Engineering X

Safer Complex Systems workshop 2020

Royal Academy of Engineering

Lloyd's Register Foundation

Safer Complex Systems workshop 2020

This is a report of a workshop held on 25 September 2020 where a diverse group of engineers and non-engineers from around the world came together to discuss safety in complex systems. This report contains the themes that came up during the discussions and we welcome your views and feedback on this workshop summary. Please note this report is not a Royal Academy of Engineering policy document.

Professor Roger Kemp MBE 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 978-1-909327-53-5

Contents

1

Executive summary

1 Executive summary

The workshop, held on 25 September 2020, was part of the Engineering X Safer Complex Systems mission. It brought together (virtually) 131 participants from 20 different countries across six continents. In early sessions, two recent reports produced by the mission were discussed: *Safer Complex Systems* – an Initial Framework, written by a team from the University of York and completed in September 2020; and *Exploring the Safety of Super-sized Structures*, which summarised the conclusions of a specialist workshop held in May 2020. Later sessions discussed challenges in managing the safety of complex systems – particularly those that evolve unplanned as 'systems of systems' with no overall management structure.

Participants considered that the University of York report was a very useful way of analysing complex systems. However, it has been evaluated on only a limited subset of complex systems. There was a consensus that the framework should continue to be developed and used on complex systems in a wide variety of sectors. In addition to further development and validation of the University of York framework, the following six areas of work were considered important.

Definitions – a lexicon of safety

There is evident confusion over definitions and the relationships between safety, resilience, robustness, efficiency, security, anti-fragility, and other terms used to define aspects of safety or, in some cases, used as a synonym for it. To add to the confusion, many terms are used differently in different domains and there are few internationally agreed methods of measuring the things the above terms describe.

Engineering X was encouraged to support the production of a lexicon, focused on end-users, that analyses the various terms, their usage, and definitions in different environments and how they can be translated across disciplines, between academic study, public usage and internationally.

More specifically in relation to this mission, it would be useful if we could agree, and disseminate, a clear definition of 'safety' in the context of Safer Complex Systems.

Acceptable levels of safety

Over the years, there have been many efforts to explore what constitutes an acceptable level of safety. Few have been successful, even for systems with clear definitions of undesirable outcomes, and people's perceptions change over time. It is particularly difficult to articulate what counts as 'safe enough' for an ad hoc complex system that affects a spectrum of communities or where the outcomes of a systems failure might be psychological trauma, malnutrition, lack of security, financial destitution or other detriment that resists easy numerical quantification. A further important issue that arose was the security of complex systems and the extent to which 'safety' needs to encompass resilience to (external) malicious intent.

For any given system, who is consulted on what is 'safe enough' and who decides? A related question is what, if anything, does 'safety' mean in, for example, a humanitarian aid environment where a failed outcome is difficult to quantify in conventional safety engineering terms? To a large extent the definition is unimportant if the system dependably delivers a high-quality service.

It was suggested Engineering X could support a study to investigate the way in which people view and assess safety – including differences between regulators and the public. This is a busy field and the work will have to concentrate on 'the white spaces', as they relate to complex systems, rather than trying to cover the whole field.

Regulating the safety of complex systems

Internationally, there are many different regimes for regulating the safety of hazardous situations. Most work adequately for well-understood hazards but can produce anomalous decisions for complex or unusual hazards and are poor at regulating low-probability, high-impact events. Regulation of hazardous systems is often based on the assumption that there is an individual or organisation who can be held responsible while, for many complex systems, safety is an emergent property of a system-of-systems, each component system having a separate management structure with no commitment to the safety of the whole – and no one person or organisation who understands the whole system.

There is a clear need for an international review of how public authorities can regulate the safety of complex systems within their jurisdictions. Are existing laws adequate and, if not, are there any alternatives? There are already several ongoing studies on regulation of complex systems, including a *Foresight Review*, expected by the end of the year, and work on the regulation of driverless cars. An additional study will need to be carefully structured to avoid duplication and to make a significant contribution.

Support for well-structured case studies

In MBAs and other business courses, case studies are widely used to increase students' understanding of key issues. However, there is not a comparable library of case studies in complex systems. A challenge with complex systems can be convoluted feedback loops and ill-defined interactions involving individuals and organisations. A classic narrative form often doesn't capture the important points and a new style of case study might be needed, along with a new way of using them.

Engineering X is already supporting the development of case studies and the workshop encouraged this activity, as well as more analytical work to determine the most appropriate form for case studies to take to ensure that suitable information is provided to maximise learning.

Education

It was widely recognised that engineering and business degree courses are generally deficient in teaching about complex systems: the courses have not kept up with the way the world has changed. It was suggested Engineering X could set up a *Safer Complex Systems Education and Training Group* to work towards an international programme of education, guided by the broader community who will be the beneficiaries. An understanding of complex systems is important for policymakers who may determine the governance layer and also for engineers who need to be able to see their own (small) system in the much broader interactive context. Whether this should be a role for the Safer Complex Systems mission or whether it would naturally fall under a different Engineering X mission is less important than that the work be done.

Diversity and inclusion

To ensure all aspects of a complex system are considered, a multidisciplinary team is needed. It is important to include people from different backgrounds and viewpoints – for example, giving a voice to occupants and users of a building, not only the owners and architects. The workshop also heard how complex systems should avoid being described as an exclusively technical domain and needs to expand the scope to cover anthropological and sociological aspects as well as greater use of social and behavioural issues in framing the risk.

Could Engineering X commission a good practice guide on diverse team building and communication, and is this an activity that should be taken forward outside the Safer Complex Systems mission?

2

Introduction

2 Introduction

The workshop took place on 25 September 2020 and was held online because of the COVID-19 pandemic. It was run under the auspices of the **Engineering X Safer Complex Systems mission.**

Engineering X is a new international collaboration, founded by the Royal Academy of Engineering and Lloyd's Register Foundation, that brings together some of the world's leading problem-solvers to address the great challenges of our age. The Engineering X community connects partners from around the world, building on a network of global alliances to tackle the most pressing engineering, safety and sustainability problems, and developing practical, sustainable and accessible solutions for the engineering profession worldwide.

There were 131 participants in the workshop. The four diagrams below show a participant breakdown by country of residence, organisation type, gender, and career level.

