service life assessment and maintenance planning of concrete structures. Journal of Structural Engineering, 132, 810–825.

[20] Cost Engineering is a review exercise undertaken on an original design in order to remove apparently unnecessary cost. The original purpose of (eg safety) features may be lost in this process.

[21] The Future of National Infrastructure: A System-of-Systems Approach, edited by Jim W. Hall, Martino Tran, Adrian J. Hickford, Robert J. Nicholls, 2016.

[22] F. Sasangohar and M.L. Cummings, Human-System Interface Complexity and Opacity, HAL2010-03, MIT Department of Aeronautics and Astronautics, Cambridge, MA 02139, December 2010.

[23] S. M. Rinaldi, J. P. Peerenboom and T. K. Kelly, "Identifying, understanding, and analyzing critical infrastructure interdependencies," in IEEE Control Systems Magazine, vol. 21, no. 6, pp. 11-25, Dec. 2001.

[24] L Benner, Accident investigations: multilinear event sequencing methods, Journal of Safety Research, 7 (2) (1975), pp. 67-73

[25] B. Flyvbjerg, A. Ansar, A. Budzier, S. Buhl, C. Cantarelli, M. Garbuio, C. Glenting, M. S. Holm, D. Lovallo, D. Lunn, E. Molin, A. Rønnest, A. Stewart, B. van Wee, 2018, Journal of Transportation Research Part A: Policy and Practice.

[26] Projections into the future of expected safety margins

[27] This relates to viewing activity phases and the operational hierarchy as rows and columns in a grid

[28] Dame Judith Hackitt: Building a Safer Future; Interim report December 2017, Final, May 2018

[29] Thinking Fast and Slow: Kahneman D (2011) Penguin ISBN 978-0-141-03357-0

[30] Black Swan events: https://en.wikipedia.org/wiki/Black_swan_theory

[31] FMEA – Failure Mode Effects Analysis

[32] Piper Alpha disaster – see use-case example section

[33] https://www.ellenmacarthurfoundation.org/

[34] www.carbonbrief.org/qa-why-cement-emissions-matter-for-climate-change

[35] Comments in the DCLG Building Regulations Advisory Committee (BRAC) 2011

[36] https://blockgeeks.com/guides/what-is-blockchain-technology/

[37] Distributed ledger technologies

[38] Continuing professional development

[39] Research and technology organisations

[40] S.C.C. Bate, Report on the failure of roof beams at Sir John Cass's Foundation and Red Coat Church of England Secondary School, Stepney, 1974

[41] L.W.D. Cullen, The public inquiry into the Piper Alpha disaster, 1993.

[42] Salge M., Milling, P.M., Who is to blame, the operator or the designer? Two stages of human failure in the Chernobyl accident, System Dynamics Review Vol. 22, No. 2, (Summer 2006): 89–112, 2006.

Open Source