The Safety-Critical Systems Club Newsletter

Safety Systems

Vol 32 No. 3 – Oct 2024

OVER THE HORIZON
Learning from the Post Office Horizon Scandal

COSTING THE EARTH?
Assessing Global Hazards

FEMALE PERSPECTIVES
Reflections on Women in Engineering



SCSC

thescsc.org



SCSC Publication Number: SCSC-198

While the authors and the publishers have used reasonable endeavours to ensure that the information and guidance given in this work is correct, all parties must rely on their own skill and judgement when making use of this work and obtain professional or specialist advice before taking, or refraining from, any action on the basis of the content of this work. Neither the authors nor the publishers make any representations or warranties of any kind, express or implied, about the completeness, accuracy, reliability, suitability or availability with respect to such information and guidance for any purpose, and they will not be liable for any loss or damage including without limitation, indirect or consequential loss or damage, or any loss or damage whatsoever (including as a result of negligence) arising out of, or in connection with, the use of this work. The views and opinions expressed in this publication are those of the authors and do not necessarily reflect those of their employers, the SCSC or other organisations.

© SCSC CIC 2024 except where explicitly stated for specific articles, reports or images.

Front cover and editorial: AI generated images
In Brief images may be subject to copyright – contact the SCSC Newsletter Editor for details.

Contents

WELCOME

Editorial 3

Opening words from the SCSC Newsletter Editor.

In Brief 4

Recent system safety news items from around the world.

FEATURES

Ensuring computer reliability after the Post Office Horizon Scandal 5

Harold Thimbleby asks how issues arising from the Post Office Horizon scandal can be avoided in the future.

Environmental Hazard And Impact Identification 9

Nick Hales provides an example of his modified Doughnut Economics ring to assess hazards on a global scale.

Women in Engineering: Reflections 19

Wendy Owen interviews leading female engineers reflecting on the challenges faced by woman in engineering.

SCSC Safety Systems Crossword 40

The annual SCSC Safety Systems crossword returns for a 3rd year!

Test your system safety knowledge and you could win a £100 voucher!

REPORTS

Seminar: Frameworks for Safe AI Systems 27

Highlights from this SCSC seminar discussing frameworks for safe AI.

Seminar: Developing Safe AI Systems 32

Highlights from this SCSC seminar discussing AI systems development.

Recent Safety Publications 37

The latest publications relating to safety.

60 Secs with ... Nick Hales 38

Nick answers some quick-fire questions on system safety and life!

GROUPS

Working Groups 43

Details of the SCSC Working Groups.

SCSC Steering Group 50

Who's who in the Steering Group.

EVENTS

Calendar 52

Events Diary 53

Safety Critical Systems Symposium SSS'25

Tuesday 4 - Thursday 6 February, 2025 - York, UK



The Safety Critical Systems Symposium SSS'25 will be held at the Principal Hotel, York from 4-6th February 2025, featuring submitted papers, keynote presentations, exhibition, poster sessions and more.

Come and learn about the latest developments in applied system safety!

Booking is now open!

Early-bird rates available until Friday 13th Dec 2024

Residential double tickets, covering two delegates, are available for £1,875. The second delegate must be from the same company, under 35 or a full-time student. To take advantage of this offer please contact Alex King, alex.king@scsc.uk

Event Programme

See inside back cover for a summary of the event's programme and here: scsc.uk/e1099

The call for abstracts for presentations is now closed.

If you would like to discuss topics for presentation, either as a talk or a poster, please contact Mike Parsons, mike.parsons@scsc.uk

Exhibiting at SSS'25

The tools, vendor and recruitment exhibition will run over Tuesday 4th Feb and Wednesday 5th Feb.

If you would like to exhibit at SSS'25 or for further details, please contact Alex King, alex.king@scsc.uk

Editorial

In our line of work we often come across pithy words of wisdom such as "Safety First!" and "Don't Learn Safety by Accident!" While we might debate how impactful such expressions might be on changing behaviours, I'm sure we'd agree the sentiment is in the right place. I was therefore surprised to come across another expression recently: "Safety Third!"



It did require a bit of a doubletake; not least that safety wasn't considered the upmost priority but wasn't even a close runner up! It seems it really is "a thing" and you can indeed literally buy the tee-shirt, so you can promote this philosophy yourself, often with images accompanied by some dangerous acts such as riding a wild bear, beer in hand, or proudly exhibiting the results of your recklessness with a couple of bloodied missing fingers.

As far as I could gather, the elements taking priority over safety are firstly, the mission itself, and secondly, the commitment and enthusiasm of those taking part. Unfortunately, the philosophy appears not to be constrained purely to the young devil-may-care thrill-seeking adventurers venturing into the woods to find bears. A poignant example is Stockton Rush and his endeavours with his deep-sea exploration company OceanGate. Rush saw safety as stifling innovation and so choose not to seek safety certification for the Titan submersible, which unfortunately imploded in June 2023 killing himself and four others. Rush was quoted as saying "… *at some point, safety is just pure waste. I mean, if you just want to be safe, don't get out of bed … At some point, you're going to take some risk, and it really is a risk-reward question".*

Arguably, Rush's endeavours were on one extreme of the risk-reward balance. The huge efforts being undertaken toward enabling Urban Air Mobility (UAM) – electric flying taxis to some – is arguably another unprecedented area of innovation with significant momentum. We are now seeing early flights of such vehicles, but progress towards remotely piloted or autonomous variants is still slow as much of the regulation required for true integration with crewed vehicles is still being developed and may take many years. Some businesses have already folded and others are hostages to their first accident, which would likely irrevocably damage their brand and put them out of business.

The key question (assuming we do want to get out of bed!) is where should the risk-reward balance lie and who makes that determination? Consumers ultimately perhaps, but despite signing waivers there will still be an expectation that safety is being managed – other stakeholders have a part to play and opinions can change almost overnight after a mishap. In conclusion "Safety Third" in my view is a philosophical approach that cannot be lightly dismissed and needs careful management in its own right, but how? Does a method or calculus exist for trying to quantify this precarious risk/reward balance? Views (or articles) welcome!

In this edition we have three great articles, two seminar event reports and a return of the annual SCSC Safety Systems crossword! We are also preparing for our next SCSC Symposium to be held in York in Feb 2025 so see the end pages for programme details.

Paul Hampton
SCSC Newsletter Editor
paul.hampton@scsc.uk



In Brief



Grenfell Tower: the fire, the findings, who's to blame and what happens next



Sir Martin Moore-Bick's report paints a horrifying picture of failures in the construction industry and officialdom – but justice is some way off. The report of the public inquiry into the causes of the Grenfell Tower fire has been published – and it forms a devastating verdict on the incompetence, dishonesty and greed that made possible a disaster in which 72 people died. *theguardian.com*



Cyber attack sees over 1,000 NHS ops postponed

More than 1,000 planned operations and over 3,000 outpatient appointments have been postponed amid disruption caused by a cyber attack that impacted London hospitals. *bbc.co.uk*

Air ambulance says drone near misses going up



An air ambulance service said it has experienced some near-collisions involving drones. Wiltshire Air Ambulance pilots say that the trend of drone collisions is going up and they are seeing more people fly drones over accident sites. *bbc.co.uk*

Huge Microsoft Outage Caused by CrowdStrike Takes Down Computers Around the World



A software update from cybersecurity company CrowdStrike inadvertently disrupted IT systems globally – taking Windows machines offline. Banks, airports, TV stations, health care organisations, hotels, and countless other businesses all faced widespread IT outages, leaving flights grounded and causing widespread disruption, after Windows machines displayed errors worldwide.
wired.com

Tesla Cybertruck's first fatal crash raises safety concerns for Elon Musk's electric pickup



A man has tragically died after his Tesla Cybertruck veered off the road and burst into flames in what is believed to be the first fatal crash involving Elon Musk's latest electric pickup. The vehicle, which has yet to undergo independent crash tests, was reportedly involved in the deadly accident for 'unknown reasons'.

Despite Tesla's strong safety record with its vehicle line-up, this incident raises questions about the durability of the Cybertruck, which is touted as exceptionally robust. *mirror.co.uk*

Ensuring Computer Reliability After The Post Office Horizon Scandal



As the enquiry into the Post Office Horizon scandal continues, Harold Thimbleby explores this and other cases where IT system failures have had significant impact on welfare and safety. He discusses the legal factors that make it hard for IT systems to be called into question, and proposes measures that could be taken to prevent these issues arising again in the future.

In the UK, the Post Office prosecuted nearly 1,000 postmasters — plus more who settled out of court — for fraud, theft, and false accounting. The evidence used in court is now known to have been corrupted by bugs and unauthorised access to the Post Office's Horizon computer system. The Court of Appeal Judge said the Post Office's malicious prosecutions and failures were so egregious as to make the prosecutions an affront to the conscience of the court. Following the powerful 2024 ITV drama *Mr. Bates vs The Post Office* about the problem the Government promised to cancel prosecutions and pay compensation, and has since passed the Post Office (Horizon System) Offences Act 2024, which has exonerated and ordered compensation for many (but not all) affected postmasters.

Horrendous as the Post Office IT case has turned out to be, it's by no means unique.

In the Netherlands the prime minister, Mark Rutte, and his Government resigned in January 2021 after more than 1,000 children had been forcibly taken into care because SyRI, a computer system used for predicting fraud, had erroneously charged people with fraud and demanded payments of hundreds of thousands of euro. A Dutch court ordered the government to stop using SyRI as it violated human rights and had ruined thousands of lives.

In Australia, a computer system called Robodebt led to welfare recipients having to pay non-existent debts. The burden of proof was moved from the system needing to verify the information to the individuals having to prove they didn't owe anything. In 2022, the Australian government finally forgave the debts of 197,000 people.



In 2024, CloudStrike's routine cybersecurity update crashed 8.5 million PCs worldwide, including putting many healthcare systems from Australia to the UK out of action. Delta Airlines who suffered major problems was served a class action suit by passengers, and in turn Delta blamed CrowdStrike for its $500m loss — yet Delta would have signed off CrowdStrike's software disclaimer, which says *"TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW CROWDSTRIKE SHALL NOT BE LIABLE."*

That such ubiquitous end user licence agreements (EULAs) have force is underlined by Disney who argued in court that, as a person who died from an allergic reaction to food served in a Disney Park had agreed to a EULA for a free trial of a Disney streaming service, that therefore the court should compel arbitration and stay the proceedings against them. The Disney EULA states *"You and Disney DTC agree to arbitrate, as provided below, all disputes between you (including any related disputes involving The Walt Disney Company or its affiliates)"* However a major public backlash against Disney led them to "waive their right to arbitration" which simultaneously makes them look good yet retains the sweeping interpretation of the EULA.

The NHS as a whole is riddled with IT problems too, as is made clear by the booklet: *Patient Safety — Stories for a digital world*, available at https://www.harold.thimbleby.net/booklet





The Royal College of Anaesthetists advise doctors that they should ignore the output of any computer monitoring, and make all necessary clinical observations and controls themselves. The reason is that the technical specification of the equipment and the programs are "commercial in confidence" and therefore cannot be trusted because nobody who knows (if anyone does!) will tell the anaesthetists exactly how they work.

Like the Post Office case, many NHS IT problems surface in court with unfortunate results, often prosecuting nurses for problems caused by inadequate computer systems.

James Christie shows that lawyers and the law itself do not understand IT [1]. Central to the Post Office's approach to prosecution was the flawed common law presumption that computer evidence is correct [2]. In practice, this evidential presumption turns "innocent until proven guilty" on its head, reversing the burden of proof on the defendant to show why the computer evidence should not be relied on as a true statement of fact. This is nearly impossible to do as the presumption cannot easily be rebutted. In many cases, the legal presumption undermines justice, but it also insulates the courts from technical arguments that would go over everyone's heads. Justice isn't served either way.

Artificial Intelligence is making the problems more acute. Generally, nobody really understands how AI works, as it isn't just programmed by humans (with enormous programs that themselves will contain bugs) but also learns, and can learn anything from incorrect and misleading data. Indeed, bias (such as gender and racial bias) in data is recognised as a serious problem. Worse, AI companies make amazing promises so AI has become irresistible to adopt in all sorts of areas, and adoption is happening much faster than we understand how to use it safely. Police profiling, driverless cars, credit rating systems, and medical diagnosis are just some of the areas where AI has already created problems after removing human oversight.

Regulating AI has become an internationally-recognised concern, but strangely there has been little interest in regulating IT more widely, let alone regulating professional developers. Regulation in other critical areas is broader; for instance in mains electricity, not just the products are regulated, but the types of use and the electricians themselves are regulated too. Moreover, in electrical and other safety critical industries there are rarely complaints about regulatory burden or stifling innovation through regulation.



VICTORIÆ REGINÆ.

CAP. XC.