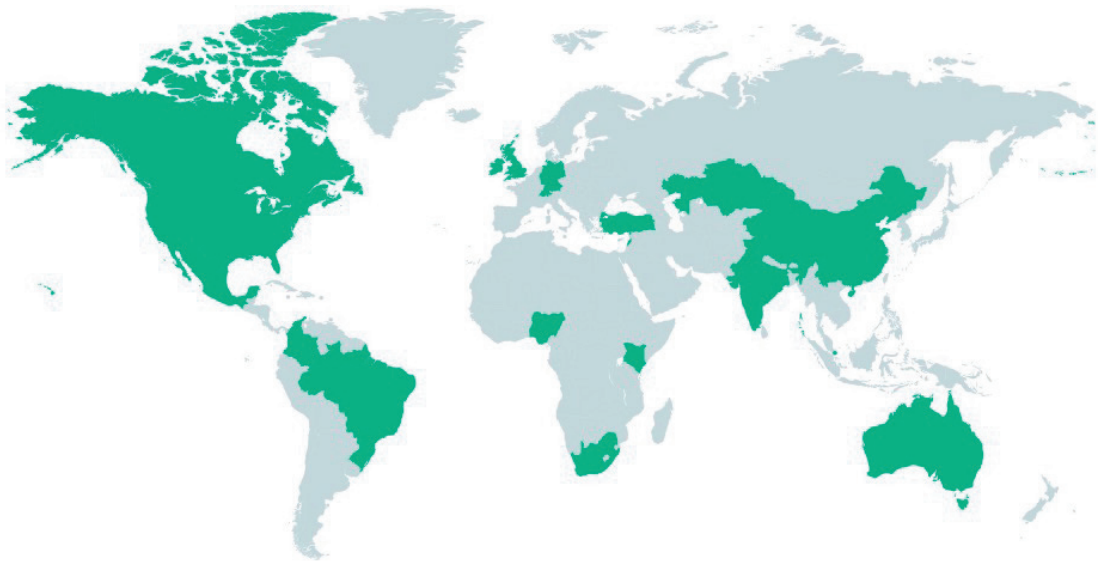


Figure 1: Country of residence

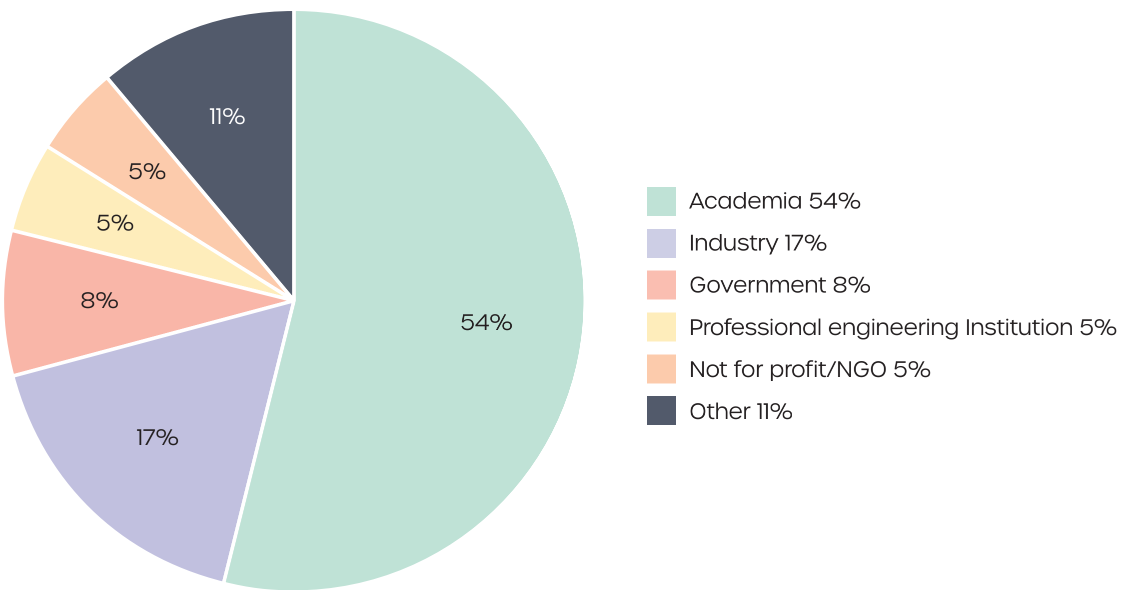


Figure 2: Organisation type

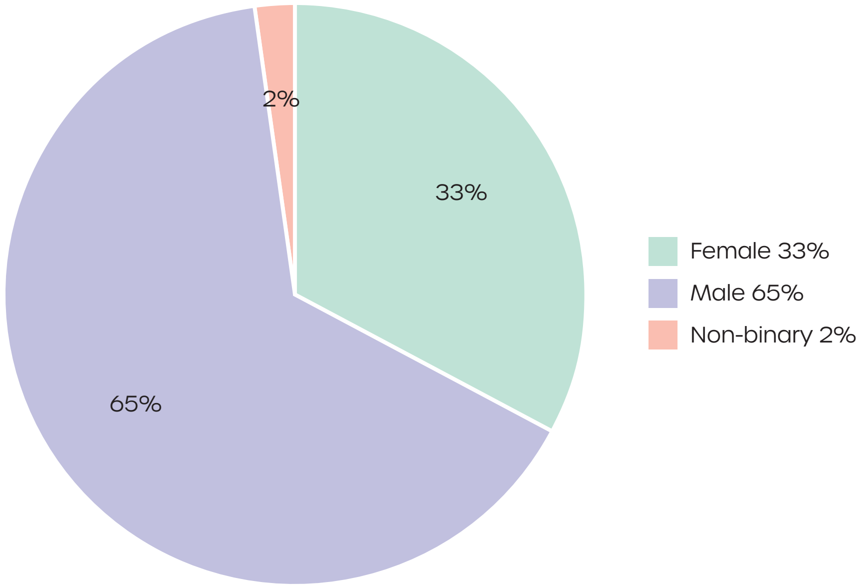


Figure 3: Gender

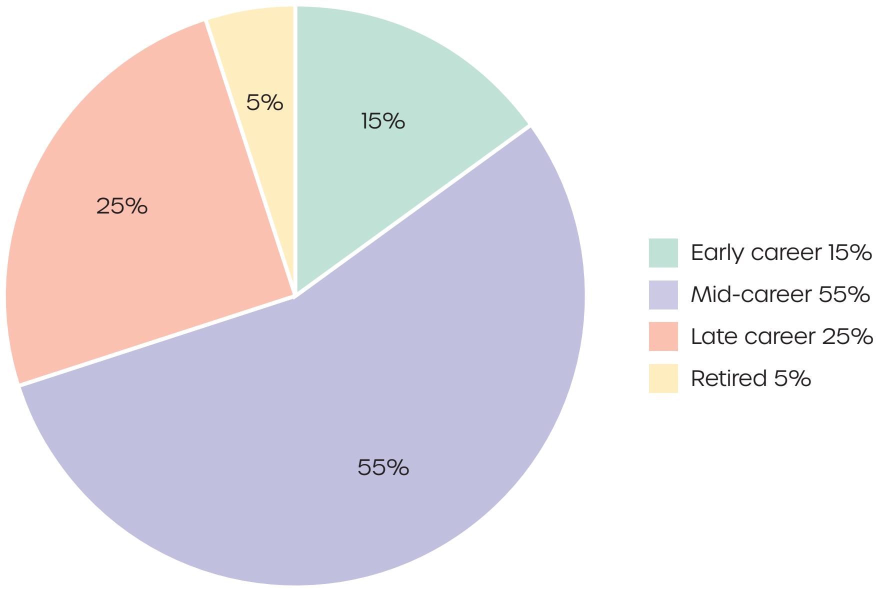


Figure 4: Career level

The event was heavily over-subscribed. Organisers made efforts to balance specialisms away from traditional engineering and were pleased to welcome people working in crisis zones, child safeguarding, natural and humanitarian emergencies, health and social care, defence, insurance, and many other non-engineering sectors.

There were two sessions, using the same agenda, each with around 65 participants. Because of time zones, people from Asia and Oceania tended to be in the earlier group and those from the Americas in the latter group. The agenda can be found in Annex A, the organisers and staff involved in Annex B and the list of participants in Annex C.

This report of the workshop is intended to convey the ideas that were discussed. It is not a formal set of minutes or a verbatim account. Ideas are grouped for clarity, rather than representing the order they were raised or the groups in which issues were discussed. Inevitably, a half-day workshop did not come to many hard and fast conclusions. With some exceptions, this document elaborates on the issues raised, several of which are contradictory. It does not aim to present a coherent set of conclusions.

Except for the Chair's introduction, this report does not attribute statements to any individual. We hope it explains the arguments put forward and increases understanding of complex systems.

2.1 Introduction to the workshop

Delivered by Dame Judith Hackitt DBE FREng
(Workshop Chair)

Welcome to the workshop. Participants have had the opportunity to watch the pre-recorded presentation for this event, which has helped to frame this workshop and summarise the key points of each report. As a brief recap:

- The frame of reference has been shifted by COVID-19
- The scale and urgency to deliver solutions to safely manage complexity has now increased
- We need your help to decide the most important next steps for this mission

At this workshop, we will consider the recommendations and usefulness of the two reports that have been circulated ahead of this workshop, and we will discuss the possible ways for us to build on the work we have already done:

- We will look at **risk, trust and acceptable levels of safety**, and discuss how we assess safety of ad hoc systems that have developed almost by accident (such as the supply chain for medical personal protective equipment [PPE]) as opposed to engineered systems (like self-driving cars), and who decides on acceptable levels of safety.
- We will discuss **resilience and reliability**, and will ask if safety is the most important focus for the regulation of complex systems or can resilience and/or reliability be as important?
- We will consider **regulatory structures and policymaking** and ask ourselves whether current models of governance are appropriate for managing safety in complex systems, and if not, how does the model need to change?
- We will look at the important role that **diversity and inclusion** plays in the safety of complex systems. We will discuss how we can avoid the dangers of groupthink and explore ways to consider the beliefs and experience of all sections of the community to ensure complex systems are safe for all.
- We will examine **tools and techniques for safety management of complex systems**, and consider to what extent should simulation, model-based analysis and digital twins be used to manage safety in complex systems. How can artificial intelligence and machine learning be used to assess safety-critical software? What sectors have made significant steps in managing complex systems – who can we learn the most from and why?
- And finally, we will discuss **competencies, education and capacity building**, and will think about what specific skills and competences are needed for the development of safe complex systems.

Research into these areas is just one approach that the Safer Complex Systems mission is taking to tackle these 'wicked' problems. We are developing a range of innovative activities, which can be read about in more detail on the Engineering X website.

2.2 A brief history of the safer complex systems mission

On 19 July 2019 Engineering X convened 43 experts from a broad range of professional backgrounds to explore and inform the scope of their Safer Complex Systems mission.

In an opening address, Dame Judith Hackitt noted the challenges in defining what is meant by complex systems, suggesting that they can be viewed as interconnected, interdependent networks of systems. In many cases, they involve stakeholders from different industries with varying degrees of knowledge about each other. It follows that understanding complex systems plays a vital role in: improving our understanding of risk; identifying critical points of failure; and optimising workflows and process to bring greater safety and efficiency to all areas of society and industry. The 2019 workshop's objectives were to:

- Inform the Safer Complex Systems mission scope and strategy
- Contribute to an Invitation to Tender (ITT) for a *Global Foresight Review on the Safety of Complex Systems*
- Create a community and network that engages a diverse group of interdisciplinary stakeholders interested in improving the safety of complex systems.

The objectives of the workshop were met in that it produced recommendations that informed the Safer Complex Systems Board, an ITT was issued in November 2019, and the workshop brought together a group of people interested in taking the Safer Complex Systems mission further.

The result of the bidding process was that a contract was awarded to the University of York early in 2020. A first draft of a report was completed by the end of April 2020. This was reviewed by a Technical Advisory Group (TAG) of 30 experts in various fields (mainly different sectors of engineering) and a final draft was produced in July 2020. The paper, *Safer Complex Systems – An Initial Framework* (referred to as the York report), was published with restricted circulation in September 2020, prior to this workshop.

A second input to the present workshop was a report on *Exploring the Safety of Super-sized Structures* (referred to as the 4S report). The report summarised the conclusions of an event held (virtually) on 11 May 2020 with 33 participants. It was hosted by the Royal Academy of Engineering partnered with Lloyd's Register Foundation, University College London and BRE (the Building Research Establishment), and brought together people involved in five groups:

- **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).

Lloyd's Register Foundation had previously published an *Insight Report on Global Safety Challenges*[1], which identified issues associated with the safety of super-sized structures. The May 2020 4S workshop was held to better understand this challenge, including the identification of critical areas and knowledge gaps, and to establish which practical steps could be taken to enhance the safety of large structures and protect lives across various types of built environment and infrastructure. Typical instances might be roads and railways[2], bridges, dams, tunnels, mega-buildings, ocean-going ships, and transport nodes. Many of these share contingent risks from, for example, effects of extreme weather and climate change, seismic disturbance, fire, and inaccurate human perceptions of risks, lack of competences[3] and corporate policies[4]. 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[5].

The May 2020 4S workshop was intended to inform thinking around research needs, policy recommendations and practice guidance. Generic issues and cross-disciplinary concerns were identified across all five sector groupings. It was clear that common challenges spanned socio-technical, economic, educational and engineering domains from viewpoints including safety, risks, economics, competency, regulation and governance.

Several themes emerged from the meeting. An important issue was the need for project teams to know who is responsible for the safety of a whole system. Managing ageing structures was a common theme, with similar observations from geotechnics and offshore sectors on the difficulty of assessing asset condition and balancing safety with necessary investments in renovation. Some assets, such as Victorian rail tunnels, iconic bridges and drainage systems, have a useful life in excess of 150 years. How do we assess these structures, as well as future-proofing the new infrastructure that we are building today? The recommendations for further work are discussed in the following section.

3

Inputs to the workshop

The conclusions of the two reports, *Safer Complex Systems – An Initial Framework* and *Exploring the Safety of Super-sized Structures,* are summarised in this section. They contributed the main themes of the first part of the workshop.

3.1 *Safer Complex Systems – An Initial Framework* report

The York report identified six themes that they believed required further work:

Theme one:
Risk, trust and acceptable levels of safety.

Develop approaches for better communicating risk, increasing trust and forming consensus on acceptable levels of safety.

As systems become more complex, the concepts of risk and acceptable levels of safety become harder to define. There needs to be a greater emphasis on understanding and articulating acceptability of risk, particularly in relation to systemic failures that are, by their very nature, hard to predict. A common language for communicating risk is required that can be shared among policymakers, industry and lay people to reach consensus for setting safety targets and build trust in the systems and/or in the organisations that develop, operate, sustain and regulate them.

Theme two:
Complexity in regulatory structures and policy making.

Acknowledge and address complexity in regulatory structures, legal accountability and policymaking.

Government policymakers should consider the growth in complexity, and the trends in the scope and capability of systems, when examining regulatory structures. This should include the application of outcome-based standards and publicly available specifications as a means of increasing agility in regulation.

Furthermore, issues surrounding tort law and the allocation of accountability across multiple stakeholders, each of whose actions may contribute to harm caused by a systemic failure. By regarding regulatory frameworks themselves as complex systems, an evaluation of the effectiveness and inherent risks of regulatory failures should be continuously performed in order to consider changes in the environment and emergent risks of new classes of both engineered and 'accidental' systems.

Theme three:
Addressing diversity and inclusion.

Develop methods to address diversity and inclusion during risk management and promote diversity of thought.

This report has highlighted the influence of diversity and inclusion in several ways. Firstly, it has been shown that risk is not equally distributed between stakeholders in a system due to various diversity characteristics. Though often related to ethnic and socioeconomic background, gender or disability, some of these characteristics (or at least their relationship to risk) may not be so obvious due to system complexity. An explicit recognition of diversity factors during risk analysis and management approaches is required, supported by an appropriate methodology. Furthermore, a way of including a wider diversity of thought in risk management should be developed. This includes the recognition and support of whistleblowers but should go beyond this, involving a wider spectrum of stakeholders when formulating regulation or safety standards.

Theme four:
Data-driven prediction of systemic failures.

Integrate simulation, model-based analysis and digital twins into design and operational-time controls.

Data collection and analysis techniques need to be developed to enable the advancement of *Digital Twins* of complex systems that will allow for systemic failures to be predicted and their underlying causes to be analysed. This will involve applying a variety of techniques from model-based simulations to statistical evaluation and extrapolation, and will probably use statistical analysis or machine learning. Such models could be used to examine the effects of proposed changes to the system or its environment in order to predict limits of manageable safe behaviour – the 'safe operations envelope'.

The modelling strategy needs to include a correlation of system performance with the output of simulations to ensure the models are grounded in a practical understanding of the relationship between the simulation and real world performance. The framework proposed within this study should be used to provide context for such a strategy.

