

SSS'25 Event Report



The Safety-Critical Systems Club's annual Symposium returned in February 2025 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.

Mike Parsons introduced the Symposium and said the event's twin themes were Artificial Intelligence (AI) and complexity & interconnectedness. Mike mentioned the CrowdStrike security issue by way of example of complexity; this mass-outage cost industry over £100m and illustrates that we can construct systems with massive interconnectedness that we don't fully understand. Mike concluded by saying that he hoped the Symposium might give some solutions and ways forward for these challenges.

Looking Beyond the Horizon

Dewi Daniels presented his thoughts on the Post Office Horizon scandal and applied the Swiss Cheese model to the events where 100's of subpostmasters were wrongly convicted of fraud. Unfortunately, Dewi thought some layers had more holes than cheese and the end results were appalling with imprisonment, bankruptcy, and even suicides.

Through a series of quotes from stakeholders, Dewi painted a picture of the failings that eventually led to the 'accident'.

Dewi discussed the issue with the Common Law presumption that, for the purpose of judicial proceedings, it's assumed that computers work correctly. Dewi thought the legal system as a whole is weighted to the rich and noted that the Post Office (PO) spent £250m in legal fees.



Dewi said there were three main issues: lack of competence (I didn't know), lack of curiosity (I didn't ask) and lack of integrity (I was let down by all the people who lied to me).

Dewi then handed over to Mike Parsons who discussed the work the SCSC has been doing to make sure these events don't happen again and laid out the club's position: although the PO system was not considered a safety system, events conspired together to ultimately cause harm. It has therefore been decided to extend the remit of the SCSC to any system or systems that could cause harm. Mike then presented a generalised model with eight layers showing the typical issues and possible mitigations. Suggested fixes were things covering Information, Competence, Management Cultural and Support. Mike noted that many of these were already mentioned in the Nimrod review and presented an eight-step plan for improving the system.



The keynote was followed by Harold Thimbleby who discussed how to address the Common Law presumption that computers are always correct and talked about the Theory of Change (ToC) to effect change. Harold then invited the audience to come up with ideas on how to change for the better as part of an interactive debate.

For example, Harold felt better (even certified) developers would be the best approach for developing more reliable AI but acknowledged that there needs to be a TOC to provide a roadmap for societal acceptance of the concept. Ideas from the room included the issues around insurance costs and liability and how warnings and disclaimers can be hidden away in contracts not readily available to users.

AI Safety and Security

The next keynote speech was given by John McDermid from the University of York. John started by exploring the relationship between security and safety. He said that the adage: 'if it's not secure it's not safe' is not true in general but clearly there is a strong relationship between the two.

John discussed the upsides and downsides of AI and showed examples of deliberate attempts to fool an autonomous driving system by sticking labels to stop signs. He said that AI can also be used to help generate attacks.



John then provided a matrix for a list of activities and for each, a column covering opportunities (such as use of AI for pedestrian detection) and the associated risk/limitations, possible mitigations and observations (such as related published work).

John introduced FLAGPT an attempt to use generative system to generate failure logic from system descriptions. He concluded by covering the challenges for the traditional safety community, the opportunities that AI might bring and referred to a table in his paper intending to help promote research agendas.

Armchair Chat

The day's talks ended with the first of a new feature – "Armchair Chat" that saw Tim Kelly interview Harold Thimbleby on his view on various topics. Tim said that he'd used ChatGPT to appraise Harold's entire work and come up with questions for the interview! He said ChatGPT had 'broadly got him right' but Tim discarded 99% of the questions it had come up with.

The pair covered topics such as why there is relatively slow rates of progress in the safety world, what were the obstacles to achieving software warranties to support the admissibility of software in courts and what will the next domain be that we should be worrying about.



Technical Entertainment

Another novel feature for this year was the *Would I L-AI-e to You?* technical entertainment hosted by Paul Hampton, loosely based on the BBC TV panel game of a similar name. In this version of the show, the audience were pitted against the generative abilities of AI and asked if they could tell the difference between human and AI generated content. There were three types of challenge:

Images: three images were shown and only one was the real non-AI generate image



Mystery Guests: four guests were invited up onto the stage and three stories about the individual were told with only one being the real story and the others generated by AI



Mystery Objects: three descriptions were read out for a mystery object with one being the real story behind the object and the other two being generated by ChatGPT.

Many thanks to Jane Fenn, Tim Kelly, Yvonne Oakshott and Tom Anderson for being our guests and for Khadijah Khatun, Dave Banham and Mike Parsons for being our story tellers!

Exhibition and Drinks

The evening concluded with an exhibition with drinks and evening buffet meal (free for all delegates). The beer selection was unusual and varied with flavours such as peanut butter! Drinks were gratefully provided by Codethink.



Anecdotes and experiences with various applications of dissimilarity to meet the safety standard for transport-category aircraft

The second day started with a keynote speech from David King (Vertical Aerospace) who talked about air mobility in general and the new all-electric 4-passenger VTOL aircraft VX4. He explained the need for electric Advanced Air Mobility (AAM) but said safety is the foundation of the endeavour and that there are several approaches to ensuring there are no common-mode failures.

