SSS'26 Event Report

The Safety-Critical Systems Club's annual Symposium returned in February 2026 for another fully in-person event hosted at The Milner Hotel, York. Paul Hampton, the SCSC Newsletter Editor, provides highlights from the three-day event.

With almost 200 attendees, this year's event was one of the largest ever since its inception. There was a fabulous range of talks over three days covering Uncrewed Aircraft Systems, Addressing Complexity, AI & Autonomy and New Approaches as well as many workshops and tutorials and poster sessions. In particular, the second day's parallel streams provided a huge amount of additional and diverse content and all sessions were well-attended. Here are some highlights of the keynote talks and a summary of other significant events that took place during the week.

Staying safe from flying killer robots

Steve Wright's talk focused on defending against hostile drones, drawing from his 35 years of experience in avionics and aircraft systems. He contrasted his previous work in civil aviation safety (with mature, incremental development and one-in-a-billion failure rates) with the current drone threat environment (with 10% failure rates and technology obsolescence measured in months rather than decades).

He discussed two main types of battlefield drones: small, rotor-powered electric drones and larger long-range winged vehicles with ranges of hundreds of miles.

He provided three case study examples: the 2019 Abqaiq-Khurais attack in Saudi Arabia, the 2023 Moscow attacks and Operation Spiderweb in 2025, which involved simultaneous attacks on five distant Russian locations using over 100 Uncrewed Aircraft Vehicles (UAVs).

Steve emphasised that there is no single solution to drone defence – instead, a "defence in depth" approach is needed with multiple protective layers at different ranges:

- 100+ kms: Fighter jets with missiles (very expensive)
- 10-1 kms: Counter-drones and electronic countermeasures
- Sub-1 km: Directed energy weapons, guns and electromagnetic pulses
- Final meters: Netting, barricades, and shotguns

He highlighted a concerning paradox: as the threat gets closer and risk increases, current defensive technology becomes less sophisticated and cheaper, which is the inverse of conventional safety paradigms where higher risk should warrant greater investment.

Looking forward, Steve predicted drones will become faster, more agile, more autonomous, and deployed in much larger numbers (potentially thousands in single attacks). He concluded that while safety expectations from traditional aviation are unattainable in this environment, the same safety engineering principles of defence in depth, redundancy and flexibility remain relevant.

Armchair Chat

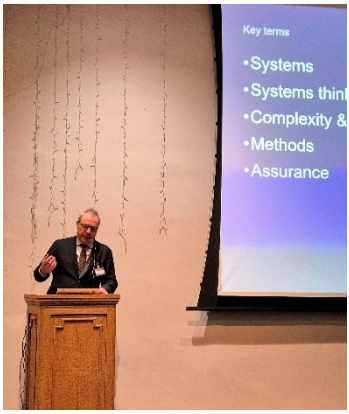
Our first Armchair Chat was with Karin Rudolph (Founder of Collective Intelligence UK) interviewing Mikela Chatzimichailidou (Professor of System Safety and Innovation at University College London).

The chat began with Mikela sharing her unconventional path to safety engineering, initially considering medicine and the military before finding her way to systems engineering and safety. She worked as a consultant for about 10 years on major infrastructure projects including railways and metro systems.

Mikela emphasized that her most inspiring colleagues were human factors specialists and systems engineers. She then went on to discuss projects she'd worked on including an NHS Healthcare project transferring communication practices from air traffic control to operating theatres.

She described herself as a "heretical researcher", explaining that good researchers must challenge the status quo and question existing assumptions rather than just reinforcing them. She went on to express concerns about AI replacing critical thinking in younger engineers. She emphasised the importance of understanding interfaces between humans and AI systems and viewing AI as more than just software. The chat concluded with Mikela discussing her work editing books that invite industry professionals to share their practical experiences, which she sees as valuable for educating future generations about how safety is applied in practice.

Complexity and Assurance



The last keynote talk of the first day was by Odd Ivar Haugen from DNV, a major classification society with 15,000 employees serving over 100,000 customers globally. Odd Ivar has nearly 30 years of experience with maritime control systems and dynamic positioning systems.

