SSS'22 Event Report



The symposium had a special flavour this year, celebrating the club's successes over the years and giving a taste of what the next 30 years in safety engineering might be like. After being forced to run entirely online last year, the Safety-Critical Systems Club's annual Symposium finally returned to an in-person event hosted at the Bristol Royal Marriott in February. This was a blended event with significant online attendance, and a mix of physical and virtual presentations – the first symposium of its kind in the club's 30-year history.

The outbreak of the Covid-19 Omicron variant towards the end of 2021 certainly put the event in jeopardy, and it was only in January 2022 that a firm decision was made to go ahead with the event. Despite the uncertainties, the event was remarkably well-attended, with approximately 120 delegates being split equally between in-person and online attendees.



Neither did circumstances detract from the quality of the presentations with excellent talks being covered in areas such as new techniques and applications, human factors, assurance, autonomy, healthcare and safety & security integration.

There was also a bumper pack of merchandise and publications for those attending in person – as well as the symposium proceedings, there were several working group guidance publications, the Feb 2022 edition of the SCSC Newsletter, the 2021 annual compendium of newsletters, and the 30 Years of Safety Systems, which included a selection of important articles published in the Newsletter over the last 30 years, with additional commentary and postscripts from some of the original authors.

Shaping the Evolution of Safety Engineering



Professor John McDermid, Director of Assuring Autonomy International Programme at the University of York opened the conference with a talk on the future evolution of safety engineering. He introduced three concepts that have a bearing on system safety: Consumerism, Contradictions and Counterfactuals:

- Consumerism: eg. public buying power can influence the products in the marketplace, but these might not be the safest or most environmentally friendly
- Contradictions: eg. cars are considered safe and widespread, but contribute to other "Excess Deaths" through air pollution
- Counterfactuals: eg. Assessing the potentially incommensurable benefits and harms that would arise if an event had, or had not, occurred.

John said that safety engineering needs to look at taking a wider stance, to consider not just the technical aspects of safety, but also to incorporate the benefits and harms to individual, society and the environment. The growing complexity and autonomy of AI and ML poses huge challenges to safety engineering and there is a need to develop new techniques and extend existing ones. John provided some examples, such as extending safety arguments to include an ethical argument, methods for measuring and comparing complex systems and the use of digital twins in exploring counterfactuals.

John concluded that safety engineering is at a crossroads, both technically and politically. Technically from the need to broaden the discipline and consider ethics and sustainability and politically, seeking to raise awareness and influence policy through the mantra of "Safe, Ethnical and Sustainable".

Stories and narratives in safety engineering



Catherine Menon, Principal Lecturer at the University of Hertfordshire, illustrated the role of storytelling in constructing the narrative for a safety case. Through a brief retelling of the Hansel and Gretel tale, she illustrated how a story can have many different meanings and how different interpretations can be drawn.

Catherine gave Use Cases as a common form of narrative and described these as "fluffy white clouds", where everything works as planned and as expected. However, in real life, things go wrong and a narrative could also be in the form of "war stories" or "black clouds". Catherine asked what narrative form a Safety argument should take, and argued that a claim that a system is safe is actually a "white cloud" narrative, for example, it may not place a focus on counter-evidence and lack of traceability or rigour.

Other forms, such as justifying the author's decision that the system is safe, tend more to the opposite "black cloud" style of argumentation. Catherine said that a safety argument should be more about exploration, open to the possibility that it may or may not be safe, with the reader and writer working together to explain, not justify.

The readership of the safety case is also diverse, for example, it could be other engineers, regulators, users, or the general public and so needs to be framed in a way that they will understand. In particular, the way we communicate to the public can encourage them to think in particular ways eg. The aircraft landing in the Hudson is presented as a triumph in contrast to the Nimrod accident report that apportioned individual and collective responsibility.

Catherine warned about the pitfalls of storytelling and how powerful stories can be, as people can believe emotions over facts. She illustrated this through references to a legal case and other safety-related accidents where, how the story was told, led to a disproportionate allocation of blame to those involved.

She concluded by saying that we should still tell stories, but we should tell those stories safely.

30 Years of Safety Quiz



The first day concluded with a special 30th Anniversary Quiz hosted by Catherine Menon and Paul Hampton. The quiz comprised 19 questions on all matters to do with system safety and the SCSC, and was open to both in-person and online attendees working individually or in teams.

Questions were wide ranging from anagram solving, picture questions, multiple choice and concluded with a challenge for contestants to create a Limerick or Haiku.

Examples of some of the contributions are as follows:

Limericks

There once was a safety engineer,
Who lived life constantly in fear.
His friends all laughed,
And said he was daft,
"Stop stressing and drink lots of beer!"

There once was a girl called Stacy,
Who had a complete disregard for safety.
She chased all sorts of thrills,
With things that could kill,
And no one has seen her lately.