David said the company is aiming for certification of the VX4 by 2028 with 150 vehicles delivered by 2030 with the infrastructure developing and maturing as the operations expand.

He said electric air mobility will be cleaner, having no emissions, and will be less expensive and quieter. Compared to ground-based transport, the vehicles will be 150mph faster and so, for example, a trip from Cambridge to Heathrow would take 25 minutes. Shorter transit times is a key motivator for air mobility as highlighted in the expression: "It's About Time". David then discussed the redundancy architecture and covered the industry debate on what the appropriate safety standard should be for AAM, in other words, asking how safe should it be? David said some say that there is a safety continuum comparing the relative higher risk of a 400-person airliner to 4-person eVTOL and so argue that the eVTOL assurance could be less rigorous. However, Vertical Aerospace's approach is to assure the vehicle to airliner standards. Although safety has improved over time for transport aircraft, the helicopter safety track record is worse with 1.3 fatal accidents per month (ie. you are 1,000 times more likely to be involved in an accident in a helicopter) and the likening of eVTOL to helicopters is a perception that the AAM industry has to overcome.

David also said they need to address common mode failures. Some design philosophies demand design dissimilarity but dissimilarity introduces complexity and brings new risks and David gave examples of accidents where design dissimilarity had caused a problem.

David concluded by saying there needs to be clearer, harmonised guidance to enable AAM growth worldwide and a pragmatic approach to addressing common mode failures needs to be agreed.

Armchair Chat

Our second armchair chat saw Bob Oates in conversation with Tom Anderson. Tom discussed the history of the SCSC, how he got into the safety domain (with some encouragement from Nancy Leveson!), provided advice for those in the earlier part of their careers and how to keep motivated in difficult environments. Tom concluded with a story about how he broke a critical safety feature while riding on the footplate of a Thompson B1 4-6-0 steam engine!



Identifying Ethical Hazards in Safety-Critical Systems: The Role of Creativity

The final keynote of the day was from Catherine Menon from the University of Hertfordshire whose talk was focussed on ethical safety. Catherine introduced the concept of “ensurance” as opposed to assurance, with *ensurance* meaning how safe the system actually is and said lack of assurance doesn't imply lack of ensurance but noted that this does not apply to ethical hazards.

Catherine then referred to an ethics standard BS 8611 (Ethical Design & Application of Robots), which provides a definition of ethical harm and noted that ethical harm is experienced differently across demographics and includes stress, anxiety, manipulation of emotion, deskilling and unfair outcomes. She also noted that perception of harm is in itself a potential ethical harm.

Catherine said that as ethical hazards are dynamic, fluctuating and dependent on the participant, creativity is essential to successfully identify ethical hazards. However, safety engineers like rigour, justification, validation, replicability and evidence so what is needed is a structured approach that includes creativity.

Catherine along with a colleague, Austen Rainer, investigated if HAZOP could encourage creativity and be used to identify ethical hazards. Catherine introduced CHAZOP (Creative HAZOP) to interrogate creative narratives through user stories, vignettes, persona definitions etc.

Catherine then introduced some of the guidewords for CHAZOP and the narrative components: Plot, Character, Setting, Theme, Voice and Structure and said two pilot workshops were held with professional authors where they were asked to apply CHAZOP to their fiction, and they concluded that the process helped promote creativity.

Catherine also introduced EHAZOP (Ethical HAZOP), which builds on HAZOP and CHAZOP to interrogate and analyse ethics of AI Systems. Catherine said two pilots were undertaken to conduct EHAZOP for a specified assistive robot with researchers and a group of school children, which produced interesting insights. Catherine concluded diverse perspectives are essential in identifying ethical hazards and although logic and structured is important, so is creativity.

Workshops

Another new feature this year for the Symposium was the introduction of workshops as an alternative to the social events running in parallel.



There were two workshops in each of three streams being held concurrently:

Stream A

Introductory workshop on “gsn2x” – a tool to create graphical representations of GSN from YAML (Jonas Wolf - Vector Informatik GmbH)



Automating Verification & Validation with Developair: a case study on improving efficiency and regulatory compliance for railways software development (Juan Carlos Rua, Developair)

Stream B



Hands-on session with the Radish Data Safety tool (Divya and Martin Atkins – Mission Critical Applications Ltd, with support from Paul Hampton).

'5 minute pitch' presentations

This session saw a number of younger delegates give five-minute presentations on a topic of their choice. The audience then voted on their favourite presentation with the winning presenter receiving a £100 gift voucher.