In the nineteenth century, Parliament passed the Medical Act of 1858 in response to the scandal that people were being treated by dangerous quacks instead of by competent doctors. In the Act's opening words, *"it is expedient that Persons requiring Medical Aid should be enabled to distinguish qualified from unqualified Practitioners."*

Why not adopt this attitude in IT? Indeed, many doctors' treatments are delivered by IT (for instance, with drug delivery systems like computerised infusion pumps) and surely those NHS computers should be as at least reliable as doctors are required to be? Yet they aren't [3].

One can anticipate that there will be opposition to any apparent increase in regulatory burden for assuring reliable IT systems — there are many large companies and people involved in the industry who would lose work and whose products would lose value or become unsellable. While the problems of failures of cowboy IT systems are not going to be completely solved [4], surely they can and should be controlled a bit better before more catastrophes happen?

There is obviously scope for a lot of debate about how to improve the reliability of computers. Here are some starter ideas:

- Our first proposal thing would be to fix EULAs. Ban use of evasive terms such as "professional intermediary" (terms which try to make the user liable), and EULAs that explicitly require users to indemnify manufacturers. Once we start considering improvements, there are many ways to improve EULAs, for instance why not void blanket terms that are frequently abused, such as in the Disney case above.
- Next, the Health and Safety At Work (HSAW) Act should be brought up to date with IT. The Act currently says every employer must ensure, so far as is reasonably practicable, that both employees and persons not in their employment are not exposed to risks to health or safety, including undertaking research and testing to minimize such risks — but nobody properly enforces the Act's stipulations across IT yet.
- If EULAs were tightened and the HSAW brought up to date with IT, manufacturers would soon start employing more competent programmers, and then the Medicine Act analogy would seem less far-fetched.
- This list isn't intended to be complete in any way, for instance it doesn't explore any technical opportunities, such as digital certificates, etc.

What are your ideas? Do email harold@thimbleby.net

With acknowledgements to the whole team who authored [2] and helped improve this article.

Further reading

[1] J Christie, "The Post Office Horizon IT scandal and the presumption of the dependability of computer evidence," *Digital Evidence and Electronic Signature Law Review*, **17**:49–70, 2020. DOI 10.14296/deeslr.v17i0.5226

[2] N Bohm, J Christie, PB Ladkin, B Littlewood, P Marshall, S Mason, M Newby, SJ Murdoch & M Thomas, "Briefing Note: The legal rule that computers are presumed to be operating correctly — unforeseen and unjust consequences," *Digital Evidence and Electronic Signature Law Review*, **19**:123–127, 2022. DOI 10.14296/deeslr.v19i0.5476

[3] H Thimbleby, *Fix IT — See and solve the problems of digital healthcare*, Oxford University Press, 2021. See also https://www.harold.thimbleby.net/booklet

[4] H Thimbleby, "Cowboy digital undermines safety-critical systems," *Safer Systems: The Next 30 Years, Proceedings of the 30th Safety-Critical Systems Symposium*, ed M Parsons & M Nicholson, **SCSC-161**:203–226, Safety-Critical Systems Club, 2022.

Image attribution:
front: Wellcome Library, London, CC BY 4.0, via Wikimedia Commons
crowdstrike ID 327905900 © Valeriia Lukashova | Dreamstime.com
diagnostics: OpenStax, CC BY 4.0, via Wikimedia Commons
Medical act | Legislation.gov.uk licensed under Open Government Licence v3.0

Harold Thimbleby

Prof Harold Thimbleby is See Change Fellow in Digital Health at Swansea University, Wales. Harold won the BCS Wilkes Medal and has previously been a Royal Society Wolfson Research Merit Award Holder. He has published over 300 refereed papers, and has given over 600 presentations around the world.

The author retains copyright of this article.

Environmental Hazard And Impact Identification



Nick Hales expands on his earlier article, published in the February 2024 Newsletter, which advocated the use of a modified Doughnut Economics ring using three rings to recognise the current situation of the global economy. Nick helps illustrate these concepts with a real-world example relating to the production of electric vehicle batteries, in particular, the mining of resources required for their manufacture.

The Chief Executive of the Royal Society for the Protection of Birds, Beccy Speight, recently wrote [1], *"Tackling the nature and climate crisis is not easy; we must be bold, innovative and think big."* This article is intended to address the challenge to be bold and innovative in engineering terms and examines how the 21 principles of the Doughnut Economy [2], given in Table 1, (covered in more detail later), could be used to provide categories of risk. In due course these or similar principles may be incorporated into a guidance document on, "A Systems Approach to Safety of the Environment". To achieve this intent, the article considers hypothetical aspects of a project conducted by an ethical corporation involved in electric vehicle car battery production. The company wishes to produce an environmental and socially focussed hazard analysis. The stage of development examined in this article is the hunt for resources for batteries for the car. A previous article [3], introduced the topic of Doughnut Economics.

The image of the 'doughnut' from the Doughnut Economics Action Lab (DEAL), website [4] given in the previous article is reproduced here (Figure 1). Just to recap, the safe space for humanity is in the 'bread' of the ring doughnut.



Figure 1

The SASEWG term for a modified Preliminary Hazard Analysis, (PHA), is a Preliminary Environmental Hazard and Impact Identification, (PEHII) analysis. This term will be used in the rest of this article. The factors which are outside the doughnut, are risks to the environment including those arising at any stage in the project lifecycle. They are beyond the ecological ceiling. Similarly the factors inside the hole in the middle of the doughnut, are the risks to people that push them below an acceptable social foundation.

The previous article [3] advocated the use of a modification of the Doughnut Economics ring with three rings to recognise the current situation of the global economy. The reason for this being that it would be unacceptable for many of those in the developed world to suddenly have all they had taken from them and replaced by a worldwide homogeneous wealth structure. The objective of the three rings is to haul the developing and underdeveloped economies up to developed status without dragging others down which may be a cause of umbrage, if it were to occur. The three rings doughnut helps in the planning of the project. Those using it should look for a net positive gain for the environment and a measurable lifting of those identified as lacking in some aspect that forms the minimum social foundation.

The three ring version as described in context in [3] is given in Figure 2. and ties responsibilities to earnings. The initial specification suggested was, though this is in no way definitive, that an under-developed salary may be under £1000 a year, developing countries salaries in the bracket £1000 to £10,000 per year and the developed world £10,000 and above.

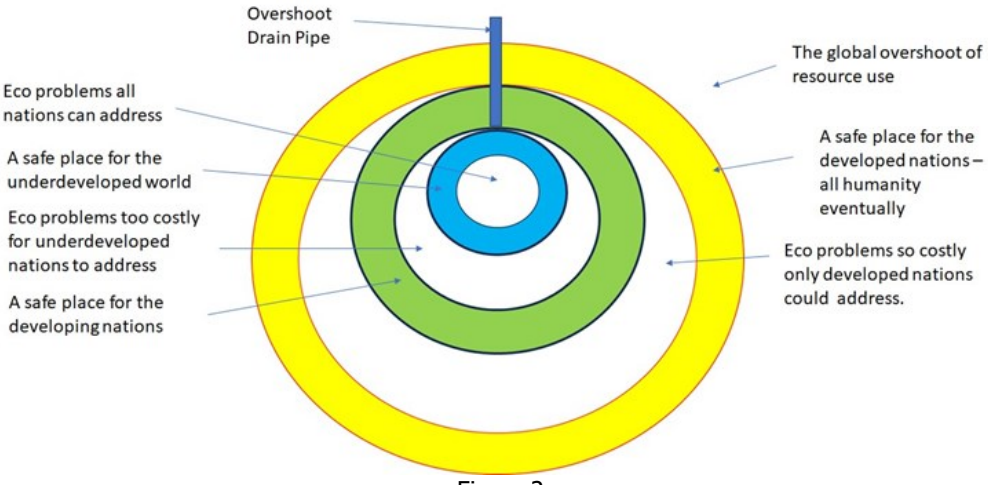


Figure 2

A company wishing to offset its overall environmental impact, in the first instance, should engage trained staff or employ an independent researcher to take deep dives into the social issues and current science around ecological matters associated with the raw materials sources they will use. These people will be the project- and resource-specific skilled members working on the PEHII. There will almost always be other science programmes looking at environmental issues that may be of use so thorough investigation is required.

Preliminary Environmental Hazard Impact Identification

Looking at how to assess what damage a project to create a manufacturing production line could do in a global sense rather than just by malfunction can seem a daunting task. The batteries alone require a good deal of raw materials from the environment in areas which are frequently sensitive and where the resource itself may be limited. Two entries for the PEHII are considered and the logic of why they are necessary is discussed. The evidence is not simplistic so sometimes needs intense consideration.

One other area examined is the problem of data veracity which is critical, as decisions will have long term effects on the planet. That does not mean that conventional tools, with a little tweaking, will not be adequate. A full Hazard Analysis may still be used for through-life control of potentially damaging substances. But issues around Dark Data[1] will certainly affect the PEHII because there are so many unknowns outside the normal concerns of a project when the through life effect on the environment is brought into consideration.

[1] In his book "Dark Data – why what you don't know matters" [6], David Hand introduces the concept and classifies types of "Dark Data" – this explores the many ways in which we can be blind to missing data and how that can lead to conclusions and actions that are mistaken, dangerous, or even disastrous.

A PEHII based on PHA tables assists with three tasks that most engineers will recognise. A good presentation on PHA can be found at [5]:

1. Identify all potential hazards and hazardous events that may lead to an accident
2. Rank the identified hazardous events according to their severity
3. Identify required hazard controls and follow-up actions

The conventional Hazard List for a PHA may consider the following, taken from [5]:

- Mechanical Hazards e.g. crushing hazard or inadequacy of mechanical strength
- Electrical Hazards e.g. contact with operator or electrostatic phenomena
- Thermal Hazards e.g. work environment too hot or scalds
- Thermodynamic Hazards e.g. over-pressure or under-temperature
- Noise Hazards e.g. acoustic signal interference or hearing loss
- Vibration Hazards e.g. poor design causing poor posture or neurovascular problems
- Radiation Hazards e.g. microwaves or gamma radiation
- Material or Substance Hazards e.g. harmful gases or microbiological

The Hazard List for the PEHII, by contrast, is provided by the doughnut economy in the default situation. Two lists are given, one for exceeding the ecological ceiling and one for leaving people beneath the social foundation. All the factors may be hazards in any particular project. These are the tabulated lists of the factors which carry humanity away from the 'dough' of the doughnut as shown in Table 1:

Table 1

Ecological ceiling	Social foundation
Ozone layer depletion	Gender equality
Climate change	Networks
Ocean acidification	Housing
Chemical pollution	Energy
Nitrogen and phosphorous loading	Water
Freshwater withdrawals	Fuel
Land conversion	Health
Biodiversity loss	Education
Air pollution	Income and work
	Peace and Justice
	Political Voice
	Social Equity

It should not be taken, however that this is the only doughnut picture. The doughnut is adaptable and the granularity can be adjusted for the setting, but for the initial PEHII, this is a very useful planning tool for those taking the systems approach to safety of the environment. The PEHII must be reviewed and updated as knowledge increases, especially in the case here of mineral resource supply.

Frequency, consequences and severity need to be considered but also the regulatory environment. Some nations may be less strict than others but lobbying for them to adopt regulations broadly accepted elsewhere is a useful activity as the consequences for the reputation of a company that is damaging the environment, even though legal in a country with a less developed approach to safety, could be dire.

Constituents Of The First Stages Of An Eco-Friendly Project

Three topics are dealt with in the rest of this article. An aspect of data safety is examined, as it is essential to have correct data in order to understand the potential consequences for the planned development and the environment. Two examples of issues for the battery development are given and after discussing the reasons for their entry, the possible appearance in a PEHII hazard list is demonstrated in the form of a table. The issues have been restricted to the following three simply due to space.

1. Deceptive or dark data
2. Deep sea mining
3. Sourcing minerals from plants

Deceptive Or Dark Data

Engineers need to be sure, in order not to breach the ecological ceiling or to prevent fellow citizens suffering by being buried below the social foundation, that the data they use to make decisions is correct. The environment must be described sufficiently too, thus ensuring the correct data applies to that environment, which may be new and unique.

In his book "Dark Data – why what you don't know matters" [6], David Hand describes a particular type of dark data addressed in this section, Type 13 "Intentionally darkened data", which he labelled as particularly troublesome. This is described in the Data Safety Guidance Annex K published by the Safety Critical Systems Club [7]. In a PEHII, bad data will always lead to false conclusions. An early victim of Dark Data was Lord Kelvin, one of the most celebrated mathematician/scientists of his day. He claimed Darwin's theory was impossible. He came to the conclusion that the sun could not have shone down on earth for as long as evolution would have taken because he was unaware of nuclear fusion. That was a case of 'Known Unknown' but that fact was ignored and Kelvin opposed without any real evidence.