Odd Ivar spoke about complexity and assurance in maritime systems. He presented several maritime accidents to illustrate complexity challenges:

- The Statfjord A collision in 2019, where a chain of failures in interconnected systems led to thruster shutdown despite redundancy
- The Hurtigruten grounding during sea trials after converting to hybrid battery power
- The Viking Sky near-disaster in 2019, where almost 1,400 people nearly died when all engines shutdown due to low lubrication oil, with the vessel coming within one ship length of grounding

Odd Ivar said the core problem was traditional assurance, which is based on component failures, redundancy and reductionism, but is insufficient for modern complex systems. Multiple control systems (engine safety, power management, fire systems, etc.) operate with their own goals and objectives but no clear overall authority hierarchy exists.

He advocated for multi-model, multi-level safety analysis, using different viewpoints (like different maps of the same city). He emphasised that assurance should focus on understanding system behaviour separately from risk assessment, and that multiple models – like System-Theoretic Process Analysis (STPA) for structure and the Functional Resonance Analysis Method (FRAM) for functions – are needed to understand emergent behaviour.

His main message was that we need to move beyond traditional component-based assurance to systems thinking approaches that account for interactions, emergence and the multiple control systems operating in modern complex systems.

Technical Entertainment

The first day's talks concluded with a fun technical entertainment session called "AI Don't Believe It!" hosted by Paul Hampton and Karin Rudolph. This was an interactive session for attendees designed to explore the creative capabilities and potential impacts of AI.

Participants were shown a range of AI generated content, including sound, video and images and asked to vote on the correct answer to the posed question. For example, AI-generated song lyrics about a safety-related concept was performed in the style of ABBA's classic song "Waterloo". Participants had to listen to the song and guess the safety-related concept.

Congratulations went to Jane Fenn as the sole participant with most correct answers!

Exhibition and Drinks

The evening concluded with an exhibition with drinks and evening buffet meal (free for all delegates). As with previous years, the beer selection was expertly curated by Tim Parsons and gratefully funded by Codethink.

Identifying Ethical Hazards in Safety-Critical Systems: The Role of Balancing Act: Navigating the Tensions Between Safety, Innovation and Sustainability

The first talk of the second day was from Mikela Chatzimichailidou. Mikela's talk focused on navigating tensions between safety, innovation, and sustainability in complex systems. The talk used interactive polling throughout to canvas and engage the audience on these topics.

The presentation drew from three years of conversations Mikela has had with industry professionals about interfaces between safety, innovation and sustainability priorities.

Mikela challenged the "save the planet" phrase, arguing the focus should be on humans and that safety depends on context, stressing that no system is 100% safe in all situations.

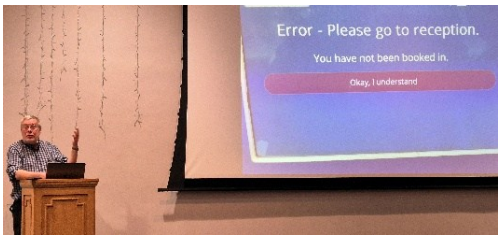
She examined three pairings:

- Safety vs Innovation (Boeing crisis – prioritizing market speed over safety protocols)
- Innovation vs Sustainability (electric vehicles – lifecycle concerns including battery disposal)
- Safety vs Sustainability (rapid technology deployment without adequate testing)

One key message was that responsible innovation requires both rigorous safeguards and courage to advance. Mikela recommended that we should consider entire lifecycles, not just stages, treat safety as separate from reliability, use systems-theoretic models like STPA for complex problems and focus on interactions between components.

Mikela's final thoughts were looking to the future and considering whether the safety profession needs to evolve, possibly requiring systems integrators to coordinate across disciplines rather than traditional safety engineers working in isolation.

A framework to update the Common Law presumption that computer evidence is reliable



Harold Thimbleby gave the next keynote speech of the second day. His talk focused on the urgent need to update legal and regulatory frameworks to address the reality of unreliable computer systems, particularly in safety-critical contexts.

Harold shared personal experiences with failing computer systems in healthcare (eg. NHS apps and hospital registration systems) and transport (train ticketing), demonstrating widespread "technical incompetence" and "technical debt" where users pay the cost of poor software development.

He highlighted numerous other catastrophic failures, some involving the mishandling of Excel spreadsheets that put lives at risk. In some cases, he said the systems lacked basic computer science principles, proper documentation and error detection mechanisms.