Theme five:
Holistic approaches to risk assessment.

Develop an integrated and complementary set of methods for analysing risks in complex systems.

Deriving strategies and associated methods for analysing and managing safety risk associated with complex systems is obviously a key area of future work. This will involve extending existing approaches and looking beyond these for a set of complementary techniques that compensate for deficiencies or limitations of current methods. This could include techniques that cover what formal and technology-focused analysis can or cannot do, and could include story-telling, rich pictures, simulation and reflective equilibrium to ensure that a diverse set of opinions from different stakeholders are captured when determining the risk associated with the system.

Theme six:
Resilient complex systems.

Identify design-time and operation-time controls for increasing system resilience.

Design-time and operation-time controls can help to reduce safety-related risks. Current complex systems suffer from faults but normally they are successfully managed to ensure safety. In the York report resilience is viewed as the ability of the system to remain in a safe state despite unforeseeable events. Resilience is an operational concept but it needs design-time support to enable it, including for human oversight and control. Future work should develop ontologies of design-time and operation-time controls for increasing resilience at the governance, management, and task and technical layer to provide practical guidance to designers and operators of future systems.

3.2 *Exploring the Safety of Super-sized Structures (4S)* workshop summary

The 4S workshop identified three categories of safety issues:

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.

High-consequence, low-probability hazards pose both social and physical science problems. The understanding of, and response to, such risk is difficult. The statistics and science of this type of risk are also hard; there may be very little experimental evidence to model or predict likelihoods, and the chain of precursors can be complex.

Few large structures exist simply as engineering structures. Most form part of complex socio-technical systems where the organisation and objectives change over the life of the asset. 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.

Monitoring and managing residual risk is important, but it is increasingly easy to be overwhelmed with data, and a key skill is to convert this into reliable and useful information. In the future, artificial intelligence and machine learning are likely to play a role in this, reducing human cognitive burdens.

The study identified eight research questions; many are highly relevant to an understanding of complex systems:

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

4

Safer Complex Systems workshop 2020

4.1 Programme

The first discussion session in the workshop was concerned with the two reports and asked participants to consider the question *"To what extent have these two initial reports helped us on our journey to Safer Complex Systems?"*. In particular, participants were asked whether they found the analytical framework in the York report to be a helpful way of viewing the hazards of complex systems with which they are familiar.

The second, longer, breakout discussion condensed the issues raised by both reports into six topics listed, along with prompt questions, below:

Risk, trust and acceptable levels of safety:

- How do we assess safety of ad hoc systems that have developed almost by accident (such as the supply chain for medical PPE) as opposed to engineered systems (like self-driving cars)?
- Who decides on acceptable levels of safety?

Resilience and reliability:

- Is safety the most important focus for the regulation of complex systems or can resilience and/or reliability be as important?
- Many complex systems, particularly ad hoc systems that provide a service to all members of society, are unlikely to cause an accident or fatality on their own but, if they shut down, the knock-on effects could have severe consequences on death rates and ill health in some sections of the community. How should this be reflected in the safety governance and management structure?

Regulatory structures and policymaking:

Safety regulation in many countries is based on the concept of a duty holder who can demonstrate to a regulator that the risks inherent in their activity are adequately controlled.

- Can this model apply to complex systems, comprising many independent subsystems, often owned and managed by different bodies with no overarching controlling mind or systems authority and subject to different regulatory regimes?
- If not, how does the model need to change?

Diversity and inclusion:

- Accident inquiries often conclude that people responsible for safety management suffer from groupthink, which exacerbates risks in complex systems. How can governance arrangements avoid this problem?
- What mechanisms could be used to ensure that the governance of complex systems considers the beliefs and experience of all sections of the community and makes best use of a diversified safety management team?

Tools and techniques for safety management of complex systems:

- To what extent should simulation, model-based analysis and digital twins be incorporated into design and operational-time controls of complex systems?
- What techniques could be developed for the assessment of safety-critical software using artificial intelligence and machine learning?
- Some non-engineering sectors and disciplines, such as finance/banking, have made significant steps in managing complex systems. Which sectors can we learn the most from and why?

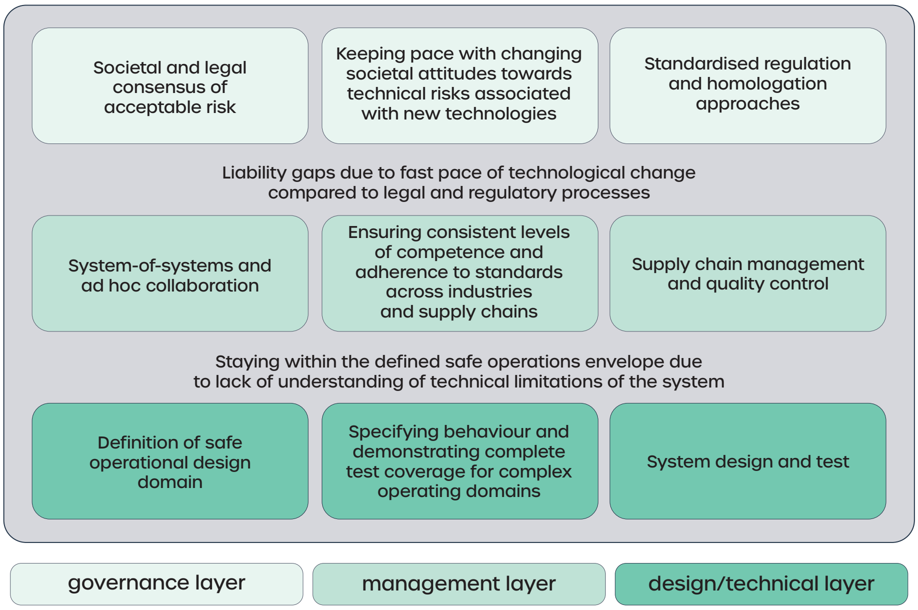
Competencies, education and capacity building:

In many countries, the education of engineers and technicians has not changed as quickly as the systems-based working environment:

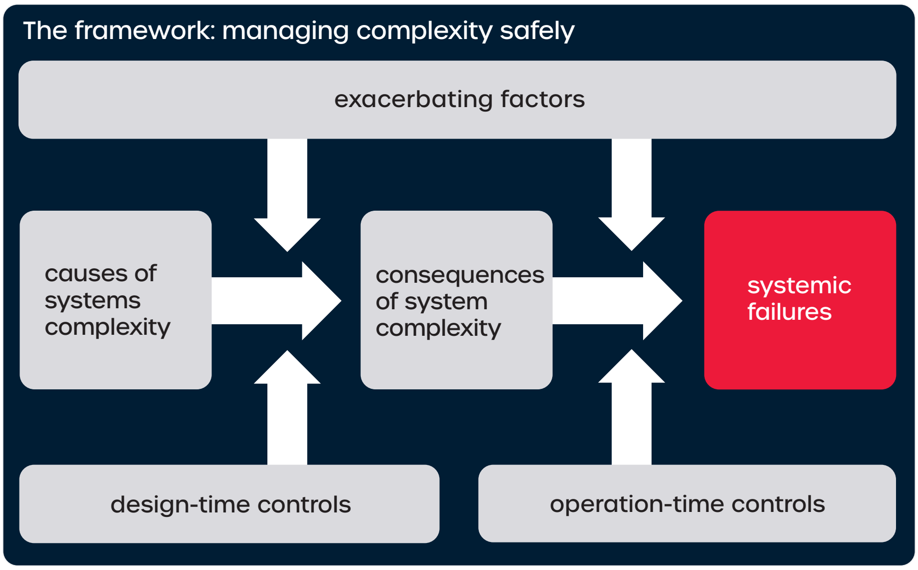
- What specific skills and competences are needed for the development of safe complex systems? Where are these people needed?
- How should the engineering profession respond to preparing new entrants for the challenges of complex systems?

4.2 A framework for analysing complex systems

The York study was based on an analysis of the issues that arise within the governance, management and design layers of complex systems and at the interfaces between each layer. This is shown in the following diagram:

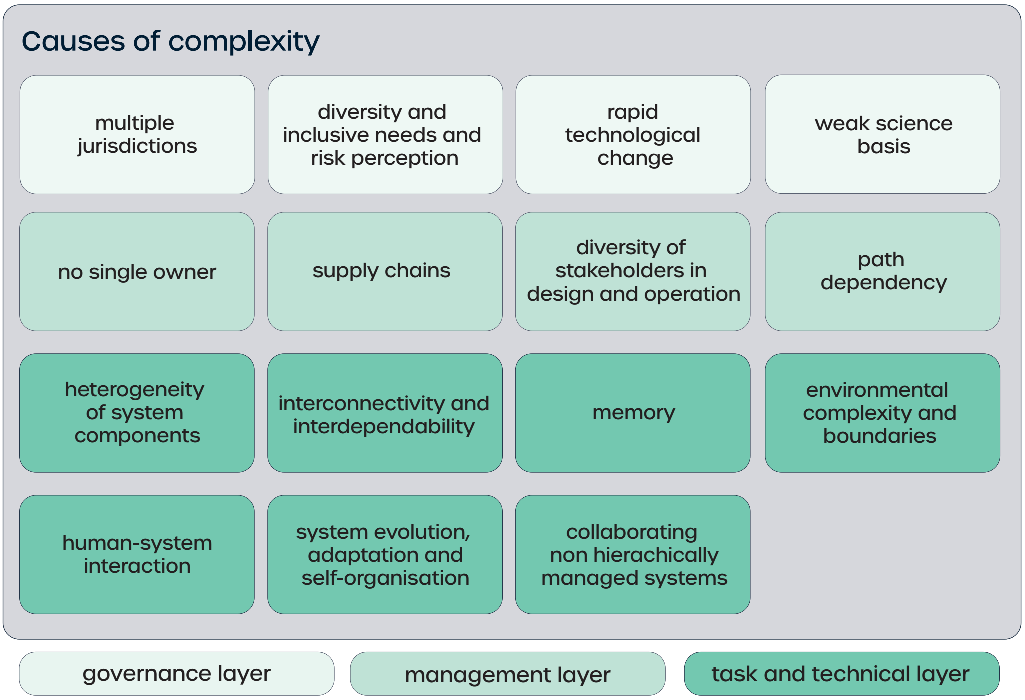


The above diagram is a static representation of the factors involved. During the course of the study, the University of York team produced a framework that shows the dynamic process as a project moves from the conceptual phase, through design and operation. This is shown in the following diagram:

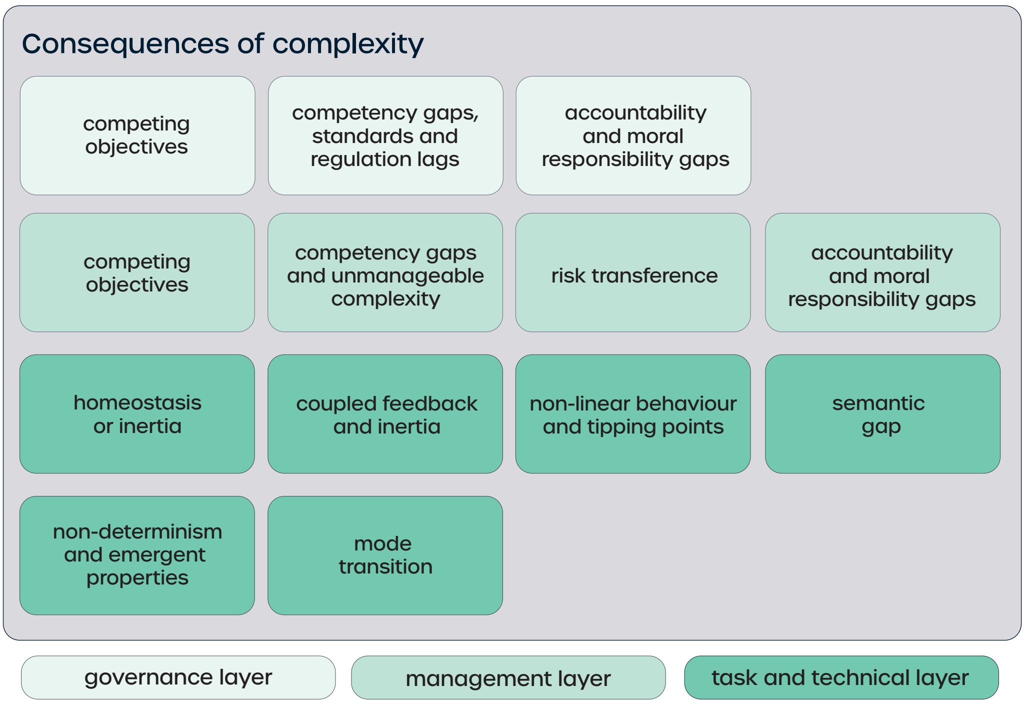


On the left are possible causes of system complexity. Depending on the hazard mitigation that takes place during the design activity, these have consequences that import hazards to the final project. However, just because there are hazards, does not necessarily mean that there are unacceptable safety risks. Operation-time procedures and controls can manage the risks to ensure the activity is adequately safe. The hazards only become systemic failures if the operation-time controls fail.