In his book, The Skeptical Environmentalist, [8], Bjorn Lomborg highlights the gamble the economist Julian Simon offered all comers, that any given raw material would drop in price over a year or more later. Lomborg claimed Simon could not have lost, yet neither lithium nor lithium carbonate were in the extensive table of materials that Lomborg produced to illustrate his point.

UK inflation between 1997 and 2024, as calculated from the composite price index published by the Bank of England [9].

1. Lithium carbonate was around $2,100 per metric tonne in 1997
2. Lithium carbonate was $68,100 per metric tonne in 2022
3. By the Bank of England calculator, the price by 2022 should have been about $3,600

Lomborg was either ignorant, (which is not a crime), consciously biased or unconsciously biased. One hopes it was not consciously biased which would be Dark Data Type 13 in [7]. From the SASEWG position of protecting the environment and not crossing Doughnut Economy lines, Data errors could lead to destruction of any social foundation already established.

The lithium extraction process uses a lot of water – approximately 500,000 gallons (1.9 million litre) per metric ton of lithium. South America's Lithium Triangle, is one of the driest places on earth. Evaporation used in the extraction activities consumes 65% of the region's water, which is having a large impact on local farmers. Some communities have to get water elsewhere, pushing them below the acceptable social foundation[2].

PEHII Analyses

Two PEHII analyses follow, one for the Ecological Ceiling aspect and the other on the Social Foundation. As will be seen, very large amounts of research and explanation is needed to back up just single entries in the PEHII. Artificial Intelligence may assist with the process. How the entries in a PEHII might appear are given at the end of each of the two problem descriptions.

PHEII Risk – Breaching The Ecological Ceiling

If proof were ever needed that researchers aren't always manipulated to find results that agree with what their paymasters want to be the truth, then the most recent work of Andrew Sweetman, on sea bed mining provides it. This was reported in New Scientist [10]. In 2013 Sweetman found that oxygen was present but not declining when his team sealed off areas of the abyssal Pacific ocean. Something was maintaining the oxygen level. The oxygen source, whatever it is, is important for marine life at a depth where light does not penetrate to enable photosynthesis to supply the gas. The floor of the sea being investigated was rich in minerals needed for car batteries and much of the zone has already been licensed for exploitation. The minerals are found in potato sized nodules containing manganese, cobalt and nickel that litter the floor of the ocean. Those are exactly the elements that electric vehicle battery manufacturers require, so they are keen to mine these deep underwater plains. Sweetman ignored his result in 2013 because he thought the instruments used must be wrong. Then in 2021, he got the same result in a different area of the Pacific ocean using different instruments, so began to think his 2013 results may have been correct.



The initial theory Sweetman is now working on is that some forms of natural batteries are being created in the sea water, by the nodules, and splitting the water molecules to produce oxygen and hydrogen. It remains *"unclear under what conditions the reaction takes place and the contribution this dark oxygen makes in sustaining surrounding eco-systems"* [10].

How creatures and plants survive in the abysses without a ready supply of light for photosynthesis remains a mystery, but this could explain some of it. Mining of the ocean floor, that extracted all the sources of oxygen, would likely lead to extinction of the many tens of thousands of species we know so little about in the dark parts of the oceans. So again, the need to be extremely careful about where resources are sourced from arises.

[2] The acute dependency on water in the Lithium Triangle is illustrated by the storyline of the Bond film: "Quantum of Solace". In the film, the villain from Spectre, Dominic Green, blackmails corrupt military and politicians to control water in the Lithium Triangle.

In 2016, investigation of the seafloor in the Clarion-Clipperton Zone,(CCZ), was found to contain an abundance and diversity of life – more than half of the species collected were new to science. Estimates are that some 6,000 to 8,000 species could be waiting to be discovered in the CCZ alone, according to a June 2023 study published in the journal Current Biology [11], so concern for biodiversity there is high. Sweetman's original sponsors, The Metals Company, are trying to develop a rebuttal of Sweetman's findings because, if his results are correct, global mining of the ocean floor, such as the CCZ, will be paused and perhaps halted completely. The following table shows the PHEII hazard assessment entry:

Ref	EC1
Hazard	Potential for severe ecology disruption
Event/Error	Sea creatures dependent on abyssal plain minerals for oxygen go extinct due to bottom trawling
Cause	Deep water oxygen may be produced by metallic nodules of cobalt, nickel and manganese. Extracting nodules may cause hypoxia in life on the plains
Prevention	Halt bottom trawl for manganese-nickel-cobalt nodules until scientific research completed
Probability	High
Severity	Very High
Comment	Bottom trawl could become a crime, if science consensus reached

PEHII Risk - Dropping Below The Social Foundation

Taking, as an example, a nation in the developing bracket, a corporation could expand investment in projects that are showing promise. The science could be conducted in the field in a developing country with assistance from the parent companies research units in the developed world. Here, relatively small amounts would be invested and for a small amount extra, good relations with the people of the nation could be established with the construction of a technical college or some other environmental or social problem tackled to help the nation rise above the social foundation.

The complexity of the process involved in creating an unbiased, fair and accurate PEHII can hardly be overstated. For this example, which has just one single entry on the PEHII register, some quite remarkable science being conducted in Albania has been selected; this was reported in New Scientist [12]. The average salary in Albania is £750 per month, equivalent to £9000 per year, so the people fall into the category of a developing country, using the ratings in the original article [3], when earnings are between £1000 and £10,000 per year income. The development selected is an agricultural programme to reduce CO_2 emissions and provide a source of Nickel, which will be much needed in the near future for batteries for our electric cars, especially if bottom trawling is banned in many areas.

Albania has high nickel levels in its soil. Demand for nickel is expected to increase hugely with Brazilian mining company Vale estimating that 6.2 million tonnes would be needed by 2030 [13]. The plants native to that nation are resistant to the effects of metals in soils which are toxic to many other plants from elsewhere on the planet. A farm in Albania is growing plants that accumulate nickel. The programme is overseen by a University spin-off business called Econick. It operates several soil remediation operations using hyperaccumulator plants. The joint company with Aperam, a leading French steel producer, is called Botanickel and is engaged with local communities which helps raise them to a point above the social foundation and could transform them over the years into a fully developed nation with average salaries above the £10,000 threshold set. On their website [14], they declare they will "*develop opportunities in research, education, training, employment and energy production that are aligned with local priorities".*



The return may seem small at 2% of dry weights of the flowers of the plant Odontarrhena Decipiens but, in fact, hyperaccumulator plants growing in metalliferous soils safely accumulate extraordinarily high amounts of heavy metals, including cobalt, cadmium, manganese, zinc, and nickel. Aperam's website [4] states it is in fact a relatively good return, estimated at 400Kg per hectare.

The cleaning up of the soil enables the growing of normal crops that cannot tolerate these soils as they are, but could be grown once the heavy metals have been sucked out of the ground by farming Odontarrhena Decipiens. The following table shows the PHEII hazard assessment entry for this activity:

Ref	SF1
Hazard	Investment in poor soil harvesting proves ineffective.
Event/Error	Insufficient minerals obtained from the flowers for commercial success.
Cause	Market price of minerals reduces year on year
Prevention	Make sure stocks of the minerals are obtainable elsewhere
Probability	Med
Severity	Low
Comment	The science is good since the plants improve the soil

Conclusion

It is clear that increasingly corporations are recognising that some effort towards conserving the planet biodiversity and treating people decently has to be made in order to maintain reputation. The technique of using a PEHII in parallel to the more familiar PHA offers one opportunity to recognise formally the problems of factors outside the boundaries of the project. Other methods of creating such an analysis may arise and engineers should always be on the look out to source better resources, utilise better processes and, in due course, produce better products and outcomes. If data is not correct then an opportunity to protect the oceans and the thin layer of soil we live on, may be missed. Blasé attitudes such as those Lomborg appears retrospectively to have encouraged, can have terrible consequences such as the killing of two rangers in Mexico who were trying to protect the Monarch Butterfly wintering sites. Lomborg's book declares there was no threat to the butterflies, the rangers recognised there was and paid with their lives [15].

References

[1] Beccy Speight, "The RSPB Magazine", Our Media Limited, Summer/Autumn 2024.
[2] Prof. K Raworth, "Doughnut Economics", Cornerstone.
[3] Nicholas Hales, "Engineering, Ethics and 'Doughnut' Economics", Safety Critical Systems Club, Safety Systems Newsletter Vol 32 No.1 February 2024 (https://scsc.uk/scsc-193)
[4] DEAL https://doughnuteconomics.org , accessed Sep 2024.
[5] Risk Assessment Chapter 9. Preliminary hazard analysis, https://www.ntnu.edu/documents/624876/1277591044/chapt09-pha.pdf
[6] David Hand "Dark Data – why what you don't know matters", Princeton University Press, 2020
[7] Data Safety Initiative Working Group "Data Safety Guidance V3.6", SCSC York University, 2024, https://scsc.uk/scsc-127I
[8] Bjorn Lomborg "The Skeptical Environmentalist", Cambridge University Press, 2001
[9] Bank of England, inflation calculator, https://www.bankofengland.co.uk/monetary-policy/inflation/inflation-calculator, accessed Sep 2024.
[10] Madelaine Cuff, "Dark Oxygen found in the deep", New Scientist, 27/7/2024
[11] Muriel Rabone et al, How many metazoan species live in the world's largest mineral exploration region?, https://www.cell.com/current-biology/fulltext/S0960-9822(23)00534-1
[12] James Dinneen; Mining Flowers for Nickel, New Scientist – 13/7/2024
[13] Reuters, Vale sees 44% increase in global nickel demand by 2030, https://www.reuters.com/markets/commodities/vale-sees-44-increase-global-nickel-demand-by-2030-2022-09-07, accessed Sep 2024
[14] Botanickel, using plants to extract nickel from soil and then turning that nickel into stainless steel, https://www.aperam.com/sites/default/files/documents/BOTANICKEL_EN.pdf
[15] NPR, https://www.npr.org/2020/02/03/802359415/sadness-and-worry-after-2-men-connected-to-butterfly-sanctuary-are-found-dead, accessed Sep 2024.

Image attribution: lead image: AI generated (Midjourney), doughnut: DoughnutEconomics, CC BY-SA 4.0 via Wikimedia Commons, three ring doughnut © Nick Hales, ocean floor manganese nodule © Walter Kölle licensed under the Creative Commons Attribution-Share Alike 3.0 Unported license. odontarrhena: Nina Filippova, CC BY 4.0, via Wikimedia Commons

Nicholas Hales

Nicholas Hales, (C.Eng), is a retired critical avionics engineer and project manager, formerly working in the MOD's Technology Office. His work involved de-risking technologies prior to full investment. He is currently a member of both the Data Safety and Systems Approach to Safety of the Environment, Safety Critical Systems Club working groups. He is currently looking forward to a second appearance as a pantomime actor, this time in an adult version of Aladdin.


Safety-Critical Systems Club
SCSC
FOR EVERYONE WORKING IN SYSTEM SAFETY
Safe Autonomous Transport - the Good, the Bad and the Ugly
Thursday 28 November, 2024
Munich, Germany
This 1-day seminar looks at progress in autonomous and highly automated transport and problems that have been encountered. It will also cover latest developments in the standards arena. It features talks from industry speakers and a discussion session.
The seminar is aimed at practitioners working in safety engineering including Safety Engineers, Safety Consultants and Safety Managers.
Speakers Include:
Simon Burton, University of York, UK
Safety Under Uncertainty: Automotive Standards for AI Safety and Research Perspectives
Alex Haag, Futurail
How Safe is Safe Enough for Autonomous Trains? Analyzing Human Performance as a Reference System
Torben Stolte, Volkswagen
ADMT's Approach Toward Arguing Safety for Automated Driving - An Introduction
Mario Trapp, Safe Intelligence, Executive Director Fraunhofer IKS, Full Professor @ TUM
Assuring Safety in the Face of the Unpredictable
thescsc.org/e1134

Women In Engineering: Reflections



Back in June, Wendy Owen wrote an article celebrating International Women in Engineering Day (INWED). The article was published on the SCSC website to tie in with the INWED event, which occurs on 23rd June every year. Wendy has kindly agreed to reproduce the content in this edition of the newsletter; this will help make the insights arising from her group discussion with prominent female system safety engineers available to as wide as readership as possible and ties in with Ada Lovelace Day (findingada.com) also celebrated this month.

INWED began in the UK in 2014 as a national campaign from the Women's Engineering Society (WES). Since then, it has grown enormously, receiving UNESCO patronage in 2016 and going global the following year. INWED promotes the amazing work that women engineers across the globe are doing and gives them a profile when they are still hugely under-represented. It plays a vital role in encouraging women and girls to take up engineering careers.