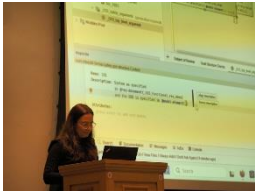
There were presentations from:

- Prenika Anand – AI led Skin Cancer Triage: Safe for all?
- Laure Buysse, KU Leuven – Operationalising Dynamic Safety Cases for Safe Autonomy
- Shaun Feakins – Safety Critical Training Data? Searching for Legal Obligations
- Luke Jackson, Ebeni – The Importance of Correctly Setting Requirements
- Claudius Jordan, Modelwise – Safety DevOps – Continuous FMEDA
- Suemaiya Zaman – Balancing Safety and Innovation: Deployment Challenges for Drone Base Stations in Beyond 5G Communication

The winning presentation was from Prenika Anand.

Stream C

Management of Change in an Ever-Changing World
(Wendy Owen - Independent Consultant) Wendy led this workshop on managing change and a full report of the workshop can be found on page 41.



FASTEN: Carmen Carlan led this workshop covering an open source environment for the specification, verification and assurance of critical systems, addressing: requirements, design, safety analyses and assurance arguments.

Social Events

Several social events were arranged for delegates as an alternative to attending the more technical workshops. The first, organised in two 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.



The second option was a guided walking tour of York given by the excellent Maureen covering the history and heritage of the marvellous city of York.

Poster Session

The days 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 generated a lot of interesting and interactive discussions.

Banquet

The end of the second day concluded with the traditional Symposium banquet. After an excellent meal, the attendees were entertained by recently retired Graham Jolliffe.



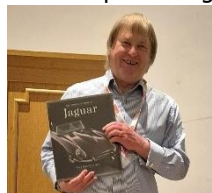
Graham discussed some of the issues he'd experienced during his career including technical failures, like the battery charger fires on Dreamliner, and management failures like poor safety culture, inadequate processes and poor communications.



Graham stressed the need to get the basics right, learn from the mistakes of others, whilst keeping abreast of new developments in safety engineering. Most important is the need to ensure communications are effective across management levels, other domains, and stakeholders. Graham concluded by saying it's our role as safety engineers to avoid mis-communication and achieve a common understanding.



The Banquet also gave the opportunity for the club to thank Roger Rivett for his five years of service as the chairman of the SCSC Steering Group. Roger has now handed over the role to Dewi Daniels. Roger's gift of a book about Jaguar cars was a nod to his years of experience in the automotive industry.



The final day of the Symposium opened with a talk from Paula Palade (Jaguar Landrover) on ethical frameworks for autonomous vehicle behaviour.

Paula started with the early history of car legislation through the 19th century Locomotive Act, which was highly constraining on vehicle use and drew analogies with the AV vehicles of today, in that public acceptability is critical to their successful adoption.



Paula referred to the ethics of the 'trolley problem' and how nuanced and difficult it is depending on the circumstances. While this generates interesting philosophical debate, she said it is not particularly helpful and referred to a number of publications providing guidance from organisations such as the IEEE and the European Commission (EC). Paula focussed on two which she has contributed to. Firstly, she covered the Ethics of Connected and Autonomous Vehicles, guidance commissioned by the EC aiming to tackle issues and dilemmas around road safety, risk, data, ethics, privacy, fairness, expandability and responsibilities. Paula then provided some examples of the 20 guidance recommendations in the document.

The second document was an ISO standard (ISO 39003:2023) for providing guidance on ethics for road traffic safety of AVs. It is not a technical or management standard or framework but rather gives a set of protocols for manufacturers to self-certify. The standard also includes an ethical assessment and Paula ran through some of the high-level points of the assessment process. Paula concluded by saying AI Ethics is quite a complex landscape of regulations and hard to navigate and described their limitations, mainly around practical guidelines on how to implement 'ethics by design'.



After lunch we had our third armchair chat with Catherine Menon being interviewed by Yvonne Oakshott. Catherine fielded questions including: how her work has evolved over the course of her career, how engineering and life as a successful fictional writer intersect and what would the subject be if she coauthored a book with a robot!

The final keynote talk to close the Symposium was from Richard Hawkins from the University of York. Richard stressed that safety cases remain as important as ever but practices often remain poor and better processes are required for them to be more effective.

Richard discussed some of the problems with Safety Cases, referring to the Nimrod Report and said that we need Safety Cases that are risk-focused, consider ways in which the system may not be safe, drive safe design and encourage people to think about and understand why their system is safe (and when it isn't).



Richard said we don't need more techniques but rather get better at using the tools we do have, and summarised some of these tools as:

- Goal Structuring Notation (GSN)
- The 6-step method for applying the GSN notation to create arguments
- Ways of capturing challenges to arguments through, for example, dialectic arguments
- Techniques for developing confidence arguments
- Link operational arguments in design Safety Cases
- Ways to establish through-life monitoring of a Safety Case, such as, Safety Performance Indicators

Richard then proposed an elaboration of the 6-step method to help bring all these components together in the form of a Safety Case Development Process and provided examples of applying this at each stage.

Crossword Competition

The 3rd SCSC Safety System crossword was published in the Oct 2024 edition of the newsletter and was also given to delegates to complete during the Symposium. There were 15 entries in total, and the winner was drawn from the correct entries in the 'hat' by Mitali Atkins with the winner, Fabian Picca, receiving a £100 gift voucher.

The answers to the crossword are given below.

