Management and Oversight of Complex Systems Seminar Report



The SCSC held this Seminar on Thursday 3rd December 2020. Unfortunately, given the ongoing COVID-19 pandemic, this event (like many others this year), had to be held over ZOOM rather than the physical face-to-face gatherings to which we were all previously accustomed. But despite the lack of cake and coffee, the presentation was very well attended online, with around 45 attendees drawn from a variety of industry sectors and of course academia.

Background

This seminar was aimed at those who have some involvement in the management, approval, regulation or operation of complex systems that have a safety aspect, for example Air Traffic Control systems, Nuclear Plant, Military Vessels or Power Transmission systems.

Complex systems have behaviours that are emergent properties of the interactions between the parts of the system, which are not apparent from knowledge of those parts and their interactions alone. By this definition, many modern safety-critical, socio-technical systems, for example healthcare and transport, are also complex. As well as emergent properties, complex systems have other defining characteristics such as dynamic and ill-defined boundaries (the scope of the system can change) and tipping points (the behaviour of a system can change suddenly). Complexity therefore provides challenges for safety engineering and management – for example, safety engineering normally starts by defining the system boundary.

The Seminar

SCSC Lead – Mike Parsons opened the seminar and presented the outline agenda. The Seminar itself comprised three short presentations with a follow-on wrap up session after each to address questions arising from the attendees. Mark Nicholson then presented a final wash-up session at the end of the afternoon.

The rationale for holding the seminar is that it is obvious that so many systems are becoming more complicated. Everything is much more connected and there is less isolation. Legacy systems that were originally designed to be standalone are now being interconnected.

There is often lots of software integrated into these systems that is continually being updated. Therefore, interaction between components is often difficult to predict with any certainty.

The situation is likely to become even more complicated by the development of autonomous vehicles whose system boundary may be difficult to clearly define – we cannot predict with certainty which roads will be taken down or what obstacles/incidents such vehicles will encounter.

The recent COVID-19 outbreak and the very complex logistical task of a vaccination roll-out programme probably demands application of systems thinking.

A Framework for Governance and Management of the Safety of Complex Systems

John McDermid, University of York presented a three-layer framework which has been developed as part of a study funded under the Lloyds Register Foundation/Royal Academy of Engineering Safer Complex Systems Programme. The framework considers drivers of complexity, systemic failures, exacerbating factors and controls to reduce the risks arising from complexity (as opposed to the normal focus of safety engineering on "failures").

John outlined the basis of the Framework which originates from a short study funded by the Royal Academy of Engineering known as 'Engineering X'. The study itself consisted of a project team (four people) with John responsible for delivery of the programme overall.

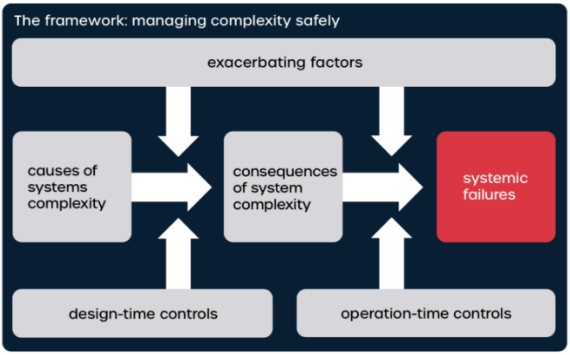
The project aim was to develop conceptual clarity around what is meant by 'Safer Complex Systems' by producing a framework that supported a common way to communicate about the safety of complex systems across sectors and between different levels of expertise.

John began by identifying the nine 'characteristics of complex systems' including Unity, Emergence, Semi-Permeable Boundary and Non-Linearity.

The essence of the Framework subsequently presented was the concept of a three-layer model comprising Governance, Management and Task & Technical.

- **Governance** being the cross-jurisdictional incentives and requirements for organisations to adhere to best practice through direction regulation
- **Management** being risk management and informed design trade-offs (supply chain dynamics and the sustainment of long-term institutional knowledge for long-lived and evolved systems)

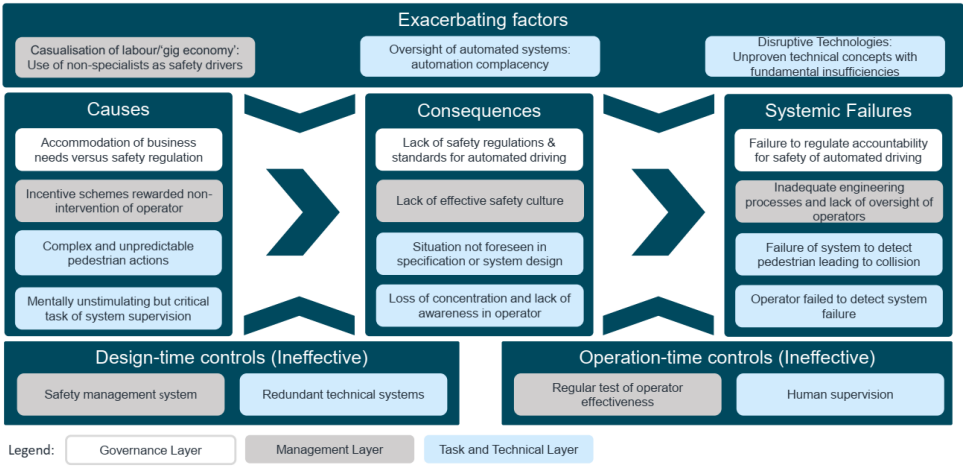
- **Task & Technical** being the technological components and tasks by the users, operators and stakeholders within a socio-technical context.



Given Safety comprises Causes, Consequences and Controls that culminate to produce 'systemic failures', John presented a series of slides which in-turn 'overlayed' this Framework on to each of these components and interactions to identify topics of concern.