Haiku

Safety fans beware
Incidents are everywhere
Common sense is rare

Blossoms are falling
So is the plane I am on
Safety case was wrong

The winners of the quiz were Dewi Daniels and Roger Rivett with 66 out of 104.

You can try the quiz by following this link: https://scsc.uk/re797.24.

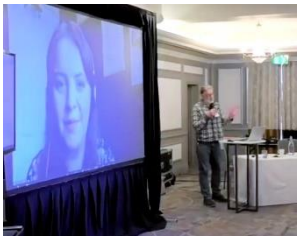
Answers can be found here: https://scsc.uk/re797.25

Events



As well as a number of ad-hoc events organised by delegates themselves through the Whova app, an organised tour of Bristol was arranged for delegates on Wednesday morning. This was a walking tour and took in some of the sights of Bristol such as the Bristol old Vic and Bristol Cathedral.

Ethics and Safety for Connected and Automated Vehicles



Paula Palade, from Jaguar Land Rover, discussed the status of various reference frameworks that are being developed to cover the ethics of Connected and Autonomous Vehicles (CAVs). One such framework was funded by the European Commission and Paula, as a member of an independent expert group developed 20 recommendations on road safety, privacy, fairness, explainability and responsibility. The purpose of the report was to explore some important questions:

- How safe should CAVs be?
- Are pedestrians and cyclists more at risk with CAVs in traffic?
- Do you need to understand the technology behind it?
- What kind of data will a CAV share?
- Can the decisions of a CAV be trusted?
- Who is responsible for its behaviour?



The report provided 20 new recommendations for a safe and ethical transition towards driverless mobility. Each recommendation was accompanied by more specific guidance, and Paula illustrated this by discussing some of the recommendations in more detail – for example:

- **Recommendation 1:** Ensure that CAVs reduce physical harm to people. The report recommended that data and statistics around collisions and near misses should be widely shared as there is usually lack of details about the exact circumstances of a collision and events are rare;
- **Recommendation 2:** Prevent unsafe use by inherently safe design. Manufacturers, deployers, together with researchers, should create intuitive, user-centred systems that are designed to prevent unsafe use.
- **Recommendation 3:** Define clear standards for responsible open road testing. A comprehensive and rigorous framework for open road testing would be most appropriately addressed at European level.
- **Recommendation 4:** When to break the rules… In some cases it may be safer to allow the CAV to break the road rules eg. to mount the pavement to allow an emergency vehicle to pass. Paula referred to promising work in this area using "ethical goal functions" as part of a hybrid AI system.

Paula also touched on other security related aspects, such as, issues around data privacy where many vehicle systems will store personal data that may be accessible by 3rd parties, and systems that may use a driver's behavioural and movement patterns for commercial gain.

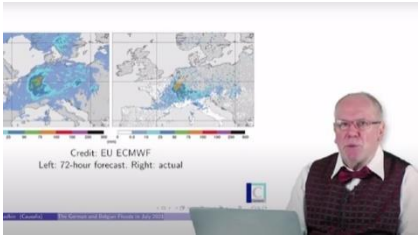
Paula concluded by referencing IEEE Std 7000-2021: *Standard Model Process for Addressing Ethical Concerns during System Design,* and said this gives a high-level view of how to include ethical considerations in the design process, but lacks the linkage to how to translate ethics into actual non-functional requirements. She said that *BS ISO 39003 Road Traffic Safety (RTS) – Guidance on safety ethical considerations for autonomous vehicles* is currently in development and is intending to provide more detail in this area.

The report itself can be download from: https://europa.eu/!VV67my

The German and Belgian Floods

Peter Ladkin of Causalis, concluded the second day with a virtual presentation on the exceptional flooding that occurred in July 2021 that claimed the lives of over 220 German and Belgian citizens and caused over 33 billion Euros of damage.

Peter said the primary issue was that the "problem" rivers had large catchments in mountainous areas and flowed down into populated high-sided valleys. There were also problems even on flat land with human activities worsening the effects with "sealed soil" (tarmacked and built-up areas) and also in one case, a gravel pit excavation was suspected of leading to subsidence and landslide.



The floods were predicted 3 days in advance but the location of rainfall is not generally predictable to within 100km, and the predicted rainfall in some locations was as wide as 20mm-150mm.

Peter highlighted that one of the problems was on communication as some people were not aware of the severity of the floods in time to be effectively evacuated. He noted that the communication and disaster response is set along a political organisational hierarchy and not one better suited to disaster alerting and response. Peter suggested a different organisational model that might improve the management of such disasters and suggested that this model (which would require a change in German law) may have led to a quicker response and hence, better outcomes from the flooding that took place.