Harold said that a fundamental issue is the "legal presumption problem" where British law presumes computer evidence is correct and the veracity of it cannot be challenged as highlighted by the Post Office's Horizon IT scandal. Harold proposed some solutions to this and the other highlighted problems:

- Computer evidence should be presumed unreliable and inadmissible unless there is a forensic-relevant warranty
- We should create Computer Science Qualified Persons (CSQPs) qualifications, similar to qualified persons in pharmaceutical manufacturing and create an independent professional body to certify computer science practitioners
- We should establish professional standards – comparable to driving regulations (which run to 10,000 pages and are globally harmonised)

Armchair Chat

Our second armchair chat saw Phil Koopman from Carnegie Mellon University, being interviewed by Roger Rivett.

Phil discussed his career path in safety engineering, which began with embedded systems work and evolved into self-driving car safety at Carnegie Mellon University.

He shared examples from his experience, highlighting the excellent safety culture in the US submarine force (where he served during the Cold War) combining rigorous maintenance, operational procedures and nuclear power safety culture.

Phil also discussed problematic practices he had encountered, particularly in small embedded systems companies that lack proper safety expertise and treat safety as an afterthought. He emphasised that many practitioners don't understand the difference between knowing how to code and being a software engineer, and that safety engineering education is inadequate in many universities.

Phil said that we need to move beyond the "useful fiction" that systems certified on day one remain safe forever, advocating for lifecycle monitoring and continuous improvement and stressing the importance of goal-based approaches and safety cases. He also expressed concerns about AI-based systems and accountability and the challenges around companies often deflecting liability rather than taking responsibility.

Phil concluded with advice for early-career safety professionals, and this was to accept that safety is rarely the primary priority, to get practical hands-on experience rather than treating safety as purely theoretical paperwork and to be satisfied with making incremental improvements rather than achieving perfection.

Streams

The symposium then split into three parallel streams with presentations held concurrently in two additional plenary rooms alongside the main auditorium. This gave delegates the opportunity to attend 12 additional presentations and workshops.

Experience of static analysis

Possibility Analysis

Building Systems in Rust

Sensitivity Analysis

A number of social activities were also available throughout the day for those wishing to take a break from the formal presentations.

One special session was for Young and early-career speakers to give a 5-minute presentation on a topic of their choice. The audience then voted for their favourite presentation and Mohammad Cherry received the most votes winning a £100 Amazon voucher with his talk on the Air France Flight 447 Accident.

Scutoids!

This year there was a special treat in delegate packs with the inclusion of a "scutoid" sweet box. This innovative design is the work of Mitali and Divya Atkins and it was a great privilege to be able to adopt this as a conference gift. See Mitali and Divya's earlier article on page 33 that provides more information about the discovery, design and evolution of the shape into the packaging used at the Symposium.

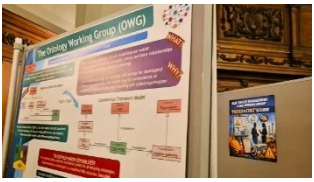
Social Events

Several social events were arranged for delegates as an alternative to attending the more technical workshops. The first, organised in three separate visits, was to the York National Railway Museum, home to iconic locomotives and an unrivalled collection of engineering achievements, celebrating the past, present and future of innovation on the railways.

Other social events took the form of walking tours of York with options for a traditional historical tour or a spooky ghost tour!

Poster Session

The day's talks were followed by a poster session in the main exhibition area where members of the SCSC Working Groups and others working on interesting projects and developments presented posters summarising their work on large presentation boards.



This was well-attended and the 19 posters generated a lot of interesting and interactive discussions.

This year there was also a competition for the best poster. Judging was conducted by Anne Seldon, Bill Blackburn and Mark Sujan and Laure Buysse won the prize with her poster on "Toward Dynamic Safety Cases for COBOTS".

You can find a copy of most of the presented posters after this report.

Clicking on the poster in the pdf version of this newsletter will take you to the pdf version of each poster on the SCSC's website.

Banquet

The end of the second day concluded with the traditional Symposium banquet.

The main dish of the evening was good 'ole "bangers and mash" – Yorkshire style!

After the meal there was an impromptu performance from Peter Ladkin on his simple system flute accompanied on vocals by Tom Anderson! The song was "The Keel Row", a traditional Newcastle song that refers to Sandgate, a street in Newcastle along the Tyne side.