The Influence of WES

Since INWED started, many companies in the engineering field have developed diversity, equality & inclusion (DEI or EDI) Strategies, as we now also have in SCSC (refer to the website). We are also still actively trying to encourage more women engineers to join SCSC, and role models are important and affect recruitment. SSS'24, as far as conferences go, did very well with about a third of the audience being women – in my books, this is very high indeed so we must be doing something right! It is also certain that previous women featured in the SCSC newsletter do act or have previously acted as role models for other women in SCSC and associated professional societies, within their own organisations, and within the wider engineering community. If society has a dire need for more engineers, getting more women engineers on board and retaining them is a no-brainer.

The Pleasures and Perils of Awards

For every person who gets an award or bonus, there's often many more disappointed, disheartened or demoralised other people who didn't. So, generally, I'm not keen on awards. Having said this, last year WES did something interesting – they had one for the Top 50 engineers in "safety and security", with the next 50 getting commendations. You'd have thought SCSC and SaRS members would be easy pickings for this one, however, when the results were released, literally only a smattering of system safety engineers made the Top 100 cut. How could this have happened?!

Well, without sponsors or allies, or visibility, and people from other disciplines stealing the show, as individuals we have little chance at all of being recommended to either a) sit on an awards panel (thus influencing who receives the awards) or b) actually get an award. It was truly a lost opportunity for the system safety (and security) community. It was a one-off, the theme changes every year, so the chances of this topic coming up again during a working lifetime are probably improbable. Sometimes you only get one shot. For me, the whole episode reminded me of the Beckett quote here and that "Don't Quit" poem.

"Ever tried.
Ever failed.
No matter.
Try again,
Fail again.
Fail better."
Samuel
Beckett

Anyway, here we are, a year on, with our next INWED article.

The Advance of Technology on Transport Systems and the Realities of Recruiting

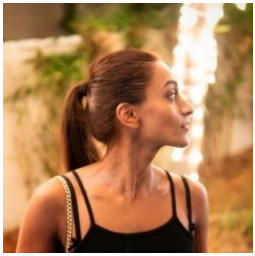
With this year's interviewees, a few common themes were noted in initial discussions; technology/software, transport systems (both civil and military) and recruitment issues. I proposed a group discussion. It included myself, Nicki Lerigo-Smith from Qinetiq www.qinetiq.com, Serrie Chapman from Women's Tech Hub www.wthub.org and Sindhura Lang from Ebeni www.ebeni.com. I had not met/spoken to any of them before. It went a bit like this…

Overview of Current Work Domains



Serrie I work in Autonomous buses on Safety. It's a relatively new field although I have been working with Safety Standards within automotive for years in semiconductors and also worked with the Safety team on the rail electrification programme. As it's so new, the standards are really playing catch up – it's a complex problem but will arrive in the not-so-distant future, and the UK is leading the way on Safety with the BSI 188x set of standards and the Autonomous Vehicle (AV) bill. We are very much involved in working on the standards and Cyber is also a major consideration as is AI usage within them. It's an exciting time and updating some of the more traditional standards to reflect the new concerns (Autonomy, AI and Cyber) is key to bringing in a more digital solution.

Sindhura I work as a Safety Engineer within Ebeni's Air Traffic Management (ATM) Business Unit and have worked on a number of ATM projects over the years, supporting ATM Equipment Manufacturers and Air Navigation Service Providers in getting new equipment/systems into operational service. I am currently working on Eurocontrol's Integrated Network Manager (iNM) Programme, supporting Eviden, a company specialising in Digital Transformation projects and working closely with Eurocontrol and Indra Safety, Quality and Security teams.



The iNM Programme is a digital transformation project with the aim of replacing Eurocontrol's core legacy systems such as Flight & Flow services and the European Aeronautical Information Service Database (EAD) with new digital architecture, hosted in a Cloud environment. Ebeni have adopted the Service Based Assurance approach developed by the SCSC Service Assurance Working Group scsc.uk/scsc-156D and have modified the approach to cater towards cloud-based services.

Nicki I work on a legacy military aircraft system which is undergoing an update for obsolescence and addition of newly developed systems, which incorporate more COTS than bespoke developments. New and updated systems bring many challenges that were not considered for legacy systems such as cloud-based technology, cyber security considerations and AI technology. These can bring many advantages but also introduce new hazards and require considerable effort to support qualification and certification of new and modified systems.

Wendy I'm not currently working in transport, although I worked in the rail and naval sectors for many years and currently sit on a regional Women in Rail committee. I'm predominantly working on legacy plant in the nuclear sector that are many decades old, which bring their own challenges in today's world. Never forget that, one day in the future (which could be next year or decades from now), all the new technology will turn into a legacy system. Full project and system lifecycle management is as crucial now as it ever was.

Complex Systems, Advancing Technology and Challenges to Standards

Wendy The systems I'm currently working on are largely analogue in nature, and physically/geographically isolated with no/few external interfaces. But even so, from a safety case perspective, there are considerations about the advent of cyber-security, drones and AI and 'the way things are going'. Even with long-standing operational systems, you cannot ignore the potential impact.

I do think safety has been given more attention in recent years, with people talking about Safe AI for example, as well as new regulations such as the Building Safety Act, an interesting development effectively dragging the construction sector more in line with existing sectors requiring a safety case.

I believe the instantaneous and high availability of news articles about accidents also influences levels of public concern.

Nicki My team do independent software assurance of safety-critical aircraft control systems, so we are very much safety-focussed. Traditionally, aircraft suppliers are

highly safety-focused and well-versed in software good practice in line with Air Recommended Practice (ARP) 4754/4761 and open standards such as RTCA DO-178.

We tend to see a different attitude from newer suppliers of innovative developments where safety seems to be a secondary consideration and priority is afforded to programme, cost and agile development methodology, rather than evidence-based engineering and application of hazard analysis and risk reduction techniques.



Societal acceptance and reaction to accidents from the advent of new technologies tends to influence change in safety legislation and will lead to the development of enhanced safety standards and legislation. Developers need to be aware of this and ensure that they develop to meet relevant certification in order to have products that are fit for purpose and meet safety requirements at the required safety integrity level.

Serrie The different approaches from countries are interesting, some companies and countries are going for a much less safety-based approach. I believe that the UK, the BSI, ISO and CCAV (Centre for Connected and Autonomous Vehicles) are all taking a very measured approach to the issues that are arising. Safety is a primary concern and being taken very seriously with a Safety-first approach. The key issues that I am seeing with some parts of the industry is, due to the standards and legislation following the tech solutions, it's causing concern with the public with their approach to some of the unregulated areas. This may affect the industry as a whole so the usual competition between companies to be the first to achieve solutions is not necessarily a good thing, as we have seen with Cruise and Tesla as examples. It is definitely an industry that has Safety as first and foremost as a concern though so, when the legislation catches up, I believe it will ensure that the right companies with the safest approach are the more likely to succeed.

Sindhura Ebeni is a consultancy that specialises in Safety Engineering, Assessment and Assurance, so Safety is always at the heart of any project we undertake. As Nicki and Serrie have mentioned, there are companies with a much more relaxed attitude towards Safety, who often view Safety as a tick-in-a-box exercise, but I've also found that these companies tend to change their attitude a little when they realise the influence Safety has when it comes to getting approval from the Competent Authority to enter operations with a new system/service.

Conversely, with the emergence of cloud-based technologies, there is a risk of playing things a little "too safe" and over-engineering solutions due to the challenges faced when trying to assure cloud-based services. This is something that could be managed with the adoption of new assurance methodologies.

Selling Safety as a Career for Women Engineers

Wendy We know there's a general dire lack of engineers, and we know there's a dire lack of women engineers within that picture. I'm currently employed as an associate/contractor, although not through choice, and I see others in similar situations. Very unusually, and even very ironically, I currently find myself working with a fairly high proportion of other women engineers, so there is hope out there.



There's a dire lack of engineers with experience in the nuclear sector at a time when the energy sector is going through a renaissance, but many thousands were laid off in the 90s, and the sector has effectively been dormant since. The workforce tends to be a mix of early career professionals and very experienced staff/experts, but not much in-between. This is simply down to historic reasons and, in my experience, much less prevalent in other UK sectors in regards balanced demographics of workforces.

Nicki In an ideal world there would be a pool of suitably qualified and experienced candidates to draw from. In reality, there is a deficit of software safety engineers and consultants with relevant scarce skills to satisfy job demand. This can price the best candidates beyond project affordability. The way that we are dealing with this is to make significant efforts to retain trusted and experienced staff members and execute a succession plan to recruit and train graduates and less-experienced personnel. It requires considerable effort with respect to developing people to satisfy future demand and balance that against urgent deliverables which must be supported by more experienced personnel, some of whom are contractors, to manage peaks and troughs in demand.

Serrie As Wendy and Nicki have pointed out – there is a lack of safety engineers, engineers with the relevant skills and women in the industry. Interestingly I am seeing more women in the safety realm in this area than I have seen previously in other more classical engineering areas. The other thing I am noting is that the backgrounds of the safety engineers is a much broader spectrum, from software, hardware, engineering and Human Factors, which all need careful consideration. I run a company called Women's Tech Hub, which supports women moving into tech and it has many women returners who have experience in the separate areas that are needed, but not the skills, confidence or training to move back into the industry. I believe they are a great untapped resource who could be reskilled into Safety and would solve a lot of the issues – if we could see some affordable reskilling options for these women then it could be a solution. The apprenticeship schemes would be a great solution here, but I don't see many schemes based around engineering, let alone Safety.

Sindhura I completely agree with Nicki's points – there is a general lack of Software Safety Engineers – regardless of gender, and there is a reliance on retaining trusted and experienced staff while trying to recruit and train graduates or less-experienced personnel. Additionally, finding candidates who are experienced and comfortable

in a heavily customer-facing role from the start, as is often required within a Consultancy environment, also adds another layer of complexity. I would also like to echo Serrie's point about seeing more women in the Safety realm than in more classical engineering areas – I would say that there is a growing representation of women within the Safety industry, particularly within the ATM domain, including women within management/senior management positions.

Advice to Hiring Managers

Nicki I would suggest casting your net wide and offer retraining to candidates. Bring in candidates of all ages and levels of experience from apprentices and graduates to principal engineers/consultants and managers to build well-rounded teams and support personal development with formal training, in-house training and work-shadowing/mentoring from more experienced personnel. Offer hybrid working and support carers and part-time workers to enhance inclusion and diversity in the workplace.

Sindhura Offer remote/hybrid working contracts. Over the pandemic we've learned that much of what we do can be done remotely and I've found that many clients now prefer to hold meetings online to save travel costs. By offering remote/hybrid working possibilities, we can cast our recruitment net wider given that potential candidates are no longer tied to office locations or surrounding areas. I currently work with a geographically diverse team spread across Europe, from the UK to Belgium, Poland, Romania and Spain; we interact daily without issue and meet face-to-face at the Eurocontrol office in Belgium when a face-to-face meeting or workshop is needed. Additionally, I've also found that mentoring and coaching of more junior staff is also possible remotely, with face-to-face meetings as and when required. It goes to show that remote working can be done and does not hinder project progress.

"Over the pandemic we've learned that much of what we do can be done remotely… and does not hinder project progress"

Serrie In Women's Tech Hub we suggest using a tool to avoid gendered wording on jobs – gender decoder is a great freebie although a bit basic. People don't want rockstars to code safety-critical systems! I believe that wording the adverts to explain that safety is a career that is there to protect people and assure that tech companies are not running ahead and putting people at risk is something that will entice women into the industry. Many companies tend to replace with like by like ... 'bob' did x, y and z so we need someone with that skill base, it's not always true as 'bob' either didn't do all they stated or they didn't actually do the work as others were doing it, or someone like 'bob' were at a stage that they were ready to move on – so taking on the same skill set is not necessarily good as they are also at a stage where the company cannot offer them onward career progression (else 'bob' wouldn't be leaving in many cases). I believe that recruiting from within and training into a role gives you a better solution. Upskilling within the workplace from below and using that as a clear career progression is a great opportunity to get loyalty and people are grateful for a culture that's supportive and gives flexibility.

Wendy Review your job adverts harshly, especially for hard-to-fill positions. I was recently unemployed; it took me 8 months to find work because I couldn't work full-time nor travel. I ended up going self-employed to get any work in at all. There are still far too many restrictive recruitment policies and work patterns around, which closed off many doors/opportunities. Many of these jobs can be done remotely and flexibly, but many line managers (or their clients) won't even entertain the idea, even for very experienced hires. A big cultural shift is needed to account for disabled workers and those with responsibilities, or simply those who wish to work part-time. Also significantly improve paternal leave for male employees and make it normalised, it's long overdue.

Final Thoughts

Serrie Most companies are keen to get women in – unfortunately it is very slow to change cultures and while they believe they are doing well getting loads of women through STEM into early careers, eventually those women get disillusioned due to the bias within engineering. We hear arguments like we have to take the best person for the job – but surely as women often out-perform in their degrees that questions whether they have got the best people in, the biggest issue is families and the breaks in careers and we often hear that the women aren't welcome back after a break – and the women also aren't keen to come back due to the bias they saw in their earlier career progression. It's not that women are being given an unfair advantage when they have taken a 'break' or that their brains disappeared when they had children, it's more that they didn't have a network to get back in or the acceptance from the industry to come back in at the level they left at.