Peter concluded with some suggestions on improving outcomes from such events such as:

- education and training for residents
- local coordination and organisation of physical-aid
- rethinking approaches to "sealed soil" and ultimately
- arresting climate change to reduce occurrences of these types of extreme weather events.

Introducing a Restorative Just Culture and the Learning Review at the Docklands Light Railway



Adam Johns is a Senior Health & Safety Coach at Keolis Amey Docklands, franchise operator of the London Docklands Light Railway (DLR).

Adam said that when it comes to safety on the front line, many organisations are poor at learning from incidents as they do not treat the people involved in the right way to get the right sort of information from them to promote learning.

Adam provided an overview of the DLR – an automated light railway that has multiple different lines but is not fully automated – it has an attendant on board to operate the doors and deal with passenger issues.

Adam said that in 2019 as a result of a number of safety culture surveys, the organisation thought its safety culture was static and not progressing. A new Safety Director embarked on a programme called "Next Platform" to implement a revised safety approach based on Sidney Dekker's "Safety Differently" concepts. Next Platform's initial three phase are:

- **To change the conversation**: adopting a different non-pejorative and neutral language for safety (for example, "investigations" become "learning reviews", "incidents" are "events", "findings" are "learning", "non-compliance" is "variation" etc.)
- **Change the approach**: introducing new processes and tools & techniques
- **Change the outcome**: a longer term objective to improve safety, system performance and human well-being

Features of the programme are that it is:

- Additive – to augment existing H&S systems
- A person-centred approach
- Aiming to redefine safety as the presence of positives, not the absence of negatives
- Focus on understanding decision making rather than punishing non-compliance
- Ultimately to improve performance through enhanced learning

Adam introduced the concept of "Restorative Just Culture" focussed on restoring trust, confidence and everyone's well-being following an incident, rather than seeking someone to blame. With this, traditional safety investigations are replaced with "Learning Reviews" where attention is given to "sensemaking" – understanding the point of view and perspective of the people involved and the thinking around the actions they took.

Thirty years of learning by accident

Graham Braithwaite, Director of Transport Systems and Professor of safety and accident investigation at Cranfield University reflected on the last three decades of system safety, which also coincided with his career in safety. Graham said that when he started out as a student, the UK transport sector was still reeling from major disasters such as the Herald of Free Enterprise at Zeebrugge, British Midland at Kegworth, and the Clapham Junction and Purley rail accidents. On one level, such events galvanised resolve to prevent such events from recurring, but on the other, it showed that there was also a level of risk acceptance that thankfully is no longer the case.

Graham went on to discuss the progress that has been made and said that the accident record demonstrates that a huge amount has been achieved. He said the role of "systems thinking" has been highly significant, not least in helping to understand the complexities of accident causation and the myriad influences on safety performance, both good and bad.

Milestone accidents have been major drivers for improved safety, but this reactive approach has also been increasingly supplemented by more proactive systems thinking, and safety science has evolved as our understanding of technical failures, human performance and organisational influences have advanced. Many new systems have been introduced, such as proximity warning systems that have improved safety, but they come at a cost of increasing complexity and opacity where operators, who are called upon more rarely in critical situations, have even less experience of dealing with them.

Graham also mentioned how the pandemic has had a complex effect on safety management, for example, maintaining recency of flight experience of pilots and even the infestation of insects in pitot tubes in grounded aircraft.

Milestone accidents which have taken place over that period remind us however, that progress has often come at the price of lives lost and property or environmental damage.

Graham covered the challenges of future flight and the race to meet the environmental challenges for aviation, not only in developing new fuel technologies but also in ensuring that novel solutions remain safe. For example, air mobility solutions have myriad issues with regards to new regulations, technology, operational, air traffic management and social acceptability. Graham said that there is now unprecedented change underway with many new disruptive technologies and many new players with novel societal impacts.

Graham concluded that the safety community has never been more important both now and in the future.

"Cowboy digital" undermines safety-critical systems



Prof. Harold Thimbleby, See Change Fellow in Digital Health, based at the University of Swansea discussed the prevalence of what he called "Digital Cowboy" programmers, who produce software that has little consideration to the safety implications of failure.

He illustrated this first by showing a poorly wired extension lead that he was PAT testing, which although appearing to work well, contained a hidden and potentially life-threatening fault.

His next example was an RCD tester that had a programmed but undocumented (invisible) feature that had resulted in readings that were erroneous and hence unsafe, for example, it registered a reading for 50V on a live circuit that was actually closer to 240V. As with the previous example, the system appears to be working when it fact it is in an unsafe state.

Another example he gave was a high-end domestic coffee machine that was physically well-made but had "Cowboy software engineering" as evidenced from its user interface; with confusing placement of a decimal point in a temperature reading to indicate which of the machine's two boilers was being measured.