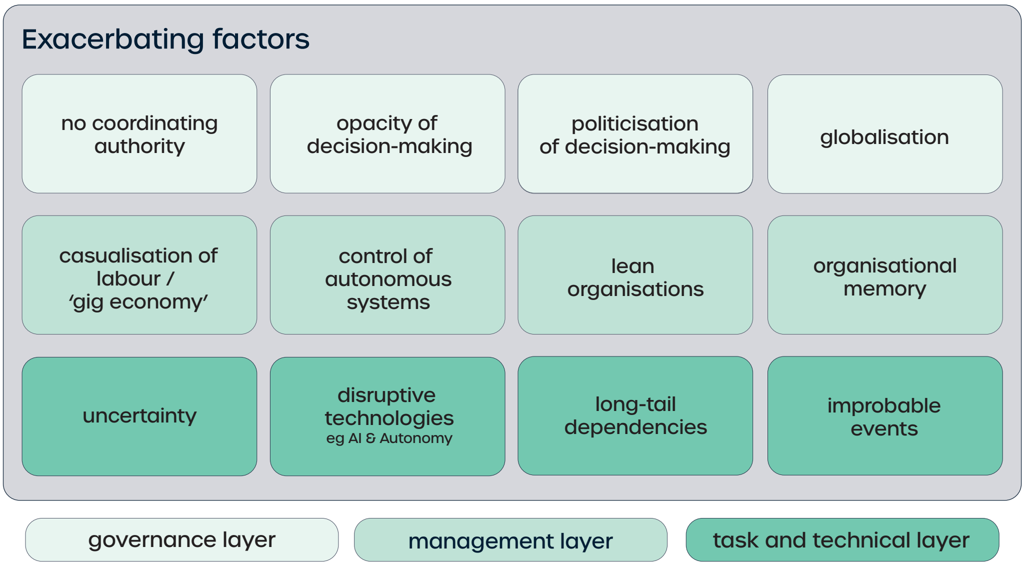
The following diagram shows some possible causes of system complexity. They are divided into three layers – the governance layer describes the legal and organisational framework within which the complex system operates; the management layer covers the people and organisations and the technical layer the technical issues:



The next diagram indicates some of the consequences of complexity. As discussed above, these do not condemn the project to be risky or unreliable but they import hazards that the operations management structure has to mitigate:



Finally, we have the exacerbating factors. As indicated in the framework diagram, these can feed into the project either at the specification/design phase of the project or during the operations phase:



4.3 Feedback from the first breakout session

In the first breakout session, all participant groups were asked to say how useful they find this way of looking at complex systems in their specialist area and, in particular, how relevant they found the framework to be. The general view was that both reports were very useful – one participant described them as *"a huge achievement, on possibly one of the biggest topics we have to think about, in terms of its breadth and depth"* and another participant was quoted as saying the reports were *"informative and useful outside of the event"*.

Participants discussed how the concepts and framework in the reports applied to their specialist areas, which included: child safeguarding, self-driving cars, food production, railways, delivery of humanitarian aid, nuclear power, shipping, healthcare, the oil and gas industry, epidemiology modelling, aerospace, finance and insurance.

Although the first group of breakout sessions were not envisaged as identifying new directions of work, a wide range of possible areas for future focus were raised. To avoid duplication, discussion of these topics has been moved to subsequent sections of this document.

There were several comments and criticisms of the reports – particularly about the framework – but some took diametrically opposed positions:

- The language and structure of the reports are complicated and they read like research reports [which they are]. To be useful, a future document should be more focused on the user and should use simpler language.
- In contrast, some considered the York framework to be over-simplistic and possibly not able to cope with real-life systems. It was recognised that the reports are both UK-centric and written predominantly about engineered systems. How well the techniques will work in different cultures and with systems that have little or no engineering content is not yet proven. Even for predominantly engineered systems, there is often a need to expand the scope to cover anthropological and sociological approaches, and also to include more social and behavioural issues when framing the risk.
- A participant working in synthetic biology (engineering of life – by definition, a complex system) noted that technology readiness is not as high as in other areas of engineering. A major concern is biosecurity rather than safety – for example, trying to prevent malicious actors creating a pathogen. Several participants suggested that security issues, including cyber-security, should be part of the framework.
- It was welcomed that the York report considered humans, not just the hardware components. However, it is important that the framework, even for engineered systems, can accommodate people *inside* the system, not just those on the *outside* – a point made by both groups. A hierarchical culture can make it difficult for more junior voices to be heard[6]. Some participants thought that humans should be the focus of a framework, including socio-cultural considerations. Others suggested that human complexity should be split out from technical complexity; the latter can be managed but the human aspect can never be truly managed. However, the manageability of technical components only applies when there are no self-learning or AI components within a system.
- The York framework uses language that is grounded in a particular subset of engineered systems. Other sectors use different language to express similar concepts. It would be unreasonable to expect them to abandon their traditional language to fit in with the framework, so a phrasebook or translation lexicon is needed. Apart from language, there is also a problem of translation of concepts and cultures.
- A few participants, generally from organisations or sectors with well-established standards and processes for managing system safety, commented that the York report used non-standard terminology or processes. They may have been triggered by the thought process: *"There are two ways of doing this – our way or the wrong way."* One of the conclusions of the workshop was the need to recognise there is no one way of describing complex systems and there is a need to share existing practices more widely.
- It was stressed that we need not only a heterogeneity of thought but also a diversity of voices – particularly those from further down the organisation and people from outside who are often excluded because they are not considered stakeholders.
- Quantitative safety measures in the report tend to be physical (such as deaths and serious injuries), which are useful for some types of incidents, such as train or aircraft crashes. In humanitarian crises, the focus can often be on wellbeing, psychological damage, financial destitution and other issues that cannot be

simply measured in physical terms. Another example of the above is the food system. Looked at from a conventional point of view, the UK food system was working smoothly before the COVID-19 outbreak. However, thousands of people were forced to use foodbanks, so the overall system *was* failing, although this wasn't shown by statistics of deaths through starvation. Frameworks should be able to accommodate non-physical harms where relevant by using DALY metrics or similar tools[7].

- The framework is like any management consultant's tool in their toolbox – useful but has to be used by people who understand it and its limitations. Groups were keen to move the framework's thinking into the real world of real programmes, but it needs experts to help make it useful – perhaps by building a consulting interface to take it into programmes. On the other hand, the research and development of the framework must not stop.
- There was wide agreement with the conclusions of the 4S report that far greater emphasis needs to be placed on educating graduates and mid-career managers in concepts of complexity.
- The York framework is good for static projects with a reasonably fixed structure, but many complex systems are more fluid, have fuzzy boundaries and are difficult to pin down. Different actors move in and out; restructuring, take-overs and privatisation change the governance and management layers; and the objective, balance of priorities, system borders, and overall scope of the project vary with time. When using a standardised framework, there may not be the incentive to regularly ask whether it is still analysing the current system. This is particularly relevant for long-life systems that may change with time. The gestation of catastrophes can be a process that takes years and the changes, as they occur, may be gradual and imperceptible[8]. There is a need to monitor the evolution of systems to see if they are becoming more brittle (prone to catastrophic failure). However, few engineered systems, let alone 'accidental' or informal systems, have these mechanisms in place.
- In many areas, tools and techniques for control engineering and systems engineering underwent rapid development between the 1930s and 1960s. Since then, technology has moved on but the availability of appropriate tools for assessing and managing the safety of complex systems has not kept up.
- Widespread adoption of digital technology and the ubiquity of mains electricity as a power source has resulted in many aspects of life, previously thought of as independent, being interconnected[9]. It is often almost impossible to determine the boundaries of such a complex system.
- Many aspects of complexity discussed in the reports are not compatible with the way things are done in current engineering contract management – particularly if the 'system' has multiple owners. There is therefore a question about which organisation might be responsible for identifying if there is a complex system and putting in place (and, presumably, paying for) the necessary risk management processes.
- The framework makes the assumption that it is possible to move smoothly and analytically from the *causes of system complexity* to the *consequences of system complexity* to the *risk of systemic failure*. In many cases this is not possible. Information may be incomplete or not available, and the analysis of moving from cause to consequence might not be amenable to established analytical methods, for example FTA or FMECA[10]. The York report was good at identifying aspects of complexity, but the distinction between causes and consequences was confusing. These aspects emerge as new components and subsystems are added to the system.
- It is difficult to use any framework to analyse systems with low-probability, high-impact consequences where many of the paths to disaster have not been identified. For many systems, the particular combination of inputs and exacerbating factors may not have been envisaged. There is also a question over the extent to which society is prepared to pay for precautions against a low-probability hazard, even if potential consequences are high. Providing 'just in case' capacity of intensive care hospital facilities is a case in point. Looking at the issue more generally, the framework is a useful way of describing complex systems but it does not replace the traditional tools (HAZOP, HAZAN, HAZID, STAMP, brainstorming, near-miss analysis)[11] necessary to identify and classify hazards.
- Some participants commented that much of the discussion was about how to ensure a good coverage of potential failure scenarios. How does that move towards making complex systems safer? Are we trying to understand safety for prediction, self-healing or recovery? And with which groups are we concerned – for example, the people who run the system, the users or members of the public, or perhaps even the shareholders – are protecting their asset value?

4.4 Feedback from the second breakout session

In the second breakout session, each group discussed a different issue from the six issues listed below. This section summarises the content of the discussions; recommendations are grouped in a later section of this report.

Risk, trust and acceptable levels of safety

There was considerable discussion on the need to extend the Safer Complex Systems mission beyond the engineering community. As the circulated reports showed, many of the hazards of complex systems are related to the governance layer and the way in which the system is created and, where relevant, regulated. This may require engagement with national administrations, particularly for ad hoc systems that spread beyond local boundaries or that involve many players with no prior relationship or knowledge of each other.