The after-dinner speech was given by Graham Braithwaite from Cranfield University. His talk was humorous with several anecdotes highlighting how different perspectives can influence safety practices. Overall, the talk served as a reminder that even in highly regulated industries like aviation, human factors remain a primary challenge and an essential area of focus for safety professionals.

After the banquet, the diners were asked to form teams for a general knowledge quiz prepared and hosted by Kevin King. This was hugely entertaining with music and picture rounds adding to the fun!

Effective and reflective assurance for AI-based autonomy

Simon Burton kicked off the 3rd day's presentations with a keynote talk focussing on achieving safety assurance for AI-based autonomous systems comparable to conventional safety-critical software. Drawing on 10 years of experience in AI safety, he addressed the challenge of building systems that exploit AI's potential while remaining safe and trusted.

He referenced Tim Kelly's "4+1 principles" for software safety standards and examined how these apply to AI-based autonomy, identifying significant gaps: difficulty defining software safety requirements in ambiguous environments, semantic gaps between high-level requirements and training data, limitations of statistical testing, lack of robustness and emergent system behaviours.

Simon proposed a model-centric continuous assurance approach built around "structural causal world models" with three layers: ontological (things in the environment), quantification (probability of occurrences), and causal (how properties interact).

These models enable:

- More precise requirements refinement using counterfactual reasoning
- Improved verification and validation strategies through Monte Carlo analysis
- Runtime monitoring to detect when systems operate outside safe conditions

He emphasised that assurance should be an iterative process – developing models over time, deriving specifications, making design decisions, testing, deploying and learning from operational experience to refine the models. Rather than relying solely on black-box testing, this approach provides explicit, rigorous models of system and context upon which safety arguments can be based, even if the models are complex and necessarily incomplete.

Armchair Chat

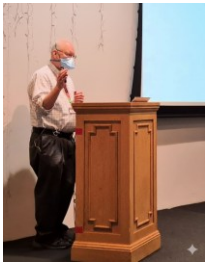
Our final armchair chat was Tim Kelly being interviewed by Tom Anderson. Tom introduced Tim, noting his background as a former professor at the University of York who worked on safety-critical systems and later became a rector in the Anglican Church, serving four parish churches in the East Riding and acting as Dean of the Beverley Deanery (overseeing 18 churches). He is also chair of a youth charity called "The Bus Stop."

Tim started by explaining the difference between a rector and a vicar, and his role as Area Dean looking after clergy in Beverley. They discussed church music, with Tim mentioning he plays piano and his son being a head chorister at Beverley Minster.

Tim revealed he had just experimented with using ChatGPT to prepare a sermon, feeding it the six-step method for Goal Structuring Notation (GSN) construction and the 4+1 principles, which he found worked well!

Tim identified his major academic influence as his PhD supervisor John McDermid, and mentioned being influenced by Toulmin's work on critical thinking and argumentation. Tim described his guiding principles as an academic: transferring knowledge openly rather than withholding it, and striving for clarity in communication. Tom ended by asking Tim about Artificial General Intelligence and whether it would have a soul. Tim's response was that it would not have a soul, but might think it has one. Tom concluded the chat by giving Tim a gift – a religious testimony booklet written by an express train driver using railway signals as a metaphor for life.

Overview of Embodied AI Safety



The final keynote talk was given by Phil Koopman who argued that doing embodied AI safety requires literacy across multiple disciplines – you don't need to be an expert in everything, but you need understanding across all relevant areas.

Phil emphasised that safety is fundamentally about risk mitigation and hazard analysis, not just testing until bugs are fixed. He explained that the traditional V-model works because the left side establishes engineering rigour while the right side validates execution. However, machine learning breaks this model because there is no traceability between requirements and training data.

He explained that AI generates statistically plausible results but doesn't truly "think". It matches patterns from training data, which means being different from the training set is dangerous. He gave examples of systems missing people in yellow raincoats or construction workers because they weren't in the training data.

He showed examples of autonomous vehicle crashes, including a Waymo vehicle hitting a pole (because it wasn't protected by a curb, which wasn't in their test scenarios) and a Cruise Robotaxi hitting a 60ft bus (because it was trained on 40ft buses).