" … the number of women in senior roles after a career break is woeful – they don't want special dispensation … they say they no longer have the energy for the fight (and why should they be fighting for a career they love and are good at?)"

Reskilling and support and returners incentives are great, but it needs the male engineers to understand that they are still equal and also to allow themselves to be managed by women who have taken a break and are still highly skilled managers. This is a bugbear of mine – the number of women in senior roles after a career break is woeful – they don't want special dispensation but some flexibility and accepting that they are in many cases the best person for the job. This is not considered from my experience talking to women in the industry, so they walk away to work in 'easier' industries, as they say they no longer have the energy for the fight (and why should they be fighting for a career they love and are good at?)

Nicki Perhaps introduce financial incentives to work placement students to get them into the workplace once they have attained their degree. Most would appreciate financial support to enter the workplace and may be more likely to stay with that company for a long duration. Workplace liaison with – and support to – universities and

visibility of safety engineering courses and career options would improve the situation. The confusion with health & safety advisors also doesn't help sell systems safety as a line of work and detracts from the engineering aspect.

Sindhura Young Safety Engineers are very few and far between – you don't often come across Graduates who immediately know they want to be a Safety Engineer straight out of university, and this could be due to a lack of understanding of what Safety Engineering entails, at least this was my experience as a Graduate. This could potentially be tackled by exposing students to Safety Engineering through modules/group projects within their Undergraduate courses, or as Serrie mentioned earlier, through apprenticeships focused on Safety (although these are also rare).

I'd also like to highlight the importance of trying to be a good role model for young engineers, particularly young women, who are early in their careers and can find the engineering industry a bit daunting at first. I've been fortunate enough to have met and worked with a number of great women and men over the years, some of whom have helped me advance in my personal and professional growth without them realising – all because they shared advice (both professional and general life advice) and set a good standard to aspire towards.

Wendy WES is now over a hundred years old. One day I hope there won't be a need for it, but I don't think it will be within my working lifetime. I have been mentoring disadvantaged students taking STEM subjects for several years now (via Brightside) but have yet to be matched with any female mentees at all. This makes me sad, but it also makes me not want to give up.

"…for several years now… I have yet to be matched with any female [student] mentees at all… "

Final Words

As per last year, the main message is, please, give women engineers a chance. Also, please challenge restrictive recruitment policies/adverts, especially for hard-to-fill positions. And, maybe, don't forget to put your women safety engineering colleagues forward for awards – even if they fail to get one, at least they will know that you believe they're worth it. Or if you're like me and dislike awards, try to advocate for them and be an ally in other ways.

Well, we hope you have enjoyed reading this article. This article is dedicated to all the women engineers working in safety, their allies in the workplace, and their supporters behind the scenes. Also, Women in Science and Engineering (WISE) and WES.

Wendy Owen

Wendy has 35 years' experience in systems assurance across a wide range of highly regulated industries covering energy, defence, transport and process sectors. Her career has largely been in engineering consultancy, also with time in manufacturing, regulatory and research. She is a Fellow of the Safety & Reliability Society and WES. She is currently self-employed, at time of writing working as an associate for Building a Safer Future (set up in the wake of the Grenfell fire) and Mott MacDonald (on Sellafield projects).

The author retains copyright of this article.

Photos courtesy of individual LinkedIn profiles and inwed.org.uk.

Seminar: Frameworks for Safe AI Systems



The "Frameworks for Safe AI Systems" seminar was held at the IET in London, on 25th April 2024 and hosted by Mike Parsons. The speakers examined the legal, ethical and regulatory frameworks around AI, as well as considering the social and societal implications of use of these systems.

The six speakers presented insightful and compelling angles on development and using frameworks for safe AI systems, covering a range of topics such as:

- George Mason (Frazer-Nash): An Introduction to Safe AI – definitions, debates and comparisons between different AI techniques, plus the underrated importance of education
- Mark Sujan (Health Services Safety Investigations Body): Human-Centred Healthcare AI – putting the human back in AI, the tricky doctor-patient relationship and AI hype vs reality
- Zoe Porter (Assuring Autonomy International Programme): A Framework for the Equitable Safety of AI-based Systems – socio-technical systems, what happens when the risk-bearers aren't the beneficiaries, and the difficulties of reconciling ethics and regulation
- Dai Davies (Percy Crow Davis & Co): De-mystifying AI – the law and AI, limitations on practical uses of AI and the all-important conundrum of human equivalence
- Phil Mulvana (UKAEA): Design Frameworks for Autonomy – a strawman safety case using SACE, plus a real-world system that's a prime candidate for AI introduction
- Gabriel Pedroza (Ansys): Design, Exploration and Evaluation of Safety-Critical Software for Integrating AI-based Algorithm – a framework to address and explore AI safety, the three axes of autonomy, and the pillars to improve AI maturity

George Mason



George Mason got the day off with a bang by challenging us to consider whether we could all, in fact, define AI (stealing the thunder from our attempt when he confirmed that no single universally-accepted definition exists!) He talked us through the potential harm that could be caused by AI, and invited us to consider how recently safety has even been a key focus of AI at all.

Moving on to the legal side of things, George introduced us to the EU's AI Act, approved in February 2024, with a key priority to uphold human rights, this is one of the most significant advancements of AI regulation. The UK's approach, by contrast, aims to balance safety with innovation which is always going to be a tricky tipping point.

George walked us through the AI Standards Hub for a quick glimpse of the comprehensive database of AI standards, pointing out that most legislation is still under development or non-existent. The rate of AI development outpaces the rate of AI legislation development; this observation had some loud agreements from the lawyers in the room! To finish up, George emphasized the importance of education in terms of understanding AI: if we don't know how to use these systems safely and reliably, he asked, then how can we be sure of the potential harm they might be causing?

Mark Sujan

Mark Sujan was up next, with one key message for us all: language matters! He took us through the ways AI might be used in healthcare, from monitoring of disease outbreaks via social media (a reason to get back on Facebook?) to appraisal of literature to scheduling of operating-room time. We were intrigued to hear about some ChatGPT hallucinations that have popped up when it's asked medical questions; in some cases it has claimed to have a "masters degree in public health and personal experience with type 2 diabetes" (!!)



Next, Mark moved onto AI hype vs AI reality, noting that very few people are working on last-mile AI, i.e. the real-world implementation of AI into healthcare systems. One example of this would be using AI to help answer emergency calls. It was edifying – if unsettling – to brainstorm all the ways this interaction might go wrong with AI in the mix, but one question kept coming up again and again: will call handlers have the confidence and authority to override the AI when they think it's wrong?

Mark then talked us through the ways in which AI might change the relationship between a doctor and a patient, and queried the extent to which organisations are ready to adopt AI. Certainly many of them are keen to do this but – in an echo of the same concerns brought up earlier – there are distinct question marks over whether these organisations truly do have the AI literacy and capacity to manage this.

Zoe Porter

Zoe picked straight back up on the healthcare concerns, this time looking at them from an ethical perspective. She introduced us to the PRAISE framework (Principles-based Ethics Assurance, an inspired acronym!) for putting together ethical assurance cases. We learnt about the four+1 ethical principles of non-maleficence, beneficence, respect for autonomy, justice (+ transparency).



Regulation continued to be a hot topic here, as Zoe told us: regulation focuses on risk and safety, with very little around ethics of AI being legally required. The legal and regulatory constraints – or lack of them – of AI was certainly emerging as a common theme for the day! Zoe invited us to consider the difference between attempting to construct a top-down vs bottom-up ethics assurance case, this being the difference between assuring a single ethical property or a suite of ethical properties.

Zoe also took us through an example of the PRAISE framework: the DORA system is a conversational AI agent, used for follow-up calls after cataract surgery. I think we were all realising just how much conversation and dialogue is involved in the healthcare field by this point, and becoming increasingly well-informed of AI's ability (or lack thereof!) to carry out such conversations safely and ethically.

Dai Davis



Following a break for lunch, Dai Davis challenged us to think explicitly about what the law requires of AI, which was certainly a question on everyone's minds after the morning talks. He invited us to consider the training data for ChatGPT 4: this is in the public domain, and ended in September 2021. While augmented Large Language Models (LLMs) – being LLMs trained on specialised and updated text – can go some way to addressing concerns about these systems being out of date, the environmental issues remain a major problem. Dai illustrated this by showing us that it would take the amount of water required by the entirety of Chester for a month, just to run the servers! (Which would you rather have: Chester or ChatGPT?? Now there's an ethical conundrum…)

Dai moved on to talk about the limitations of AI and to consider what the human equivalent of machine learning would be: hyperthemesia, which for those of us new to the word, means a photographic memory. However, he cautioned us about trying to find true human equivalents: humans, he warned, can certainly censor information, but they do so with knowledge of what the true answer is. Systems like ChatGPT censor without having the full information, a much more dangerous set of circumstances.

Finally, Dai took us through some apposite – and fascinating – legal observations. We discussed Henthorn vs Fraser (withdrawing an offer to sell a house, after the acceptance of this offer was already popped into the post box); the advent of email would surely have made this kind of situation vanishingly unlikely. He also took us through the timescales for a law to go from proposal to implemented legislation (10 years, which surprised many of us!) and highlighted some of the ways in which the Copyright, Designs and Patents Act is unfit for purpose against AI.

Phill Mulvana

Phill picked back up on the theme of frameworks, introducing us to the SACE framework (Safety Assurance of autonomous systems in Complex Environment) for building an autonomous safety case. The application system was particularly interesting: the "gloveboxes" used in the nuclear domain to allow handling of items that are hazardous to humans. As Phill's slides showed, this work requires not only a highly skilled operator, but can be particularly uncomfortable for humans to do at all.



The high-level view of the project Phill presented emphasised input from key stakeholders to feed into the AI assurance case, as well as real hardware validation. There were some very interesting reasons why SACE is well-suited to construct the strawman, most notably that it is domain-agnostic. As Phill noted, this pre-empts any potential objection that you can't use – for example – a medical framework in a nuclear setting!

Phill gave us a few more behind-the-scenes observations, including noting that the team did not do the traditional safety and compliance process. They were given eleven months and did the first four planned phases:

1. Operating context assurance
2. AS hazardous scenarios ID
3. AS hazardous scenarios ID (again)
4. Safety requirements assurance.

He also described how some of the later stages might work, and finished with some great lessons learnt, including the very timely recommendation to assess whether AI is indeed truly essential for a given system!

Gabriel Pedroza

Last but certainly not least, Gabriel Pedroza took us through a methodology to design, explore and assess AI safety. Gabriel first invited us to consider the challenges for AI development, including the three axes of autonomy: environmental complexity, mission complexity and human independence. The ideal of an AI system is to mimic human physical, biological and social features, but as Gabriel described to us, the broad range of uncertainty makes this easier said than done!



Gabriel introduced us to a methodology for certification of AI, focusing on three standards or documents: ARP-6983, EASA Concept Paper V2, ISO PAS-8800. The fundamental point made here – as we've heard in previous talks – is that safety does not change in different domains. Quite a timely reminder here, in that it's very easy to become immersed in one domain and forget the transferability of safety principles!

Finally, Gabriel took us through safety assessment, using this methodology, of the UC-F16 Flight Formation. Some fantastic videos really showed the challenges of this and helped to give us a real idea of the context. The talk finished with a discussion of the pillars of AI maturity improvement: a common theme throughout the presentations has been the need to consider just how AI systems can be improved and matured!

Mike Parsons – Wrap Up

Mike Parsons finished the day by leading a general discussion, with the thought-provoking question: what would happen if you asked ChatGPT to suggest a framework for developing safe AI?? Mike had, in fact, done just that, and the results were surprisingly good. The problem – as quickly identified – is that using these kinds of systems will get you 90% of the way there, but unfortunately human nature is such that it's very easy to then stop thinking about the remaining 10%.

All in all, this was a very interesting and lively day, with some fantastic insights into AI frameworks and the challenges that must be overcome.

Report by Catherine Menon.

Catherine Menon is a principal lecturer at the University of Hertfordshire. Her research focuses on the intersection of trust, safety and ethics in public-facing autonomous systems. She has a PhD in category theory and has worked across industry and academia and has been involved in the development of regulatory standards and guidance for safety, security and ethics assurance within autonomous systems.

Seminar Report: Developing Safe AI Systems



All images © Alex King and Mike Parsons

The "Developing Safe AI Systems" seminar was held at the BCS in London on 27th June 2024. This seminar was all about how to develop and build safe AI systems: it discussed the methods, tools and techniques that should be employed, the all-important approach to testing and V&V, and the quality and safety assurance processes that govern what has to be done. The speakers outlined possible ideas and approaches for these evolving areas.