In many societies, there is little public understanding of complex systems (or even what the term means, other than as an [incorrect] synonym for complicated). Perhaps Engineering X should attempt to reach out to society to socialise complex systems, possibly via television? This is likely to be a process lasting many years, but may be able to build on the recent experience with COVID-19 transmission or the procurement networks for PPE. Society assumes that pandemics can be managed but many people have an oversimplistic idea of the technology or actions needed.

To establish a lasting recognition of the term, could concepts of complexity be introduced into school and university curricula?

A communications and engagement strategy for establishing an underlying understanding of complexity in the community, particularly for decision-makers and opinion-formers, should be a high priority for the Safer Complex Systems mission. This must be tightly focused as the workload involved in trying to communicate with all possible groups would be completely unfeasible. Such a strategy might also have to use different language and examples for different audiences.

What constitutes an acceptable level of safety is a difficult question to answer. There is evidence that, in most countries the general public does not really understand risk. A particularly difficult question is the extent to which risks in diverse fields can be balanced against one another.

As an example, during a pandemic, is it reasonable to ask people to accept lower standards for food safety because of uncertainty about availability?

It is difficult to assess safety of systems that have developed almost by accident. As an example, it was suggested that UK provision of medical PPE was hampered by flaws about where the boundaries were drawn – the system was misidentified as being about *health* and not *health and social care*. Social care professionals have said their voices were not heard early on. The ad hoc solution was community-led groups making things, but these arrangements are fragile. Partly the solution is about routinising things that are ad hoc, but it also requires a system change to recognise governance failings.

In many projects, system safety and cyber security are treated as separate issues, often with separate teams of engineers and a different vocabulary. From the point of view of the users of a system, there is no practical difference between an accident caused by deficient systems engineering and one caused by malicious intent. The safety of complex systems should cover both eventualities.

There is no such thing as absolute safety but the public – and some campaigners and journalists – have difficulty in accepting this. In many situations, the public places trust in certain organisations or professions and is prepared to accept what they recommend, rather than taking a numerate view of the risk. The established view is that people should be involved in decisions that affect their health. But what proportion of the population want to be faced with a numerical summary of risks facing them (for example, when deciding whether or not to have an operation with uncertain outcomes) compared with those who trust their doctor to take the 'right' decisions? Similar arguments apply to many other issues in representative democracies. Is trust more important than analysis?

There is a need to develop a common language to compare case histories across sectors and silos. The York framework is a system of language but leaves the vocabulary open so can be adapted to different sector terminologies. A translation service is needed.

Resilience and reliability

Safety is a good measure for some complex systems – it can be applied to self-driving cars for example. However, it is less useful when the adverse outcomes are hunger, destitution, civil unrest or shortened life expectancy. Looking at the food system, the term antifragility – the ability of a system to learn or improve and become more resilient – might be preferable. Another definition includes reduction of vulnerability. Stress testing in the financial sector can assess the resilience of the system and regulation can subsequently improve antifragility. For all systems, an increase in whole systems resilience can boost the safety of a system, because they are closely interrelated.

Participants had different views about the usage of the terms resilience, robustness and reliability. For many people, these terms can be considered as means to achieve safety, and it is important not to confuse the means with the ends. There are many other ends that a system has to accommodate such as ease of use, affordability, security or environmental impact. On the other hand, some considered that resilience encompasses both safety and reliability.

There is an issue about the term resilient as it denotes the ability of a system to revert to a previous state when subject to disturbance, while what might be needed is the ability to recover to an improved state. Terms like robustness, resilience, security, sustainability, capability and reliability are all relevant and can help generate safer systems. One suggestion is that resilience is the ability of a system to respond to unknown disruptors while robustness is the ability to cope with known disruption. It is important to distinguish between the two. A different take on the subject is that safety and resilience are emergent properties but reliability is not.

Another view is that resilience is the capability of dealing with emergent changes, either proactively or reactively, to ensure the safety and reliability of the system. Therefore it is worth considering in system design and operations, for instance in procurement when configuring supply chains, as a measure to assess suppliers. Reliability is more about how the system is operated compared with the objectives, but these objectives can be wide and conflict with safety objectives, particularly the financial health of the system. So to regulate reliability we need to ensure system objectives do not conflict with each other.

In many sectors there is a conflict between resilience and efficiency. Particularly in ad hoc systems where the system is the responsibility of many different players (who, in some cases, don't even know the others exist) creating a resilient (or safer) system will reduce the efficiency and therefore cost money in the short term. The challenge is to balance the benefit, which accrues to society, with the costs that could bear on only a proportion of the players. Sometimes, redundancy and spare capacity has to be built into a system to provide resilience. Someone has to pay for resilience. Does this point to the need for more intrusive and independent regulation of complex systems?

In tightly-coupled systems, such as the interactions between aircraft control systems, air-traffic control computers, the pilots and the controllers, the relationship between the various players is clearly defined, system boundaries can be fixed, and it is not difficult to draw a relationship and analyse the resilience of the system to known perturbances. However, there are many loosely-coupled systems where the relationships are less clearly defined and frequently shifting, system boundaries are not fixed and estimating resilience is more challenging.

Can systems learn from other systems to increase resilience? This is one of the objectives of the Engineering X work to provide a common framework and language to enable cross-sector communication and learning. However, this currently only works between the human actors in a system. In the longer term, is there opportunity for complex systems using AI to communicate digitally with others and learn from them? An end goal could be a central role for self-adaptive systems.

An alternative view is that, as it is very difficult to analyse and manage highly complex systems, is there benefit in intentionally limiting the size and complexity of systems to increase resilience? Since the disruption caused by COVID-19, several countries are simplifying supply chains for critical supplies.

Regulatory structures and policymaking

Regulatory structures have to strike a balance between managing risks calculated by experts and those reflecting the priorities of the engaged population. In many cases, a statistical analysis of risk is very different to the views of the wider population, pressure groups and the press. As an example, abduction of children by strangers can fill the front pages of tabloids but is low in the overall risks of childhood. The weighting given to the accidental release of radioactive isotopes compared with that given to chemical discharges by industry is another example.

The public likes the comfort of having a named individual who is held responsible for risks – someone who will go to prison if a serious incident occurs. Much national safety legislation is based on this principle – in the UK, the concept of the Duty Holder is important in health and safety legislation. The 2007 Corporate Manslaughter legislation was introduced following public outrage over directors of companies not being held liable for catastrophic incidents. However, with catastrophic failures of complex systems – particularly ad hoc systems – it is often impossible to pin the blame on an individual or even a single organisation. Most engineers tend to think in a deterministic way; lawyers are similar. However, the world is not one linear chain of cause and effect and, in complex systems, a different way of analysing incidents is needed, as well as a different regulatory mindset.

There is a question of whether regulatory structures should determine who is held culpable when things go wrong or whether they should concentrate on investigating the system to prevent further incidents. People are afraid of legal culpability and the fear of self-incrimination can cause a lack of transparency and protracted (and expensive) investigations, where all parties are defensive and legally represented. Transparency, openness and even-handedness are important in achieving societal acceptance of regulation of complex systems. Successful regulatory systems, such as for the European aerospace industry, are more focused on the need to identify causes of incidents than on punishing miscreants. However, many other systems are more about establishing liability than learning from the incidents.

Maintaining an effective regulatory capacity is not cheap and, in periods when everything is going smoothly, there is a temptation to cut costs and cut regulations to 'reduce red tape'. A participant suggested that this was seen prior to the 2010 Deepwater Horizon oil spill when regulators had resources reduced to a level that meant thorough inspections were not carried out[12]. Similar criticisms have been raised about the regulation of the Boeing 737-MAX, a failure of a complex system for which the root causes are still under investigation[13].

After a major system failure, there is often an inquiry that examines the causes of the incident in great detail – and at great expense. Would it be desirable to spend a fraction of that cost earlier in the project to undertake independent audits on all potentially hazardous structures and systems before any crisis occurs?

In complex environments it is important that commissioners, regulators and investigators are familiar with the technology and have a corporate memory of previous incidents. Twenty-first century employment practices can result in people switching jobs frequently, which leads to a loss of experience and effectiveness. This is particularly evident in some government departments that employ generalists moved from department to department every year or two, resulting in a lack of corporate memory. Regulators tend to be organised in silos, while complex systems can span several silos.

There are often multiple complex systems interacting with each other, and it is the connections between the systems where some of the greatest risks can occur because no-one is observing those junctions. A new approach should be cognisant of that and require managers and operators to identify the interactions of all connected systems and find a way to build safety into the connecting nodes or moments of transition.

Participants in the workshop identified the possibility that validated and approved complex systems gradually become hazardous as large numbers of individually insignificant changes are applied to different components of the system over a sustained period[14]. This is particularly true for systems including significant human involvement, as this is generally less well-specified than technical components. Changes to the governance and management layers, for example due to restructuring, can have insidious effects, not noticed at the time.

Reading accident investigation reports, many recommendations are to add more complexity to the system – extra safety features, additional new rules, and so on. All this adds to the complexity of the system. Might it be better to simplify the system and eliminate some sources of risk, rather than increasing the complexity to manage them?

For large complex systems extending over several jurisdictions, such as climate change, food supply or pollution, the desired outcome cannot be achieved solely through regulation. A principles-based approach to inclusive design, manufacture and management would be more flexible than a rules-based approach. As an example, a Canadian participant said that the COVID-19 messaging from the British Colombian government defined the principles: be kind, be safe, be calm and so on, so the public could understand them in relation to their personal circumstances. By contrast, the UK's public health messaging was a confusing combination of a shifting set of detailed rules, in addition to a very general exhortation to 'use common sense'. Principles are more likely to be adaptable to the different sectors within a national or global context.

The same is true for the regulation of complex engineered systems. For example, the formal, detailed safety regulation used for tramways and driverless metro systems (like the Vancouver SkyTrain or London Docklands Light Railway) cannot be replicated for driverless buses or taxis[15]. A principles-based approach, although not proven, may be more appropriate.

Diversity and inclusion

Discussions in the workshop stressed the importance of including people from different backgrounds, professions and viewpoints in the design and management of a complex system to increase its safety. For example, giving voice to occupants of a building, not only the owners and architects, so that all aspects of a complex system are considered and additional risk factors are uncovered. Teams need to be as interdisciplinary as possible including, where relevant, epidemiologists, sociologists and those with understanding of population behaviour. Some engineering companies may be uncomfortable building trust with community partners or non-engineering professionals (such as social scientists and behavioural economists) and communicating with them in accessible language[16]. Organisations and companies need to develop this competence. Could Engineering X commission work on developing inclusive language to promote better community and interdisciplinary engagement in the design of complex systems?

When developing complex systems, there needs to be a team of people taking an overview of the development. In some environments, this might be a management team, in others, a regulator. For ad hoc systems this could be an arms-length body. Such oversight needs experts to understand what is being done but also needs generalists and parallel teams of non-experts able to interrogate decisions. It is important that some of the non-experts have sufficient domain knowledge to be able to question technical decisions and other experts are able to discuss authoritatively how the development might affect other systems and communities. In engineered systems, non-experts need to be able to question what a 'black box' does, where it gets its data and how its actions are validated; they should not be diverted in trying to understand the detail of what goes on inside the box.

Tools and techniques for safety management of complex systems

Participants raised the importance of everyone involved in the design of a system having a clear understanding of how it fits into any wider 'system of systems' and how it is intended to function under all normal and abnormal conditions. This is essential before attempting to produce digital twins or other management or monitoring tools. Having the conceptual understanding of the key processes involved is key to understanding things. Where simulation and modelling are useful are as a proxy if time is limited. But, if our conceptual understanding is imperfect, these should only be used as part as an overall toolkit. An alternative view was that humans cannot grasp the full implications of complex systems and so they need support from simulation and machine learning, but the humans are left having to make decisions.