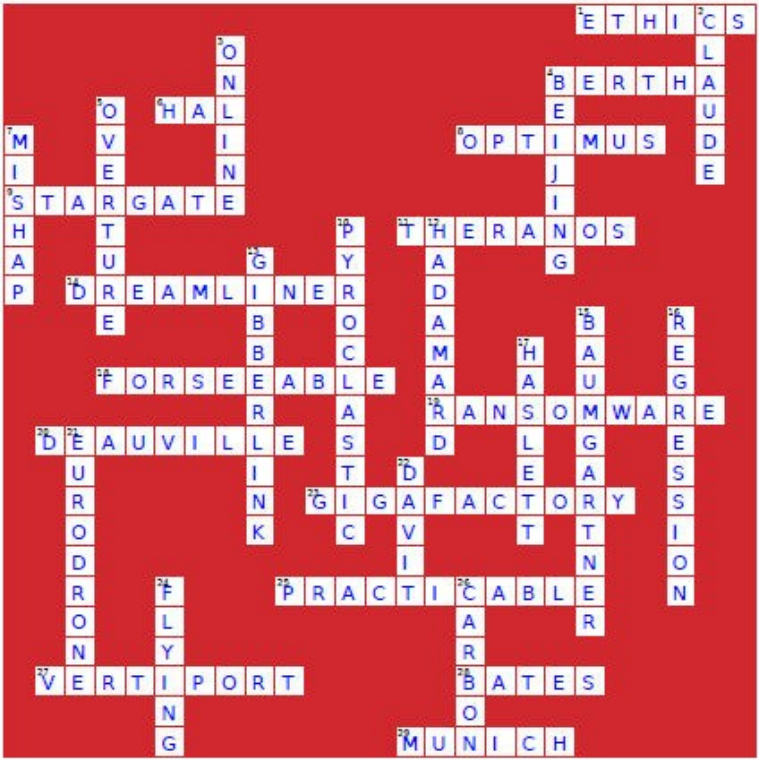
He discussed how humans are terrible supervisors of automation (known since the 1950s), with issues like perception-response time, automation bias and skill degradation with high-quality automation.

Phil concluded with a final observation that safety cannot simply be measured as "bodies per mile" compared to human drivers. He emphasised that safety is a multi-constraint satisfaction problem, not just an optimisation of fatality rates. Companies must avoid specific unsafe behaviours, compensate for others' mistakes and meet the standard of a "careful and competent human driver".

Crossword Competition

The 4th SCSC Safety System crossword was published in the Oct 2025 edition of the newsletter and was also given to delegates to complete during the Symposium. There were 19 entries in total, and the winner was drawn from the correct entries in the 'hat' by Bella Parsons with the winner, Chris Hobbs, receiving a £100 gift voucher.

The answers to the crossword are given on the next page.



Across

1 Branch of philosophy that explores moral principles
4 First name of a female pioneer driving the first automobile over long distance
6 Name of the fictional rogue computer that said "I'm sorry Dave, I'm afraid I can't do that"
8 Name of a general-purpose robotic humanoid with ambitions to leave Earth
9 A massive, $500 billion AI infrastructure project
11 Failed blood testing company whose female CEO was imprisoned for fraud
14 Common name for the aircraft that crashed 32 seconds after takeoff in June 2025.
18 Type of system misuse that might be reasonably anticipated
19 Type of malware that encrypts the victim's personal data
20 European waypoint location that led to an air traffic navigation system outage
23 A large-scale factory, primarily for the production of electric vehicle batteries
25 Technical feasibility without reference to costs
27 Designated takeoff and landing area for eVTOL aircraft
28 surname of the leading campaigner in the British Post Office Scandal
29 City that hosted the first SCSC seminar to be held outside of the UK

Down

2 A family of AI models that includes Haiku, Sonnet and Opus
3 2023 UK Act to protect children from harmful internet services
4 City holding the first ever World Humanoid Robot Games
5 Concorde-like supersonic airliner currently under developed
7 An unlucky accident
10 Type of flow of fast-moving hot gas and volcanic matter
12 Type of gate that creates a quantum superposition
13 project that developed non-speech communication between conversational AI Agents
15 Late Austrian daredevil famous for jumping from the edge of space
16 Form of testing to check if changes negatively impact existing functionality
17 Surname of a female champion of electrical safety
21 A twin-turboprop Uncrewed Aircraft Vehicle under development by companies including Airbus
22 crane-like device often used to lower a ship's lifeboat
24 Type of buttress usually providing lateral support to large structures like cathedrals
26 type of fibre used in the manufacture of a submersible that imploded in 2023