The five speakers presented insightful talks on developing safe AI systems, covering a range of topics:

- Richard Hawkins (University of York): Through-life assurance of ML systems
- Alan Simpson (Ebeni): Where are we with AI Safety?
- Iain Whiteside (ReSim): Testing Times Ahead for AI
- Gary Brown (Airbus): Certification Use Reliance (CURe) for an Aircraft Level view of an AI ML Part 21 integration
- Nick Tudor (D-RisQ): Robust AI Planning

There was also a discussion: do we have what it takes to develop Safe AI?

Richard Hawkins

Richard presented the Sense, Understand, Decide, Act (SUDA) model[1]. A question was asked about different driver behaviour in different countries. Richard replied that the fact the Machine Learning (ML) is safe in the UK doesn't mean it's safe in China. That's why requirements are so important.



Richard spoke of the importance of independent testing. Developers shouldn't know the verification dataset, otherwise they might train the system to pass the test. The testers should deliberately try and get the system to fail. The testing has to be realistic.

Richard also spoke about the importance of lifelong assurance. There can be unpredicted changes to the operating environment. How do we respond to maintain assurance?

Richard spoke about ML safety monitors. He cautioned that trying to characterise what an unsafe output looks like can be very difficult.

A question was asked about whether you could use completely simulated images. Richard replied that some people have given up using photorealistic images. Although the images look good to the human eye, different features are being activated in the ML. Self-driving car companies are using real-world images they've collected instead.

Alan Simpson



Interestingly, Alan's PowerPoint slides had been generated by AI. They were pretty good, but contained some hallucinations and a spelling mistake.

Alan presented the work of the SCSC Working Group on AI Safety, which leads on from the work of the Safety of Autonomous Systems Working Group.

Alan spoke about current research in AI for functional safety, including a plug for our friends at the University of York and their Body of Knowledge [1]. He also spoke about the IET report on The Application of Artificial Intelligence in Functional Safety [2] and the recently published ISO/IEC TR 5469:2024 on Artificial Intelligence – Functional safety and AI system [3].

It's difficult to keep up with the rapid changes in AI. Do we need more guidance, for example on how to deal with AI hallucinations? A key problem is that generative AI can make stuff up.

A survey by the Ada Lovelace Institute [4] found that the public doesn't see much benefit in self-driving cars and are concerned about them. A maxim from civil aviation is that you should only make a change if there is a notable improvement to operations or efficiency and no adverse effect on safety, or if there is an improvement to safety.

[1] Unfortunately, I missed the first half of Richard's presentation because my train, along with many others, was delayed due to a fatality between Reading and Paddington. Fortunately, Mike Parsons gave me a copy of his notes and I was also able to catch up with Richard's talk on the SCSC website.

Alan looked at how good is generative AI? A medical study of Large Language Model (LLM) accuracy in diagnosis found that ChatGPT 4 was 87% effective but was poor with rare or masquerading diseases.

Alan said there is increasing regulation and guidance on AI from the UK government and the EU (the AI Act).

Alan ended with a call for people to get involved in the Working Group, which would like to reach out to the wider safety community for concerns.

Iain Whiteside



Iain talked about embodied AI, which is AI that interacts with the world in some way in support of a task.

He made a distinction between the AI subsystem and downstream. Traditional ML metrics like precision/recall fade into insignificance. You need domain-specific metrics. He gave the example of 3D bounding boxes for autonomous vehicles, where larger errors are tolerable for objects further away.

I liked that he recognised the difference between verification and validation. The latter includes detecting contract breaches during real-world driving and downstream failures that occur without a contract breach.

In the early stages of full self-driving, it was easy to make progress. You didn't need much testing to find problems and improve. Almost every autonomous vehicle company took this route, but you grind to a halt. Enter video game designers. Teams started to build closed-loop simulators. However, different parts of the neural network light up when using simulators compared to the real world, even though the images look photorealistic. Waymo has driven over 2 billion miles in simulation, but self-driving continues to be just around the corner. The generative AI companies are making the same mistakes.

It's too much fun for robotics engineers to tinker with actual robots. There is a gap between systems engineering, robotics, ML and safety engineering. Software developers are interested in point-of-time tests. Safety engineers are interested in a more holistic approach. Systems engineers live in between.

Iain concluded that real world testing is precious but is also storage intensive. We need to be able to extract the most value from it.

Gary Brown



Aviation is a highly-regulated and safety-critical domain. Companies don't put ML on an aircraft if they don't need to – it's not a gimmick.

The certification basis remains CS-25. SAE ARP6983/EUROCAE ED-324 [5] is a draft Process Standard for Development and Certification/Approval of Aeronautical Safety-Related Products Implementing AI. ARP6983 is a consensus-based standard that provides a Learning Assurance Level (ML-DAL) with an associated set of objectives.

Gary talked about three pillars: Certification, Use, Reliance (CURe).

Nick Tudor



Nick gave a very interesting presentation on Robust AI planning. He described an autonomous vehicle that uses AI to allow real-time re(planning) on board the vehicle with no need for intervention by a human. This would particularly allow autonomous operation in environments with poor communications links such as underwater and inside buildings.

However, it's not possible to assure the behaviour of AI, so the system architectures 'cages' the AI with predictable behaviour. Formal proof of the safety monitor guarantees that the boundary cannot be violated and provides assurance behaviour. This enables the benefits of AI, while providing the necessary safety and security assurance.

The system is built using Planning Domain Definition Language (PDDL). Many general purpose solvers for PDDL-expressed problems exist, but these planners are constrained by the computational resources available on-board an autonomous system and they return plans in minutes or hours. D-RisQ will produce domain-specific real-time planners that are implemented using FPGAs, which allow parallel processing and are therefore massively efficient, allowing replanning in a few seconds. The PDDL is transformed into the hardware description language, VHDL, for implementation. A formal proof is conducted that the VHDL preserves the required safety properties of the PDDL.

References

[1] University of York, Centre for Assuring Autonomy, "Body of Knowledge", www.york.ac.uk/assuring-autonomy/about/aaip/body-of-knowledge
[2] IET (theiet.org), "The Application of Artificial Intelligence in Functional Safety", electrical.theiet.org/media/ifbjt25i/the-application-of-artificial-intelligence-in-functional-safety.pdf
[3] ISO, "Artificial intelligence – Functional safety and AI systems (ISO/IEC TR 5469:2024)", www.iso.org/standard/81283.html
[4] Ada Lovelace Institute, "How do people feel about AI?", www.adalovelaceinstitute.org/report/public-attitudes-ai
[5] SAE International, "Process Standard for Development and Certification/Approval of Aeronautical Safety-Related Products Implementing AI – ARP6983 (WIP)", www.sae.org/standards/content/arp6983

Report by Dewi Daniels

Dewi Daniels is an expert in the development and verification of safety-critical software. He has worked on many software projects across many industries. He is a Fellow of the British Computer Society. He was a member of the committee that wrote DO-178C and he is currently one of the experts representing the UK on the IEC 61508 committee.

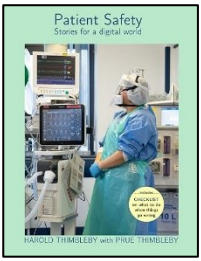
v


Vol 3, Issue 2
The Safety-Critical Systems Club
SAFETY-CRITICAL SYSTEMS eJOURNAL
SCSC
FOR EVERYONE WORKING IN SYSTEM SAFETY
scsc.uk/scsc-196

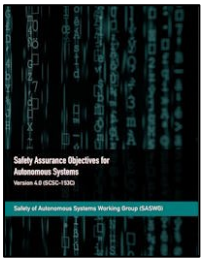
Recent Safety Publications



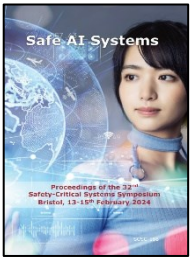
Safety-Critical Systems eJournal vol.3 no.2
Summer Issue 2024
scsc.uk/scsc-196



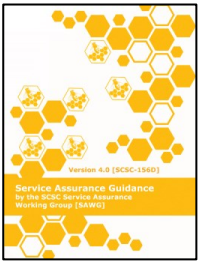
Patient Safety – Stories for a digital world
www.amazon.co.uk/dp/1399975420



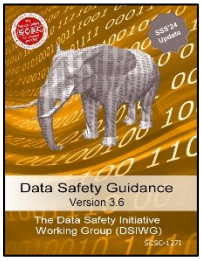
Safety Assurance Objectives for Autonomous Systems.
scsc.uk/scsc-153C



Proceedings of the 32nd Safety-Critical Systems Symposium.
scsc.uk/scsc-188



Service Assurance Guidance Version 4.0. Jan 2024
scsc.uk/scsc-156D



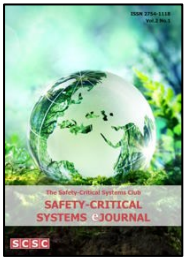
Guidance on the management of data safety risks (V3.6)
scsc.uk/scsc-127I



Safety-Critical Systems eJournal vol.3 no.1
Winter Issue 2023
scsc.uk/scsc-191



Safety Culture Working Group Position Paper Edition 1. Dec 2023
scsc.uk/scsc-189



Safety-Critical Systems eJournal vol.2 no.2
Summer Issue 2023
scsc.uk/scsc-186

60 Seconds with ... Nick Hales



Nicholas Hales, (C.Eng), is a retired critical avionics engineer and project manager, formerly working in the MOD's Technology Office. His work involved de-risking technologies prior to full investment.

He is currently a member of both the Data Safety and Systems Approach to Safety of the Environment, Safety Critical Systems Club working groups.

He is currently looking forward to a second appearance as a pantomime actor, this time in an adult version of Aladdin.

What first attracted you to working in the field of System Safety?

When living in Denmark as a hotel warden I discussed the hazards of a skip of mattresses igniting close to the hotel. I realised I had no comprehension of how to analyse that. From then I seemed to walk the path unconsciously until joining the MOD safety efforts.

What aspect of your career are you most proud of?

My ability to understand when the plug needs to be pulled on a project. It saves a lot of money.

Tell us one interesting unusual fact about yourself!

I used to organise an annual alternative fashion show.

What advice would you give to yourself age 12?

Never drop your guard. Darwin explained why.

"If you could be any fictional character, who would you choose?"

From a philosophical point of view, Ivan Fyodorovich Karamazov in "The Brothers Karamazov" by Dostoyevsky, but while he speaks many truths he does not seem able to change things for the better. Hence from a more pragmatic point of view, Arnold Schwarzenegger's character, Major Alan "Dutch" Schaefer in the film "Predator" would be my choice, because he succeeds in killing his demon that left him friendless, (in a psychological analogy), and survives.

What future changes would you like to see in the field of System Safety?

More effort put in to avoiding damaging the environment.

What's your most favourite quote or motto?

Beston's wise words: *"We need another and a wiser and perhaps more mystical concept of animals.... We patronise them for their incompleteness, for their tragic fate of having taken form so far below ourselves. And therein we err, and greatly err. For the animals shall not be measured by man. In a world older and more complete than ours they move finished and complete, gifted with extensions of the senses we have lost or never attained, living by voices we shall never hear. They are not brethren, they are not underlings; they are other nations, caught with ourselves in the net of life and time, fellow prisoners of the splendour and travail of the earth"*

If you could learn to do anything, what would it be?

How to save children from cancer, though a system approach to safety of the environment may lower the risk of some cancers.

Artificial Intelligence - a positive revolution or are we all doomed!?

The positive revolution will come once we realise we are doomed if we do not have a revolution.

Tell us more about your acting career!

Age 13 won the school interhouse drama competition, age 14 played one of Noah's sons in Britten's opera for schools, then 50 year gap. Now looking forward to third comedy role in 6 years.