We should be wary of applying a model from one sector to another, without a good fundamental understanding of the sectors – for example, a model that might be useful for system integration in Heathrow T5 may not translate into hospitals. Models are designed for a particular purpose and there is a risk if they are used for purposes that they were not intended for. There is also a need for 'sense making', which is particularly important when using models. As an example, in the shuttle disaster, NASA used one type of model for what caused the problem but another should have been used: a more abstract model rather than a design model was required.

There is no silver bullet for safety in complex systems – we need diversity in people and approaches. We need to update our simulations, for example. In many engineering disciplines, software is often developed by people with a coding background rather than a relevant engineering or domain background, which may miss important linkages and result in an inadequate description of a complex system.

Much work of engineers is related to recovery after system failure. We need more tools to capture variable parameters and changes within a system that is going right (not just when it is going wrong)[17]. In healthcare, things go wrong all the time, but staff are resilient, and the system continues to work satisfactorily.

Engineers often lack the tools and methods to undertake sufficient analytical work on complex systems. Simulation is insufficient. AI is only as good as the training sets that it learns from and, of course, we provide those and they may be limited and have bias built in. We too need to aim for complex systems to be monitorable in a way that allows enough time for problems to be spotted and action planned and taken. How that can be done is less clear. Digital twins and simulation are helpful, but with all modelling, the purpose or intent is needed to drive the appropriate level of fidelity and validation. Systems are dynamic and vary over time, so the simulations need to be maintained to keep them up-to-date. These techniques have been used for virtual clinical trials for example, or to aid with predictive maintenance. However, they are not always appropriate and need to be carefully tailored for the application. The term digital twin is often misused or misapplied so some have a negative view of the technique.

When we use modelling in more conventional engineering processes, we make assumptions about continuity of behaviour. The problem with complex systems is that there are singularities that can lead to a high impact event (a black swan event). Financial systems have demonstrated spectacular systemic failures – the 2008 banking crash and the 2010 US stock market flash crash for example. All models should be put under stress and sensitivity analysis. Commercial testing of software system is very poor so we shouldn't overemphasise the role of testing. Testing systems to their extremes and reconfiguring as a result is important; we have to break them, but this almost never happens commercially.

Competencies, education and capacity building

The groups were clear that, in most countries, the formation of professionals involved in complex systems was inadequate. Engineers are taught the fundamentals of engineering and the underlying science, but generally not involving cross-discipline systems thinking. A problem in higher education (HE) is that we assess students individually but expect them to work collaboratively on projects – this is perverse, and it creates individual behaviours that are taken into the workplace. There is also a tendency to adopt linear fact-based teaching (easier to assess?). Perhaps the stress should not be so much in the subject of module, but in the way learning is undertaken in any module – away from conformity and towards creativity and original solutions.

Competence building in understanding complex systems is not exclusively an engineering issue. It also needs to include people involved in environmental science, finance, health and many other disciplines. Possibly most importantly, people involved in the management layer and the governance layer also need to understand the issues involved[18].

Skills and competences for engineers need to include influencing, systems thinking, understanding of mental models, situational awareness, mental overload and many other topics that are more traditionally considered as psychology or sociology. Engineering should include systems thinking, including the 'social' in complex socio-technical systems and other soft skills. Critical thinking is important. Reflection is important in development and understanding how to improve. Discourse analysis is important too – how are we engaging with stakeholders when we implement developments? How do we prepare our graduates for these challenges? Corporate professional development (CPD) is critical.

These criticisms apply to engineers but also – and probably more so – to the policy-makers and managers who specify and commission the systems and who dictate many of the management structures. A participant who teaches in the management domain, not engineering, finds little room for complex systems and complexity thinking. It is often left as an extra point in a couple of operations modules and not central, like it perhaps should be. The participant said that in their management school it was hard to introduce complex systems thinking. Complexity and systems thinking are not central for degree courses, they are 'relegated' to the side-lines when this shouldn't be the case. It is useful in helping organisations to understand the problems they face and how to solve them. There are opportunities available, such as online learning. This should also be put into other disciplines, such as the business school world.

There is a particular need to build multidisciplinary competencies and skills at MSc/MEng level with strong support from case studies. Real world experience is essential to understand complex decisions but most undergraduates have not had much real world exposure so there is a limit to the extent complex systems can be taught at this level. While it is important to introduce undergraduates to the concepts of risk and complexity, detailed work should be concentrated at post-graduate level. Some case studies could learn from the accident and incident investigation approaches in aerospace, which have been key contributors to reducing risk in that industry. For this reason, it was suggested that, in the short term, Engineering X should focus on CPD and short courses for the current engineering workforce.

The academic community needs to consider how best concepts of complex systems, risk and safety can be introduced in post-experience learning for engineers in industry, either during career breaks or as CPD. The structure of an MBA could provide a suitable starting point for the design of courses for this group of engineers. Developing an understanding of concepts of risk management in ad hoc complex systems will be challenging and a different approach to course structure will be needed, in comparison with postgraduate courses in traditional engineering subjects. It is important for engineers to upskill and receive CPD to understand the latest theory, which should include dealing with complex systems. It was suggested that, in the short term, Engineering X should focus on CPD of the current workforce; then training that closes the skills gap of a new graduate and the skills employers needs and vocational education and training (VET). In the longer term, Engineering X should aim to update undergraduate and post-graduate curricula.

Competencies need to include teaching people how to communicate as those in different domains within a system may not understand each other because of different vocabularies being used. Engineers also need to be able to communicate with non-engineering professionals, so helping them to do that is a crucial competency moving forward.

In terms of competencies, the ability to distil key information in a complex situation is important. When preparing new entrants – helping them understand how to actually navigate the real world – engineers are generally not handed a clear project definition on a plate and told *"design this"*. Sharing and learning from 'story-telling' is both a way to crystallise and review understanding of events, but also a way to share lessons with others. It also encourages reflective thought.

The balance between regulations specifying standard processes and allowing professionals to do what they need to do would be worth further study. Sometimes we tend to focus on what went wrong after the event, which can result in regulations that are proscriptive, but only in a few areas. Sometimes failures happen in a broader organisational level concerning the structure of the project, rather than an individual, but inquiries focus on individuals' error in the operations phase, rather than the inappropriate conceptual design.

One area of focus in further work could be the tension between regulation and decentralisation; there is evidence that regulation is often used to 'tame' complexity, yet it can often stifle innovative thoughts and actions that can keep citizens safe. When systems get more complex, a full understanding of the system by any one person is too difficult, but we still typically train people in the system. What seems to be missing is training in the skills to make decisions in complex circumstances.

A key word in all of this is safety. A Hippocratic oath, or equivalent, is required for a number of professions, but often not for professional engineering. Engineers often have responsibility for other people's lives. The document defining the standards for UK engineers, UK -SPEC[19], states *"Chartered Engineers shall demonstrate a personal commitment to professional standards, recognising obligations to society, the profession and the environment"*. This is quite a weak commitment, compared to a Hippocratic oath, although it does cross-reference a more detailed document on ethics.

It would be advantageous for Engineering X to study *The Complex Systems Digital Campus (CS-DC)*, an international network of individuals and more than 100 universities and institutions working together and sharing resources to promote research and education in complex systems science and in integrative sciences[20].

A participant in the workshop uses the Cynefin framework to teach different responses to different situations. It is a conceptual framework used to aid decision-making. Created in 1999 by Dave Snowden when he worked for IBM Global Services, it has been described as a *"sense-making device"*. Cynefin is a Welsh word for habitat. It offers five decision-making contexts or *"domains"* – obvious, complicated, complex, chaotic, and disorder – that help managers to identify how they perceive situations and make sense of their own and other people's behaviour. The framework draws on research into systems theory, complexity theory, network theory and learning theories[21].

It was suggested Engineering X should form a Safer Complex Systems Education and Training Group and work together towards a certified international programme of education. However, complex systems should not just be a job for engineers, it should be across all sectors. Safer Complex Systems work can be used for social issues as well and aimed at everyone in society. Forming an education group and continuing this discussion would be highly informative. A course could be developed on safer complex systems. We need to be careful as Engineering X cannot take on the responsibility of solving this entirely and should work as an enabler to people and organisations of various backgrounds to contribute. Going forward, Engineering X could aim to consolidate on existing interventions, for example industry-academia partnerships in promoting best practices on safer complex systems.

5

Key points from the workshop

The following paragraphs group together the subjects that participants listed as their key points to emerge from the workshop.

5.1 Future work on system framework

The framework was considered to be a valuable resource. However, it has so far only been proven on a small subset of complex systems and it needs to be developed and tested on a wider variety of system types, while maintaining the view of it being a living thing that will continually evolve. Future work should be focused on the users of the framework in a practical environment, rather than an academic analysis of system descriptors.

The importance of the humans in the system came up frequently – in particular how to embed human and sociological issues into the analysis complex systems, without reverting to the 'human as a component' mentality. This is also an important diversity issue as not all humans will behave or think in the same way.

The framework has to accommodate systems that have fluid boundaries. In many systems, the governance layer can be a source of complexity and change, for example where outsourcing can change parameters over time due to commercial constraints.

Different sectors use different terms for (nearly) the same concepts. It is unreasonable to expect all users to switch to the same terminology and so a translation service will be needed. Some projects are turning to data science to help identify when people mean the same thing but call it something different.

Interdisciplinarity will be vital. As an example, the complex system that is COVID-19 transmission involved epidemiologists, behavioural scientists, sociologists, political advisors, economists, mathematicians, and many other disciplines. There are parallels with biological and ecological systems in their complexity and adaptation. There is also much to be done to get different subdisciplines of engineering to share their current tools and methodologies and translate them for use in other sectors.

5.2 Partners for Engineering X

There was enthusiasm for maintaining what one participant referred to as a 'transient alumni' model, based on the attendees of this and other workshops, so that we can continue to discuss recommendations and the Safer Complex Systems mission as they develop.

Safer Complex Systems is global in nature. There could usefully be more conversations with people in developing countries to understand what their engineering programmes are looking at (like energy access) and their priorities. Engineering X might consider partnering with those global organisations responsible for international standards such as IEC[22] and ISO[23] and ICOLD[24], as well as WFEO[25], which could help develop frameworks for cultural diversity in engineering. It is important to understand the focus of the partner and whether they are a potential contributor to Engineering X, a collaborator or simply recognised as another body working in the same space, with whom we exchange results.

At present, this group is dominated by UK academics. More diversity of thought might be achieved by partnering industrial organisations operating complex systems and other professional associations that have safety working groups. It would also be useful to have relations with legal bodies, such as the UK Law Commissions[26], and insurance bodies.

5.3 Case studies

There was an almost universal view that good case studies of successes and failures (from the recent past) could make a major difference to the understanding of the safety of complex systems. Case studies on business topics are widely used on MBA courses and are a good way of illustrating principles. A challenge with complex systems is the long feedback loops and their multifaceted nature – a classic narrative form often doesn't capture it. We might need a new style of case study and a new way of teaching them to better immerse people in them and learn from them. Perhaps we need to redesign the concept of a case study? This may be clearer after the present exercise to capture case studies is complete. In studies funded by Engineering X, we should try to align the case study with the York framework or use some other means to structure the case study to maximise learning.

Case studies are very useful in teaching – but it takes time to write them in useful detail as it is important to have the right information. It may be useful for some case studies to be segmented into: things known to the system, things unknown to the system, things unknown to the people designing the system. It would be particularly useful to have case studies of ad hoc or 'accidental' systems where there is no obvious duty holder. As part of a discussion on competences, education and capacity building, it was noted that creating a big open database of disasters, how they happened, how they could have been prevented and so on would be a challenge but would be very beneficial. There aren't many good examples of complex system-related studies. It is difficult to obtain quality case studies. It would be useful for the Academy to develop a database of these, which is open to all.