Using the framework it is possible to identify potential 'causes of complexity' not just consider actual failures, and the resulting consequences.

John gave several examples of applying the framework to real-life incidents such as the Boeing 737 Max and a NATS outage in the Aerospace sector, and also in the Automotive Sector with the Uber Tempe incident analysis as follows:



John wrapped up the presentation by looking at the conclusions from the study.

It is clear the Framework has many new domain applications including Urban Air Mobility, Automated Lane Keeping Systems (ALKS) and integration of such systems with Smart Motorways etc.

"technology moves far faster than the regulators can"

The Framework produced is an initial output from the Safer Complex Systems programme. Largely descriptive but can help take a holistic view, and is rich enough to support expert workshops.

Areas for future work are as follows:

- Refinement of the framework and guidance in its use
- Extending to include existing analysis methods, STAMP/SPTA etc.
- Better reflection of interdependencies (true complexity)
- Better treatment of human-system interactions
- Needs more usage to refine and mature
- Explore more successes not just the failures – which controls are the most effective?

Type 23 Frigates

James Maltby from BAE Systems focused on the different challenges posed for the management of safety on complex warships such as the Type 23 Frigate. James is based with BAE Systems Maritime Services who operate out of two Naval Bases at HMNB Portsmouth and Devonport.

These facilities are physically huge with a large number of personnel supporting approximately 70% of the Royal Navy surface ships currently in-service including the Type 23 Frigate, QEC, River Class Batch 1 OPV, Hunt Class MCNV, River Class Batch 2 OPV and Type 45 Destroyer.

For the Type 23 Frigate, there are 13 ships in this Class. Support for the vessels is delivered as an Alliance split between the Portsmouth and Devonport sites. That Alliance includes BAE Systems, Babcock International and the UK Ministry of Defence (MoD).

Each vessel is an incredibly complex piece of engineering, with many sub-systems providing many different functions with equipment sourced and integrated from multiple suppliers.

The Type 23 Frigate incorporates a mix of both 'tangible' and 'intangible' products. Tangible products being defined as physical items of equipment and kit to be installed on to the platform; and intangible products being the provision of service for installing and maintaining that equipment.

The Service Provision identifies the agreed level of safety through identification of activities that could possibly cause harm. It also identifies responsibilities for safety delegation and the assurance processes. The focus is understanding how service outputs might deviate from the required condition or quality necessary to maintain safety. The company mitigates these through a rigorously defined business processes and assurance to ensure integrity is delivered.

Classical techniques such as implementation of a Risk Register and Hazard Log are used to manage safety through the agreed documented processes, with a strong emphasis on learning from experience to improve process. This is supplemented throughout the installation process by integral design reviews and safety assessments, inspections and trials.

For the Type 23 vessel, the original design of the ship dates back to the late 1980s, consequently there are subtle variations and deviations found in the build standard across the fleet. These variations make a traditional safety case more challenging to present, but the aim is to bring all vessels toward a common standard. The integration is often further complicated with legacy equipment that may not have a contemporary safety case in existence.

Managing Operational Safety in a Large, Complex Airline

Adam Johns from KeolisAmey Docklands (and ex-Cathay Pacific Airways), presented the challenges of managing operational safety in a large, complex airline, that has adopted concepts around complex systems, systems thinking and contemporary safety science to enhance their understanding of normal operations.

Adam's background is principally from the aerospace domain (Teledyne Controls, Virgin Atlantic, CAA) but mostly recently he has become involved with Operational Health & Safety on the KeolisAmey Docklands light railway in London.

Cathay Pacific Airways is a large operation with approx. 200 aircraft, 180,000 flights per year with over 100 worldwide destinations. Cathay Pacific partition their business operation into five distinct areas: Flight Operations, Cabin Operations, Engineering, Ground Operations and Cargo, all of which are overseen by a Corporate Safety group under the Executive and Operations leadership.

Adam presented an engaging animated slide illustrating three mechanical cogs to represent the core elements of their Safety Management System: hazard identification, risk analysis & assessment and mitigation of risk by management – all underpinned by a 'just reporting culture'.

The presentation summarised the differences between Safety-I and Safety-II concepts. Safety-I tends to focus on accidents, incidents and near-misses, compared to Safety-II, which focuses on analysing everyday actions and their outcomes – to identify those events whose outcomes ended well and to understand the reasons why failure was averted.

Cathay-Pacific adopted the Safety-II culture and began to socialise new ideas by hosting a series of regular short safety presentations on bite size chunks of topics to encourage staff throughout the organisation to embrace and discuss safety openness.

"Make everyday work your unit of analysis, not just adverse outcomes"

Adam outlined the differences between 'complicated' systems and 'complex' systems. Essentially, the definition given of a complicated system being one that is technical/mechanical, static, linear, predictable, well-defined boundary etc – a jet engine was given as the example. Complex systems on the other hand include the human interaction element, so by definition are socio-technical, dynamic, non-linear, unpredictable, infinite etc – jet engine maintenance was given as the example.

Safety becomes an emergent property of the complex system of engine maintenance; but it is not the only interaction of concern since a given 'worker' interfaces with many different elements within the organisation. This can highlight discrepancies between 'work-as-imagined', the 'work-as-prescribed' and the actual 'work-as-done' offering the opportunity to identify risks to mitigate.

As a result of the safety briefings, Cathay Pacific introduced the Operational Learning Review (OLR). OLRs take a systems approach to ensure learning and improvement are the sole objectives, not to identify blame. They are designed to help people identify where work went well and why, to highlight recommendations in working practices that can be fed back into the process.

Report by Andy Williams