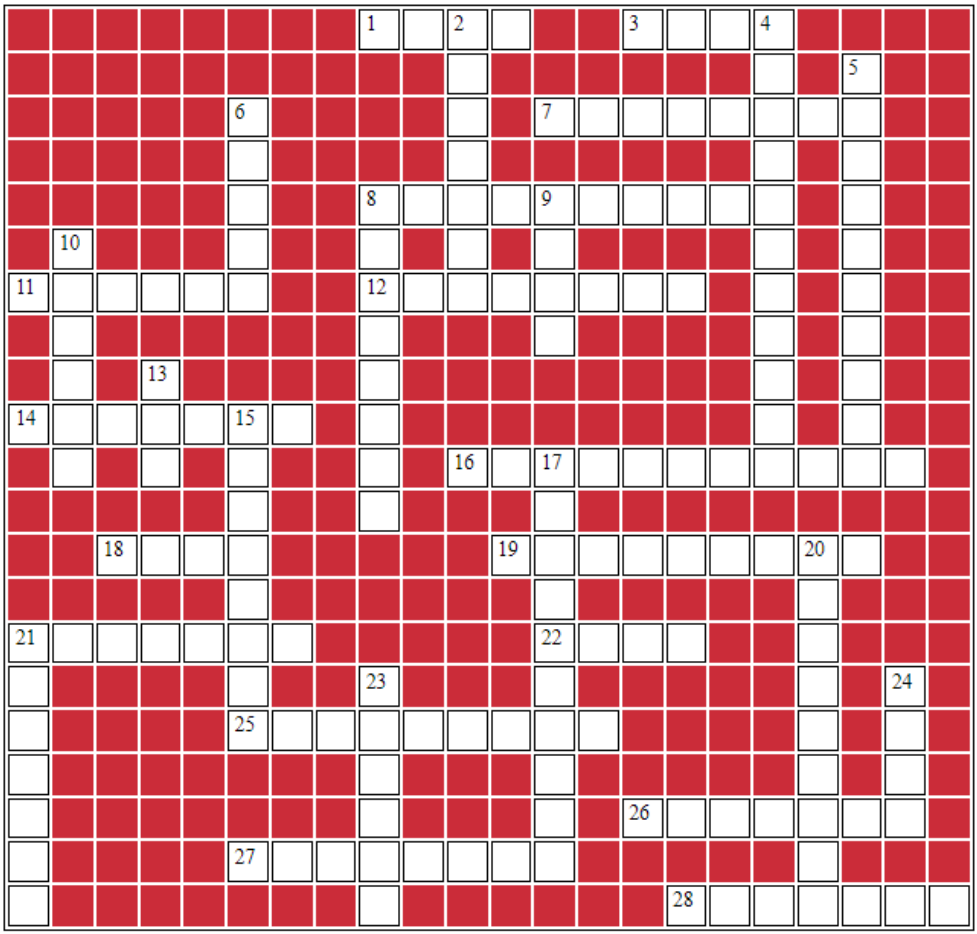


Safety Systems Crossword

Welcome to the 3rd Safety Systems Crossword prize competition where you can test your knowledge of the world of System Safety!

Send you completed grids to crossword@scsc.uk or drop into the crossword entry box at SSS'24 by 1pm on 5th Feb 2025.

The first correct answer drawn from a hat at SSS'25 will win a £100 gift voucher!



Across

1 Driver crash-protection system comprising a curved bar placed above the driver's head (4)
3 Abbreviation for a form of aerated concrete said to be at risk of collapse with little or no notice (4)
7 Town where the 'Flying Scotsman' steam locomotive crashed in 2023 (8)
8 Name of the project aiming to push the world land speed record beyond 800mph (10)
11 Safety device designed to keep a sailor attached to their boat (6)
12 A set of concepts in a subject area that shows their properties and the relations between them (8)
14 Device that uses a powerful magnetic field to confine plasma (7)
16 Uncrewed aerial vehicle used by the British Army (11)
18 Form of certification signifying the airworthiness of a particular category of aircraft (4)
19 Project that delivered the commuter rail and rapid transit system, known as the Elizabeth line (9)
21 Surname of the woman who led a government review in the wake of the Grenfell Tower tragedy (7)
22 Abbreviation for the mark of conformity with requirements for products sold within Great Britain (4)
25 Class of partially reusable spacecraft to transport crew to the International Space Station (9)
26 Surname of the first female pilot and commander of a Space Shuttle mission (7)
27 Form of cruise control that automatically maintains a safe distance through by speed adjustments (8)
28 Surname of an American specialist in system and software safety and author (7)

Down

2 Surname of the computer scientist famous for his treatment of the "Byzantine General's Problem" (7)
4 Firm that reportedly caused the largest outage in the history of information technology (11)
5 A form of AI used to create new content such as text, images, music, audio and videos (10)
6 Abbreviation for a remote sensing method that uses pulsed laser light to measure distance (5)
8 A symmetric-key block cipher, designed in 1993 (8)
9 Name of the ship that lost power before veering off course and striking a bridge (4)
10 Surname of an author of books on human error and famous for his 'Swiss Cheese Model' (6)
13 Abbreviation for the agency that regulates civil aviation in the United States (3)
15 A group of fibrous minerals used to fireproof materials, whose use is now largely banned (8)
17 Hazardous unstable air movement caused by changes in wind speed and direction (10)
20 Reasoning that makes predictions about what might happen based on what is already known (9)
21 IT System implicated in the wrongful prosecution of hundreds of employees (7)
23 A piece of text or information that helps direct an AI's response to a request (6)
24 Abbreviation for a satellite constellation that provides positioning, navigation and timing services (4)

Name: _____

Contact Nos/email: _____

Connect

The Newsletter and eJournal

Do you have a topic you'd like to share with the systems safety community? Perhaps an interesting area of research or project work you've been involved in, some new developments you'd like to share, or perhaps you would simply like to express your views and opinions of current issues and events. There are now two publishing vehicles for content – shorter, more informal content, can be published in the Newsletter with longer, more technical peer-reviewed material more suitable for the eJournal. If you are interested in submitting content, then get in touch with Paul Hampton for Newsletter articles: paul.hampton@scsc.uk or John Spriggs for eJournal papers: john.spriggs@scsc.uk

The SCSC Website

Visit the Club's website thescsc.org for more details of the Safety-Critical Systems Club including past newsletters, details of how to get involved in working groups and joining information for the various forthcoming events.

Facebook

Follow the Safety-Critical Systems Club on its very own Facebook page.

www.facebook.com/SafetyClubUK

X/Twitter

Follow the Safety-Critical Systems Club's X/Twitter feed for brief updates on the club and events: @SafetyClubUK

LinkedIn

You can find the club on LinkedIn. Search for the Safety-Critical Systems Club or use the following link:

www.linkedin.com/groups/3752227

Advertising

Do you have a product, service or event you would like to advertise in the Newsletter? The SCSC Newsletter can reach out to 1,000's of individuals involved in Systems Safety and so is the perfect medium for engaging with the community. For prices and further details, please get in touch with the Newsletter Editor.

SCSC Working Groups

Safety System Architecting

The SCSC Safety System Architecting Working Group (SSAWG) is a joint initiative between the INCOSE UK Architecture Working Group and the Safety Critical Systems Club, with a vision of addressing systems safety through the promotion of choosing, using, and developing appropriate architecture. Two focal areas are defined as:

- Safety-driven architecting – what safety drivers are likely to exist when architecting is being considered.
- Architecting system safety – what architectural factors may realise, enable, support, or preclude the achieving of safety considerations.

The groups Mission Statement is:

- To produce practical guidance on addressing system safety during system architecting.
- To encourage and facilitate collaboration between INCOSE and the club.

Statement of the Problem

The design of a system architecture is a critical first step toward addressing safety requirements. With the community moving toward digital engineering to include model-based systems engineering, digital twins and digital threads, there is an opportunity to advance current best practices in architecture to:

- Embed safety concepts into architecture concepts, as opposed to capture safety solely as an architectural view.
- Develop meaningful metrics for the evaluation of architecture against safety goals, which will feed into the overall architecture trade-offs.
- Generate (digital) architectural artefacts that contribute to the construction of the safety case.

It is envisaged that the outcomes developed in this joint working group will be beneficial to both the systems engineering community and the system safety community.

WG Operation

The WG will meet every 6 weeks online via Teams. Note that the INCOSE UK AWG meets every quarter.

If you would like to be involved in the group, please contact the co-chairs.

Cochairs: **Siyuan Ji** s.ji@lboro.ac.uk and Jane Fenn jane.fenn@baesystems.com

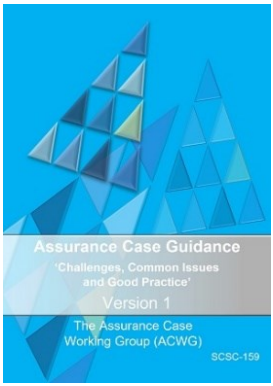
SCSC Working Groups

The Safety-Critical Systems Club is committed to supporting the activities of working groups for areas of special interest to club members. The purpose of these groups is to share industry best practice, establish suitable work and research programmes, develop industry guidance documents and influence the development of standards.

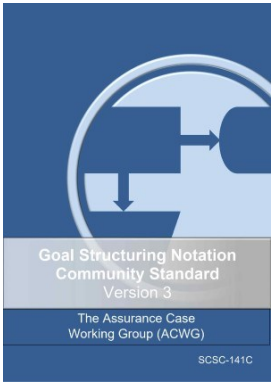
Assurance Cases

The Assurance Cases Working Group (ACWG) has been established to provide guidance on all aspects of assurance cases including construction, review and maintenance. The ACWG will:

- Be broader than safety, and will address interaction and conflict between related topics
- Address aspects such as proportionality, rationale behind the guidance, focus on risk, confidence and conformance
- Consider the role of the counter-argument and evidence and the treatment of potential bias in arguments



In Aug 2021, the group published v1.0 of the Assurance Case Guidance: scsc.uk/scsc-159



One of the working group's activities is the maintenance of the Goal Structuring Notation (GSN) Community standard.

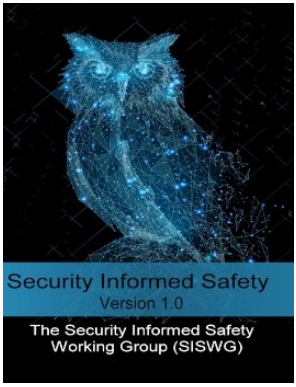
See scsc.uk/gsn for further details.

In May 2021, the group published v3.0 of the standard: scsc.uk/scsc-141C

Lead Phil Williams phil.williams@scsc.uk

SCSC Working Groups

Security Informed Safety



The Security Informed Safety Working Group (SISWG) aims to capture cross-domain best practice to help engineers find the 'wood through the trees' with all the different security standards, their implication and integration with safety design principles to aid the design and protection of secure safety-critical systems and systems with a safety implication.

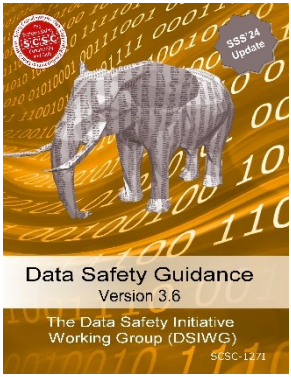
The working group aims to produce clear and current guidance on methods to design and protect safety-related and safety-critical systems in a way that reflects prevailing and emerging best practice.

The guidance will allow safety, security and other stakeholders to navigate the different security standards, understand their applicability and their integration with safety principles, and ultimately aid the design and protection of secure safety-related and safety-critical systems.

Lead **Stephen Bull** stephen.bull@scsc.uk

Data Safety Initiative

Data in safety-related systems is not sufficiently addressed in current safety management practices and standards.



It is acknowledged that data has been a contributing factor in several incidents and accidents to date and there is foreseeable harm that can arise from Machine Learning and Large Language Models' use of data by Artificial Intelligence (AI) systems that are subject to issues of biasing, interpretation and, arguably, falsification. There are clear business and societal benefits, in terms of reduced harm, reduced commercial liabilities and improved business efficiencies, in investigating and addressing outstanding challenges related to safety of data.

The Data Safety Initiative Working Group (DSIWG) aims to have clear guidance on how data (as distinct from the software and hardware) should be managed in a safety-related context, which will reflect emerging best practice.

An update to the guidance (v3.6) was published in Jan 2024: scsc.uk/scsc-127I

Lead **Mike Parsons** mike.parsons@scsc.uk

SCSC Working Groups

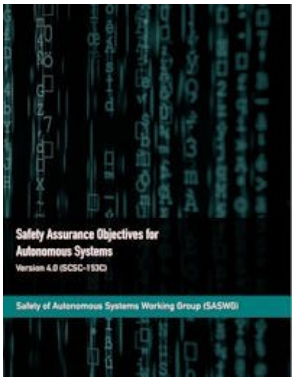
Safe AI

The SCSC Safe AI Working Group (SAIWG) aims to capture cross-domain best practice and guidance on key topics within the design, evaluation, assurance, and approval of safety systems that use or are developed using AI, bringing together emerging standards and key results from the incredible amount of research being conducted into AI safety.

The working group was kicked-off at SSS'24 and is led by Alan Simpson. The SAIWG will conduct regular meetings, workshops, and publications to share knowledge and experience on various topics related to AI and safety systems, such as coordination of safety with other disciplines, evaluation of risk, and mapping of terminology and language.

Lead **Alan Simpson** alan.simpson@ebeni.com

Safety of Autonomous Systems



The specific safety challenges of autonomous systems and the technologies that enable autonomy are not adequately addressed by current safety management practices and standards.

It is clear that autonomous systems can introduce many new paths to accidents, and that autonomous system technologies may not be practical to analyse adequately using accepted current practice. Whilst there are differences in detail, and standards, between domains many of the underlying challenges appear similar and it is likely that common approaches to core problems will prove possible.

The Safety of Autonomous Systems Working Group (SASWG) aims to produce clear guidance on how autonomous systems and autonomy technologies should be managed in a safety-related context, in a way that reflects emerging best practice.