Aviation is often used as an example, but (if we ignore unplanned actions of the crew) it is a complicated system, not necessarily a complex system. A complex system will not always behave as expected and will respond to its context/environment. When coming up with examples we must be careful to define between the two – carefully articulate the different types of system and that we need different approaches to managing them. Also, every complex system is unique, no off-the-shelf solutions. We can learn from case studies but must not see them as templates into which we simply slot the new parameters.

5.4 Communications

Communicating the output of the Safer Complex Systems mission to target audiences is essential if it is to have an impact. Different communications and engagement plans are needed for different audiences, including the public. Several workshop groups recognised the importance of communicating the issues around the safety of complex systems to politicians and others in the governance layer.

Groups explored the role for communicators to the general public; the David Attenborough who gives a sensory experience or the David Spiegelhalter who articulates the risk. However, the gap in understanding how individuals respond to that type of stimulus is an area that isn't well understood.

There are many dimensions to this area – how can we articulate an agenda that other people can buy in to or that people from diverse perspectives can relate to? Is our role to communicate complexity or to explain that, because of complexity, unexpected things might happen from time to time? It is crucial to communicate across and outside of domains – even different categories of engineer speak different languages. The International Council on Systems Engineering (INCOSE) was suggested as an example of collaboration – they can coalesce around shared agenda to multiply effort with consistent focus. However, they do not have the diversity of potential audiences that Engineering X hopes to address.

A common language across sectors is useful to a point but we don't want it to inhibit people speaking about their experience, so translation is important – perhaps especially for the technology at the intersection of silos. Another powerful thought was how can we listen to the voices at the edges of the systems boundaries and between the layers? What can be done to enable that?

5.5 Definitions and measurement

Several groups became embroiled in confusion over definitions and the relationships between safety, resilience, robustness, efficiency, and antifragility for example. There are also questions, such as how to measure resilience or robustness. What does 'safety' mean in a food distribution system where a failed outcome is stunted development and ill-health?

This is an area where Engineering X could make a useful contribution. We need someone to produce a lexicon that analyses the various definitions and how they change across disciplines, from domain to domain, between academic study and for public usage and internationally.

5.6 Acceptable levels of risk

No groups came up with a formulation of the acceptability of risk. It is a difficult concept, even in a monoculture debating a known technology, with clear boundaries, under a monolithic governance structure[27]. Defining acceptable risk in an ad hoc complex system that affects a spectrum of communities is far more difficult. A term used in the workshop was *"acceptable risk is a social construct"*. It is also important to include the risk associated with not having the system at all rather than seeing the system risk as a linear choice. An imperfect system can still be much safer than doing nothing.

Engineering X could support a study to investigate the way in which people assess risks – including differences between regulators and the public. People have different perceptions between sectors, safety versus criticality, levels within an organisation or within a system. What is safe enough is closely linked to reliability and resilience. An evolution of crowdsourcing could be a way to democratise design and the review of decisions where no one group has control of a system.

5.7 Simulation and models

Most contributors said that models and simulations are valuable but all have limitations. Dynamism and fluid boundaries are difficult to incorporate. Models and simulations can be especially helpful at design stage. More important is to know the system well at the conceptual level. Top level ontology for data management could be helpful and should be included in research. The way that people act in the system is very important and needs to be factored in. Process calculus or game theory are possible avenues for this.

Different systems require different approaches to allow for adaptation to the dynamic nature of complex systems. Digitalisation is one means to exploit, but one of only a combination of tools. Model-based analysis by itself is not sufficient. It might be useful to look at models from banking and insurance sectors.

For all digital models, one must consider software safety issues, the coding community culture, cyber security and outcomes from coded processes. There are three dimensions of complexity that must be considered: temporal extent; physical extent; extent of complexity.

5.8 Competence, education and capacity building

Most groups thought that there are inadequate numbers of people who understand complex systems and that the education and training of engineers should include more material on complex systems. The teaching of how to bring diversity into thinking needs to happen earlier at university. The document defining the standards for UK engineers, UK -SPEC[28],states *"Chartered Engineers shall use a combination of general and specialist engineering knowledge and understanding to optimise the application of advanced and complex systems."* However, it appears that the requirement is more towards engineered systems, rather than the ad hoc systems that many engineers will meet in their professional life. But this does give Engineering X the opportunity to persuade accreditation bodies to increase students' background in complexity. There was enthusiasm for this to be an international activity, with a strong link into another Engineering X mission on Engineering Skills Where They are Most Needed.

The importance of the human in the design and analysis of complex systems remains, in most university courses, a final year option in academic teaching rather than a core competence. This needs to be given greater prominence. Could Engineering X take the initiative in putting together course materials to teach this more appropriately?

In countries that developed an engineering industry centuries ago, there is usually a culture of standards and procedures that registered engineers are expected to follow. In many developing countries there is not the same structure of professional standards and those that there are may be based on a colonial legacy that envisaged a different role for engineering. Engineering X could collaborate with alumni of this workshop who work in developing countries to create suitable standards.

Engineers are often only a minority of the people who become involved in the specification, design and operation of a complex system. There is a need for the directors of organisations and policy-makers in government to be aware of complexity itself and the risks it can generate and, in particular, of unaudited changes to the governance and management layers. Could Engineering X work with management schools to ensure MBA courses include a proper appreciation of complex systems?

It would be useful to produce guidance on how to assemble multidisciplinary teams. Diversity of teams and the diversity of thinking that comes from that is there in the structure. Some groups felt that diversity and inclusion was key to achieving safety and hoped this would come through strongly. This could be combined with work to enable voices that are not properly heard – for example junior employees or members of a team. The term maverick thinker was not widely supported but the concept of giving a voice to those who think differently was.

There will be a need for specialist engineers within an engineering team to design or operate a complex system. There will also be a need for generalist engineers who are capable of taking an overview of the engineering system and how it interfaces with people, organisations and other systems. These are skills of the generalist – people who see issues at the interface and ask the questions. Can we build this skillset in engineers more widely? We also need to embed a culture that sees questioning as supportive of the project, rather than as always trying to pick holes.

6

Conclusions and future work

The workshop did not include a final session, which discussed an agreed set of conclusions. The fact that the workshop ran in two consecutive half-day sessions also meant that somewhat different ground was covered in the two sessions. This section pulls together ideas that gained widespread support in the workshop. Several of them identify extremely difficult problems that justify further work.

6 Conclusions and future work

Building on the York report

This report is very useful. Further work is needed to test the relevance of the framework on non-engineered systems. There is also a need to expand the scope to cover anthropological and sociological aspects and for more social and behavioural issues to be taken into account when framing the risk. Security issues could usefully be included.

A lexicon of safety

There was confusion over definitions and the relationships between safety, resilience, robustness, efficiency, and antifragility for example, which are used differently in different sectors. There are also questions, such as how to measure resilience or robustness and how to factor in security associated with external malicious intent. Engineering X could support the production of a lexicon that analyses the various definitions, their usage in different environments and how they can be translated across disciplines, from domain to domain, between academic study and public usage and internationally. There is also still confusion over the differences between complex and complicated.

Acceptable levels of risk

None of the groups came up with a formulation of the acceptability of risk. Defining acceptable risk in an ad hoc complex system that affects a spectrum of communities is particularly difficult. Engineering X could support a study to investigate the way in which people view and assess risks, including differences between regulators and the public. What does 'safety' mean in, for example, a humanitarian system where a failed outcome is destitution, stunted development and ill-health? There is also a need to factor in the risk of the system versus the risk of 'doing nothing' – particularly important when the system is designed to counter pre-existing hazards. For many systems, quantitative measures of safety may not even be possible. If this is the case, should trust be the objective?

Regulating the safety of complex systems

Internationally, there are many different regimes for regulating the safety of hazardous situations. Most work adequately for well-understood hazards but can produce anomalous decisions for complex or unusual hazards and are poor at regulating low-probability, high-impact events. Are existing laws adequate and, if not, what changes are needed and how might complex systems be regulated?

Support for case studies

Good case studies of successes and failures could make a major difference to the understanding of the safety of complex systems. A challenge with complex systems is the long feedback loops and the interactions with humans in the system. A classic narrative form often doesn't capture it and so we might need a new style of case study and a new way of teaching them. Perhaps we need to redesign the concept of a case study or at least recraft the structure to enable maximum learning? In studies funded by Engineering X, it would be useful if authors could align the case study with the York framework and/or comment on the appropriateness of the framework for that study.

Diversity and inclusion

To ensure all aspects of a complex system are considered, a multidisciplinary team is needed. It is important to include people from different backgrounds and viewpoints – for example, giving a voice to occupants and users of a building, not only the owners and architects. Some of these groups will be uncomfortable with the terminology of risk analysis or expressing themselves in the erudite language often used by safety professionals. Organisations, and the professionals employed by them, need to develop means of communication that can be widely understood by diverse groups of people. Could Engineering X commission work on diverse team building and communication?

Education

Engineering and business degree courses are generally deficient in teaching complex systems: the courses have not kept up with the way the world has changed. It was suggested Engineering X could set up a *Safer Complex Systems Education and Training Group* to work towards an international programme of education. An understanding of complex systems is particularly important for policymakers who may determine the governance layer.

7

Annex A: Agenda

7 Annex A: Agenda

First workshop timings (BST)	Second workshop timings (BST)	Session
9.00am	**2.00pm**	**Welcome and introduction** Dame Judith Hackitt DBE FREng Professor Roger Kemp MBE FREng
9.15am	**2.15pm**	**Discussion one:** *To what extent have these two initial reports helped us on our journey to Safer Complex Systems?*
9.55am	**2.55pm**	**Discussion one feedback** Professor Roger Kemp MBE FREng
10.00am	**3.00pm**	**Discussion two:** *What are the priorities for further work?*
10.50am	**3.50pm**	**Comfort break**
11.00am	**4.00pm**	**Discussion two feedback**
11.30am	**4.30pm**	**Discussion three:** *What new ideas have the reports and workshop sparked?*
11.50am	**4.50pm**	**Closing remarks** Dame Judith Hackitt DBE FREng
12.00pm	**5.00pm**	**Workshop close**

8

Annex B: Team

8 Annex B: Team

Workshop Chair

- Dame Judith Hackitt DBE FREng
  Chair, Make UK

Workshop Convenor

- Professor Roger Kemp MBE FREng
  Emeritus Professor, Lancaster University

Workshop organisers

- Shelley Stromdale
  Programme Manager – Safer Complex Systems, Royal Academy of Engineering
- Nisa-Lin Croad
  Events Assistant, Royal Academy of Engineering

Facilitators and notetakers

- Robert Adediran
  Senior Manager – Diversity and Inclusion, Royal Academy of Engineering
- Hazel Ingham
  Programme Manager – Safer End of Engineered Life, Royal Academy of Engineering
- Dr Alex Smyth
  Senior Programme Manager – Positive Response, Royal Academy of Engineering
- Ben McAlinden
  International Partnerships Manager, Royal Academy of Engineering
- Marine Shah
  Senior Manager – Policy Centre, Royal Academy of Engineering
- Pippa Cox
  Communications Manager, Royal Academy of Engineering
- Dr Nick Starkey
  Policy Director, Royal Academy of Engineering
- Joy Aston
  Policy Officer – Research and Innovation, Royal Academy of Engineering
- Dr Andrew Chilvers
  Senior Policy Advisor, Royal Academy of Engineering
- Marie-Laure Hicks
  Policy Advisor – Research and Innovation, Royal Academy of Engineering
- Shaarad Sharma
  Senior Programme Manager – Engineering X, Royal Academy of Engineering
- Guy Paul
  Education Policy Assistant, Royal Academy of Engineering