Harold finally presented an example from the Healthcare domain where a system was being showcased for perinatal care but carried a disclaimer that it was not intended for diagnosis or treatment decisions. Harold said that this would not be permitted in Aviation systems like jet engines, but it is widely tolerated elsewhere as seen from the previous examples. Harold concluded with a final call that as an industry "we must do better".

At the interface of engineering safety and cyber security

Dr Reuben McDonald is Head of System Safety, Security & Interoperability at High Speed Two (HS2) Ltd, which is building a new high speed railway connecting towns in the South, Midlands and North of England. Reuben said that a modern railway is a highly electrotechnical system with connectivity and networks inherent in its design. For High Speed 2 this means a design which is based on a confluence of different wired and wireless networks. These networks support the delivery of safety critical, safety related, operation critical and wider business functions.

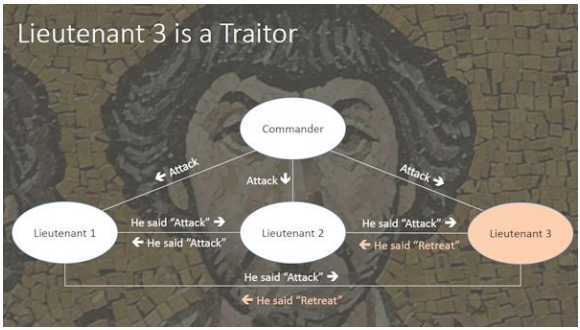
His talk explained how HS2 is assessing its safety and cyber risks in an efficient manner, leveraging products and assessments from the application of the Common Safety Method on Risk Assessment to support cyber assessments based around IEC 62443 risk methodology and associated control.

What do Byzantine Generals and Airbus airliners have in common?

Dewi Daniels from Software Safety Ltd, first described the events surrounding a China Airline's flight involving an Airbus A330 in 2020. During the routine landing, all three primary flight control computers shutdown causing several systems to become unresponsive, such as the spoiler deployment, reverse thrust and auto-brake. Both pilots were then forced to manually brake the aircraft, which eventually stopped just short of the end of the runway.

Dewi went on to explain the architecture of the flight control systems where each of the flight control computers has an independent (and diversely developed) monitor that can shut down the computer if processing outputs disagree.

In the Air China incident, all three computers failed and Dewi drew parallels between this failure and the "Byzantine General Problem". In the Byzantine General Problem, a General in charge of several Lieutenants must get agreement on common actions amongst the lieutenants for the overall campaign to be successful.



However, one of the commanders is unreliable and so may send misleading messages to the other commanders to sabotage the campaign. Dewi said that the well-known computer scientist, Leslie Lamport, wrote a paper in 1982 describing a solution to this form of problem where each Lieutenant cross-checks the General's instructions with each other to discover the unreliable Lieutenant.

Dewi then likened this to a 2 out of 3 voting system where the same input is given to 3 separate processors and results from each compared. Failures of one of the processing units can then be detected by the other two, which would share a common output value.

While this gives added resilience for individual processing unit failures, it does not help when the inputs are erroneous to start with, and this is what happened in the Air China incident – Weight on Wheels signal fluctuation, the pilot moving the rudder pedal and clock drift, meant that the monitors calculated different values from the main processors and shutdown all computers within the space of a second.

Thought for the Symposium

Tim Kelly from the Church of England and former Managing Director of the SCSC, concluded the event with his "Thought for the Symposium". You can find the full transcript of his talk on page 37.

Banquet



Despite reduced numbers, the traditional evening banquet was a huge success with not one, but two, speakers during the evening. Wendy Owen gave an excellent pre-dinner speech where she discussed her involvement and experiences with co-authoring the "30 Years of Safety Systems" book. Wendy's talk is reproduced in full on page 33.

We then had our first ever virtual after-dinner talk from Tom Anderson, former Managing Director of the SCSC. Tom's entertaining talk discussed the lessons he'd learnt on how to give after-dinner talks after listening to 30 years of after-dinner speakers. Such lessons were: "Brevity is the soul of wit" and quoting Tom Lehrer: "Plagiarise, plagiarise, let no one else's work evade your eyes, but please call it research!"

On a more serious note, he shared the economist Tim Harford's concerns around "Motivated Reasoning" (similar to "Policy-based Evidence" and "Confirmation Bias") – finding facts and seeking experts that support your claim.

Tom concluded with reference to one of the quiz questions in which he had featured – asking whether he was famous for reciting the Robert Burns poem "Tam O'Shanter". In lieu of reciting all 200 lines of the poem, Tom gave an amusing summary of the poem, and with its final message to be wary of the costs incurred "Whene'er to Drink you are inclin'd", he toasted the Pearl anniversary of the club with a glass of Scotch Whisky!

Report by Paul Hampton, SCSC Newsletter Editor