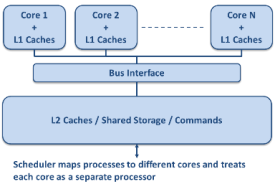
The group will work closely with the new Safe AI Working Group (SAIWG) as AI is used extensively in Autonomous Systems.

The group published v4 of its guidance Safety Assurance Objectives for Autonomous Systems, in Feb 2024 scsc.uk/scsc-153C

Lead **Philippa Ryan** pmrc@adelard.com

SCSC Working Groups

Multi- and Manycore Safety



It is becoming harder and harder to source single-core devices and there is a growing need for increased processing capability with a smaller physical footprint in all applications. Devices with multiple cores can perform many processes at once, meaning it is difficult to establish (with sufficient evidence) whether or not these processes can be relied upon for safety-related purposes.

Parallel processes need to access the same shared resources, including memory, cache and external interfaces, so they may contend for the same resources. Resource contention is a source of interference which can prevent or disrupt completion of the processes, meaning it is difficult to know with a defined uncertainty the maximum time each process will take to complete (Worst Case Execution Time, WCET) or whether the data stored in shared memory has been altered by other processes.

The Multi- and Manycore Safety Working Group (MCWG) has been established to explore the future ways of assuring the safety of multi- and manycore implementations.

Lead **Lee Jacques** Lee.Jacques@leonardocompany.com

Safer Complex Systems

The Safer Complex Systems Working Group (SCSWG) builds on the IET/RAE work already done in this area. It is recognised that the RAE work is ongoing and collaboration is encouraged. The group's mission is to produce practical guidance on developing, managing and assuring complex systems throughout their lifecycle (so as to achieve and justify their safety).

The following provides a statement of the problem:

- It is acknowledged that complex systems are becoming more prevalent with more opportunities to cause harm
- There are also new complex systems arising from using combinations of existing systems and services which are then used for safety purposes
- Complex systems are not sufficiently addressed in current safety management practices and standards
- In particular, complex interactions and emergent behaviours are not currently assessed and managed sufficiently
- There could be benefit in developing new analysis, tools and techniques to manage complex system risks
- There are clear business and societal benefits, in terms of reduced harm, reduced liabilities and improved business efficiencies, in improved management of complex systems risk

The group is aiming to produce draft guidance for SSS'25.

Contact the group lead if you would like to attend future meetings or find out more.

Acting Lead **Mike Parsons** mike.parsons@scsc.uk

SCSC Working Groups

Service Assurance

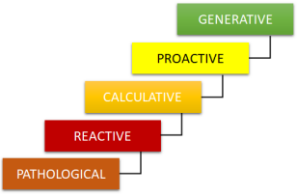


Risks presented by safety-related services are rarely explicitly recognised or addressed in current safety management practices, guidelines and standards. It is likely that service (as distinct from system) failures have led to safety incidents and accidents, but this has not always been recognised. The Service Assurance Working Group (SAWG) has been set up to produce clear and practical guidance on how services should be managed in a safety-related context, to reflect emerging best practice.

The group published guidance v4.0 in Jan 2024: scsc.uk/scsc-156D

Lead **Kevin King** kevin.king@baesystems.com

SCSC Safety Culture



The Safety Culture Working Group (SCWG) has been established to provide guidance on creating and maintaining an effective safety culture. The group seeks to improve safety culture in safety-critical organisations focussed on product and functional safety, by sharing examples and latest approaches collated from real-life case studies.

Meetings provide an opportunity to discuss any particular aspects attendees are interested in taking forward, and to help set future directions for the group.

In Dec 2023, the group published a position paper for assessing and managing safety culture. https://scsc.uk/r189:1

Lead **Michael Wright** michael.wright@greenstreet.co.uk

Systems Approach to Safety of the Environment



The Systems Approach to Safety of the Environment Working Group (SASEWG) is a new group intending to apply Systems Safety practices to systems that are embedded within the natural environment, while focussing on that environment.

The group aims to produce clear guidance on how engineered systems should be developed and managed throughout their entire lifecycle so as to preserve, protect and enhance the environment.

Please get in touch with the working group lead if you would like to join or find out more about this group.

Lead **James Inge** james.inge@scsc.uk

SCSC Membership

The SCSC provides a range of services to the System Safety community including seminars, tutorials, leadership events, specialist topic working groups, the annual symposium and a comprehensive body of publications. Membership brings many valuable benefits such as free access to online events, the SCSC Newsletter and access to presentations and other resources from events.

Individual Membership

To become an individual member of the SCSC please register on the SCSC website using the icon at the top right of any page and select "Register". Complete and save your account registration and then verify your email address. Once registered and logged in click the link "why not join the SCSC..." inviting you to become a member at the top right of the page or select "Pay membership" from the icon.

Individual membership can be paid online using a credit/debit card through our secure payment partner Realex Global Payments or contact Alex King for other payment methods. For student or retired member rates please contact Alex King to get your account status changed.

Corporate Membership

Your company contact with the SCSC should arrange the membership and any renewals for your organisation. To join as a member covered by a corporate membership, register as per the instructions for an individual member and then contact Alex King to confirm your affiliation.

Renewing Membership

You should be notified by email when your membership is almost expired or shortly after it has expired. These notifications will contain a link to the online renewal page or you will be able to renew when logging onto the website through the 'click to renew' link.

Membership Fees

The following fees are applicable from January 2025 for new and renewing members:

- 1 year Individual Membership: £149
- 2 year Membership: 8% discount: £275
- 3 year Membership: 16% discount: £375
- 1 year SFI Membership: FREE for first year, £35 for years 2 & 3
- 1 year Membership, retired member rate: £35
- For Corporate Membership discounts contact Alex King

A one-month Publication Pass is also available for £15. This allows access to all SCSC website publications in a particular calendar month.

Contact Alex King using office@scsc.uk

The SCSC Steering Group


Tom Anderson
Honorary member


Stephen Bull
stephen.bull@scsc.uk


Dewi Daniels
dewi.daniels@scsc.uk


Jane Fenn
jane.fenn@scsc.uk


Louise Harney
louise.harney@scsc.uk


Brian Jepson
brian.jepson@scsc.uk


Tim Kelly
Honorary member


Alex King
alex.king@scsc.uk


Yvonne Oakshott
yvonne.oakshott@scsc.uk


Mike Parsons
mike.parsons@scsc.uk


Felix Redmill
Honorary member


John Spriggs
john.spriggs@scsc.uk


Phil Williams
Honorary member


Robin Bloomfield
Honorary member


Carmen Carlan
carmen.carlan@scsc.uk


Dai Davis
Honorary member


Paul Hampton
paul.hampton@scsc.uk


James Inge
james.inge@scsc.uk


Graham Jolliffe
Honorary member


Khadijah Khatun
khadijah.khatun@scsc.uk


Mark Nicholson
mark.nicholson@scsc.uk


Wendy Owen
wendy.owen@scsc.uk


Davy Pissoort
davy.pissoort@scsc.uk


Roger Rivett
roger.rivett@scsc.uk


Sean White
sean.white@scsc.uk

Club Positions

The current and previous (marked in italics) holders of club positions are as follows:

Managing Director

Mike Parsons 2019-

Tim Kelly 2016-2019
Tom Anderson 1991-2016

Programme & Events Coordinator

Mike Parsons 2014-

Chris Dale 2008-2014
Felix Redmill 1991-2008

Newsletter Editor

Paul Hampton 2019-

Katrina Attwood 2016-2019
Felix Redmill 1991-2016

eJournal Editor

John Spriggs 2021-

Diversity, Equity and Inclusion (DE&I) Lead

Wendy Owen 2023-

Steering Group Chair

Roger Rivett 2019-

Graham Jolliffe 2014-2019
Brian Jepson 2007-2014
Bob Malcolm 1991-2007

Manager

Alex King 2019-

Honorary Solicitor

Dai Davis 2022-

University of York Coordinator

Mark Nicholson 2019-

Website Editor

Brian Jepson 2004-

Administrator

Alex King 2016-

Joan Atkinson 1991-2016

Safety Futures Initiative Leads

Khadijah Khatun 2024-
Zoe Garstang 2019-2024
Nikita Johnson 2019-2021, 2023-2024

Calendar

October '24

M	T	W	T	F	S	S
	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30	31			

November '24

M	T	W	T	F	S	S
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	

December '24

M	T	W	T	F	S	S
						1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29

January '25

M	T	W	T	F	S	S
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30	31		

February '25

M	T	W	T	F	S	S
					1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28		

March '25

M	T	W	T	F	S	S
					1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30

April '25

M	T	W	T	F	S	S
	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30				

May '25

M	T	W	T	F	S	S
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30	31	

June '25

M	T	W	T	F	S	S
						1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30						

July '25

M	T	W	T	F	S	S
	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30	31			

August '25

M	T	W	T	F	S	S
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31

September '25

M	T	W	T	F	S	S
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30					

Events Diary



16 Oct 2024
SCSC Working Group Meeting
Zoom 3.30pm-5pm

SCSWG#13: SCSC Safer Complex Systems Working Group meeting #13
scsc.uk/e1151

22 Oct 2024
SCSC Working Group Meeting
Teams 3pm-5pm

OWG#89: Ontology Working Group meeting #89
scsc.uk/go

22 Oct 2024
Conference
Newport, UK

HISC 2024: High Integrity Software Conference
www.his-conference.co.uk

24 Oct 2024
SCSC Working Group Meeting
Bath, UK and Zoom

DSIWG#86 SCSC Data Safety Initiative Working Group Meeting #86
scsc.uk/e1150

28-31 Oct 2024
Symposium
Tsukuba, Japan

ISSRE 2024: 35th IEEE Int. Symp. on Software Reliability Engineering
issre.github.io/2024

13-15 Nov 2024
Symposium
Osaka, Japan

PRDC 2024: 29th IEEE Pacific Rim Int. Symp. on Dependable Computing
prdc.dependability.org/PRDC2024/

20-22 Nov 2024
Conference
Catania, Sicily, Italy

ICSRS 2024: System Reliability and Safety
www.icsrs.org

28 November 2024
SCSC Seminar
Munich, Germany

Safe Autonomous Vehicles - the Good, the Bad and the Ugly
scsc.uk/e1134

26-29 Nov 2024
Symposium
Recife, Brazil

LADC 2024: Dependable and Secure Computing
ladc.sbc.org.br/2024

5-6 Dec 2024
Conference
Pisa, Italy

EAI SCS 2024: -Critical Software and Systems
scs-conference.eai-conferences.org/2024

4-6 Feb 2025
SCSC Symposium
York, UK

Safety Critical Systems Symposium SSS'25
scsc.uk/e1099

The SCSC has supported the system safety community since 1991

This year's symposium has three main themes of AI, Complexity and Security in a systems context: all of these are hard to assure and can have large and unexpected consequences of failures

System safety must evolve to make best use of AI, both in development of systems and assurance of them. Ways to analyse AI and autonomous systems for safety aspects need to be established

Systems are getting ever more complex, inter-connected and inter-dependent. As the CrowdStrike outage illustrated, they are also less robust. New tools and techniques are needed to analyse and manage such systems to identify unintended fragility

The SCSC **Safer Complex Systems Working Group** has produced initial guidance in developing and managing complex systems - available now

Other SCSC WGs have also been covering the area including the **Security Informed Safety Working Group (SISWG)** and the the new **Safe System Architecting Working Group (SSAWG)**

Safety Critical Systems Club - Supporting Development of Safer Systems
The Systems Safety SCSC Community and Club

The Safety-Critical Systems Club

invites all delegates to its 33rd Annual Symposium

This is the programme for the 33rd Safety Critical Systems Symposium (SSS'25) held February 2025 at the Principal Hotel York, UK

The Symposium is for all safety practitioners: both early career and experienced delegates are welcome

Six keynote talks from distinguished experts

Themes are: New Safety Scope, Security with Safety, Addressing Complexity, New Methods and Techniques, Assuring Autonomy, Safety Cases

Six technical workshops are included in a parallel afternoon stream

Poster sessions

Double ticket for early-career delegates

A great opportunity to learn and develop new connections and build networks

Tools and Suppliers Exhibition

Working Group meet-up

SSS'25 extends across 3 ½ days of presentations, grouped into key themes

After-dinner speech

Armchair chats with experts in the world of system safety

Working group updates provided by posters

Guided visit to the York Institute of Safe Autonomy

Full proceedings volume

Mix with experts and learn new ideas that can help with career progression

Technical entertainment

Symposium Banquet

York social activities available

Interactive sessions


SCSC
FOR EVERYONE WORKING IN SYSTEM SAFETY
thescsc.org/membership
SSS'25
33rd Safety-Critical Systems Symposium
4 - 6 February 2025
Principal Hotel, York, UK
www.scsc.uk/sss