Safer Complex Systems Board

- Dame Judith Hackitt DBE FREng
  Chair, Make UK
- Dr Jan Przydatek
  Director of Technologies, Lloyd's Register Foundation
- Edward Fort
  Global Head of Engineering Systems, Lloyd's Register
- Dr Nick Starkey
  Policy Director, Royal Academy of Engineering

9

Annex C: Participants

9 Annex C: Participants

Name	Organisation	Country of Residence
Corey Crawford	Alluvium House	United States
Dr Erin Chiou	Arizona State University	United States
Tim Chapman FREng	Arup	UK
Steve Yianni FREng	Association for Innovation, Research and Technology Organisations	UK
Professor Dawn Bonfield FREng	Aston University	UK
Angela Bines	BAE Systems	UK
Jane Fenn	BAE Systems	UK
Sarah Tricker	BAE Systems	UK
Dr Richard Judge	Bartlett Judge Associates	UK
Daniel Barlow	British Standards Institution	UK
Professor Jeremy Watson FREng	Building Research Establishment	UK
Dr Hussam Mahmoud	Colorado State University	United States
Andrew Wright	Constructive Collaboration	UK
Dr Antonio Pugliese	Cornell University	United States
Professor Helen Atkinson FREng	Cranfield University	UK
Emeritus Professor Philip John FREng	Cranfield University	UK
Professor Simon Pollard FREng	Cranfield University	UK
Roshni Prasad	Department for Business, Energy and Industrial Strategy	UK
Hannah Tooze	Department for Transport	UK
Dr Michael Do	Drexel University	United States
Professor Catherine Alexander	Durham University	UK
Wahidullah Azizi	Engineering X	UK
Dr Mark McBridge-Wright	EqualEngineers	UK
James Buckley	Expectation Coaching Inc	Canada
Claire Louise Travers	Field Ready	UK
Julie Pierce	Food Standards Agency	UK
Nic Holt FREng	Fujitsu	UK

Name	Organisation	Country of Residence
Professor Roderick Smith FREng	Future Rail Research Centre	UK
Dr Esra Albarahmieh	German Jordanian University	Jordan
Marissa Looby	Greater London Authority	UK
Dr Nick Shaw	Hazards Forum	UK
Captain Panos Stavrakakis	Health and Safety Executive	UK
Professor Guillermo Rein	Imperial College London	UK
Professor Atula Abeysekera	Imperial College London	UK
Professor Jennifer Whyte	Imperial College London	UK
Professor Rahul Nabar	Indian Institute of Technology Bombay	India
Apurba Kar	Indian Register of Shipping	India
Dr Zsuzsanna Gyenes	Institution of Chemical Engineers Safety Centre	UK
EUR ING David Eaton	Institution of Mechanical Engineers and Newcomen Society	UK
Kerry Lunney	International Council on Systems Engineering	Australia
Meaghan O'Neil	International Council on Systems Engineering – System Safety Working Group	UK/United States
Danielle Antonellis	Kindling	United States
Andrew Rose	Llanbury Consulting Ltd	UK
Dr Chris White	Lloyd's Register Foundation and Safer Complex Systems Advisory Group member	UK
Dr Jan Przydatek	Lloyd's Register Foundation and Safer Complex Systems Board member	UK
Dr Stefan Andreas Hoffmann	Manchester Institute of Biotechnology	UK
Patrick Mockridge	Metcalfe Energy	UK
Dr Sergio Alcocer	Mexican Academy of Engineering, US National Academy of Engineering	Mexico
Dr Aysegul Aksoy	Middle East Technical University	Turkey
Dr Nejan Huvaj Sarihan	Middle East Technical University	Turkey

Name	Organisation	Country of Residence
Sarah Knight	Ministry of Defence	UK
Professor Steve Gwynne	Movement Strategies	UK
Muir Macdonald FREng	muirmacdonald.com ltd	UK
Professor David Fisk FREng	National Infrastructure Commission	UK
Professor C. G. Koh	National University of Singapore	Singapore
Dr Bonnie Johnson	Naval Postgraduate School	United States
Dr Jay Sagin	Nazarbayev University	Kazakhstan
Brian Tomlinson	Network Rail	UK
Professor Peter Goodhew FREng	New Model in Technology and Engineering	UK
Dr William Earl Scott III	Newcastle University	UK
Wendy Middleton	Office for Product Safety and Standards, Department for Business, Energy and Industrial Strategy	UK
Dr Chris Elliott FREng	Pitchill	Switzerland
Dr Magda Osman	Queen Mary University of London	UK
Dr Andrew Clark	Royal Academy of Engineering	UK
Shane McHugh	Royal Academy of Engineering and Safer Complex Systems Advisory Group member	UK
Dr Michael Parsons	Safety-Critical Systems Club	UK
Claudia Rezende	SEIP 7	Brazil
Dr Diane T Finegood	Simon Fraser University	Canada
Professor Susan Gourvenec	Southampton Marine and Maritime Institute, University of Southampton	UK
William Miller	Stevens Institute of Technology	United States
Anne Wacera Wambugu	Strathmore Energy Research Centre	Kenya
Basil Mahfouz	SynSapien	UK/Beirut
Associate Professor Ali Mostafavi	Texas A&M University	United States
Dr Marilia Ramos	The B. John Garrick Institute for the Risk Sciences, University of California, Los Angeles	United States
James Knight	The Manufacturing Technology Centre	UK

Name	Organisation	Country of Residence
Dr Rania Aburamadan	The Middle East University	Jordan
Professor Jeffrey Johnson	The Open University	UK
Dr Isabel Hadley	TWI Ltd	UK
Dr Michael Dodge	TWI Ltd	UK
Dr Ujjwal Bharadwaj	TWI Ltd	UK
Professor Duncan Kemp	UK Ministry of Defence	UK
Professor Ramon Fernando Colmenares-Quintero	Universidad Cooperativa de Colombia	Colombia
Maria Alejandra Wilches Mogollon	Universidad de Los Andes	Colombia
Professor Liz Varga	University College London	UK
Dr Jing Xu	University College London	UK
Alberto David Inda Razo	University College London – Institute for Innovation and Public Purpose	Mexico
Professor Jonathan Dawes	University of Bath	UK
Professor Karen Yeung	University of Birmingham	UK
Dr Neil Carhart	University of Bristol	UK
Dr Kristen MacAskill	University of Cambridge	UK
Dr Manuel Herrera	University of Cambridge	UK
Professor John Clarkson FREng	University of Cambridge	UK
Dr Katherine Bloomfield	University of Hull	UK
Alexandra Bowring	University of Leeds	Ireland
Steve Brewer	University of Lincoln	UK
Dr Michael Humann	University of Liverpool	UK
Dr Richard Kirkham	University of Manchester	UK
Professor Joachim Sturmberg	University of Newcastle	Australia
Professor Gary Burnett	University of Nottingham	UK
Professor Timothy Denison	University of Oxford	UK
Dr Ogheneruona Endurance Diemuodeke	University of Port Harcourt	Nigeria
Dr James Chakwizira	University of Venda	South Africa
Professor Carsten Maple	University of Warwick	UK

Name	Organisation	Country of Residence
Dr Markus Andreas Kirkilionis	University of Warwick	UK
Professor John McDermid FREng	University of York	UK
Dr Philip Garnett	University of York	UK
Professor Simon Burton	University of York	Germany
Dr Rob Weaver	University of York and Rob Weaver Advisory	China
Dr Jeffrey Hudack	US Air Force Research Laboratory	United States
Dr Guru Madhavan	US National Academy of Engineering	United States
Dr Valentina Donzella	WMG, University of Warwick	UK
Dr Siddartha Khastgir	WMG, University of Warwick	UK
Dr Marlene Kanga	World Federation of Engineering Organisations (WFEO)	Australia
Dr Mikela Chatzimichailidou	WSP UK and HS2	UK

References

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

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

[3] 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, pp.673–692. New York, NY, USA: Cambridge University Press.

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

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

[6] An example is the difference between cockpit hierarchy in JAL and Virgin – the latter having a much less strict hierarchy.

[7] Disability-Adjusted Life Year (DALY)

[8] See, for example, Loss of Control and Impact with Pacific Ocean, Alaska Airlines Flight 261, McDonnell Douglas MD-83, N963AS, About 2.7 Miles North of Anacapa Island, California, United States National Transportation Safety Board, 2003

[9] See, for example, the interlinking of systems in Living without electricity, Royal Academy of Engineering, 2016.

[10] FTA – Fault Tree Analysis; FMECA – Failure Mode, Effects and Criticality Analysis

[11] HAZOP – Hazard and Operability Study; HAZAN – Hazard Analysis; HAZID – Hazard Identification; STAMP – System-Theoretic Accident Model and Processes

[12] Report of Investigation into the Circumstances Surrounding the Explosion, Fire, Sinking and Loss of Eleven Crew Members Aboard the Mobile Offshore Drilling Unit Deepwater Horizon, United States Coast Guard, 2011

[13] Final committee report: the design, development & certification of the Boeing 737 max, The House Committee on Transportation and Infrastructure, 2020

[14] What Sidney Dekker referred to as Drift into Failure; ISBN 978-1-4094-2221-1, Ashgate, 2011

[15] Kemp RJ; Regulating the safety of autonomous vehicles using artificial intelligence. Communications Law (ISSN 17467616) Vol. 24, No. 1, 2019.

[16] It is possible that these sophisticated communication skills will not be found within engineering companies, however there are many community engagement methodologies that have a good track record over many years, which could be adopted or adapted.

[17] What Eric Hollnagel describes as including both positive and negative outcomes, unlike the traditional risk matrix that only considers the latter. Resilience Engineering in Practice, ISBN 978-1-4094-1035-5, Ashgate, 2011

[18] See, for example, Business re-engineering and health and safety management: Best practice model, HSE CRR96123, UK

[19] The UK Standard for Professional Engineering Competence and Commitment (UK-SPEC), 4th edition, Engineering Council, August 2020

[20] See www.futurelearn.com/partners/unesco-unitwin-complex-systems-digital-campus

[21] Description from Wikipedia

[22] The IEC (International Electrotechnical Commission) is the world's leading organisation that prepares and publishes International Standards for all electrical, electronic and related technologies.

[23] The International Standards Organisation ISO is an independent, non-governmental international organisation with a membership of 165 national standards bodies. Many national standards are aligned with both the IEC and the ISO through networks of overlapping committees.

[24] International Commission on Large Dams (ICOLD) is an international non-governmental organisation dedicated to the sharing of professional information and knowledge of the design, construction, maintenance, and impact of large dams.

[25] The World Federation of Engineering Organizations (WFEO) is the international organisation for the engineering profession. Founded in 1968, under the auspices of UNESCO, WFEO brings together national engineering institutions from some 100 nations and represents more than 30 million engineers.

[26] The Centre for Connected and Autonomous Vehicles (CCAV) has asked the Law Commission of England and Wales and the Scottish Law Commission to undertake a far-reaching review of the legal framework for automated vehicles, and their use as part of public transport networks and on-demand passenger services.

[27] The tolerability of risk from nuclear power stations, HSE 1988, revised 1992.

[28] The UK Standard for Professional Engineering Competence and Commitment (UK-SPEC), 4th edition, Engineering Council, August 2020

Open Source