The Safety-Critical Systems Club Newsletter

Safety Systems

Vol 34 No. 2 – May 2026

X-RAY VISION
Managing risks from cosmic rays

OBJECT LESSONS
Embracing the Ethics of Personhood

BOXING CLEVER
The Scutoid story unfolds!

YORK TRIUMPH!
Highlights from SSS'26

AI IN THE LOOP
Human Factors in the AI age

SCSC

thescsc.org

SCSC Publication Number: SCSC-212

Front cover: AI generated image
Editorial: NASA astronaut Christina Koch, Artemis II mission specialist, peers out of one of the Orion spacecraft's main cabin windows on Saturday, April 4, 2026, looking back at Earth, as the crew travel toward the Moon. NASA
In Brief images may be subject to copyright – contact the SCSC Newsletter Editor for details.

Contents

Invitation to submit an abstract

35th Safety-Critical Systems Symposium (SSS'27)

February 9-11th 2027, Bristol, UK

Suggested topics are:

www.scsc.uk/sss

Accident Analysis
Agile Methods
AI: LLM's & Generative AI
AI Training Data
Autonomy
Airworthiness
Analyses
Assurance Cases
Architectures
Autonomous Vehicles
CAV
Certification
Complex Systems
Data Safety
EMC/EMI
Embodied AI
Environmental Safety
Human Factors
Machine Learning
Methods and Tools
Model-Based Techniques
Multicore / Manycore
Ontologies / Formalisms
Prompt Engineering
Quantum
Regulation
Resilience
Robotics
Security
Safety Culture
Safety Management Systems
Safety Practice
Services Safety
Software
Standards and Guidance
Through-Life Safety
Tool Qualification
Training Data
UAS
Uncertainty and Risk
Validation and Verification

Authors submit a title and 200-word abstract to: **mike.parsons@scsc.uk**	**by 30th June 2026**
Authors notified if their abstract has been accepted	**by 31st July 2026**
Authors submit their paper for inclusion in the proceedings book	**by 16th Oct 2026**
Review comments fed back to authors	**by 13th Nov 2026**
Final versions of papers submitted	**by 31st Nov 2026**

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

If you would like to give a tutorial, run a workshop or present a poster at SSS'27, please contact mike.parsons@scsc.uk

Editorial

Christina Koch's view of Earth from the Orion spacecraft

With Artemis II, for the first time in over 50 years, we witnessed a crewed space vehicle fly around the Moon and return its occupants safely to Earth. The 10-day mission paves the way to further missions with the ultimate aim to land on the Moon, possibly as early as 2028, key steps along the road to establishing a long-term human presence on the lunar surface.

The mission was of course hugely successful not least measured by the safe return of the astronauts, but it might be better described as "Almost Perfect". The mission did not go without some worries; some practical: a blocked toilet and a more worrying cabin leak alert, which proved to be a problem with the sensor.

The endeavour nevertheless still remains a highly risky one. From reports, NASA consider the "loss of crew threshold" to be 1 in 30 and aimed to get below 1 in 50 for Artemis; that's still a 2% chance of catastrophic failure for the mission; perhaps akin to picking the Bonus Ball in the National Lottery. I certainly salute those involved in the programme and especially the astronauts.

It shouldn't need to be said of course, but the diversity of the crew was also notable and arguably a key component of the mission design. These were not just tourists on the ultimate fairground roller-coaster ride, but ambassadors, not just for this particular mission but the whole programme of humans returning to space. A permanent base on the Moon and onward thoughts to Mars are multi-generational aspirations and so it is just as important to win the hearts of the younger generations who will be those astronauts of the future. This is borne out in the many quotes that have appeared from the crew and I was particularly taken by Victor Glover's quote:

> "*People need to be able to see themselves in the things that they dream about".*

This resonated as it is applicable not just to spaceflight but our industries as well. The more diversity we see in the workplace, the more accessible careers will appear, and hence, become to all – and aren't we a much better team overall when we bring everyone to the game?

In February this year we had a fantastic Symposium with one of the highest attendances ever. There was a huge number of great talks especially on the second day when we split into three separate streams (four if you count the social events!). I provide a full report of the event in this edition with Mitali and Divya Atkins providing insights into the design of the "Scutoid" treat box distributed to delegates. Our feature article is from Dewi Daniels talking about the upsets cosmic rays may have on aircraft and how airline manufacturers protect (or in some cases don't) from their effects. I have great pleasure in introducing Nippin Anand who covers aspects of his book 'Are We Learning from Accidents?', which I reviewed in the Feb'26 newsletter. Dorthea Mathilde Kristin Vatn and Thor Myklebust provide insights into how Human Factor frameworks need to be modified in the age of AI.

Our 60 second interview is with Mikela Chatzimichailidou, Professor at University College London.

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


SCSC
Working For The Safe Use Of Systems
Safety-Critical Systems Club (SCSC)
Corporate Membership
Membership for your organisation
Support your safety culture
Network with senior managers
Share knowledge and experience
Develop your staff
Learn about current standards
Understand best practices
Influence new guidance
Raise your organisation's profile
To take advantage of the corporate membership rates, contact office@scsc.uk
www.thescsc.org
www.scsc.uk

SCSC

For Everyone Working in System Safety

How to Make the Most of AI: A Workshop for Safety Engineers

Includes prompt engineering techniques

Work with LLM AI tools to get the most benefit

Includes workshops to experiment with different approaches

Speakers include:

Ben Fulford, BMT

Rudi (Redford-Brown) Hennessy, NHS England

Alan Simpson, Ebeni

25th June 2026

Hilton London Euston hotel, London, UK

Safety-Critical Systems Club (SCSC)

Safety-Critical Systems Club (SCSC)

www.thescsc.org

www.scsc.uk

In Brief






Thousands at risk after Everest flood warning system left to rust

An early flood warning system designed to save the lives of thousands of people in the Everest region may no longer be working, Nepalese officials have admitted after it was allowed to fall into a state of disrepair.

The disclosure came after villagers in the local Sherpa communities said no inspection of the UN-supported project had been carried out for many years after the dangerous Imja glacial lake was last drained in 2016. *bbc.co.uk*

Should you really trust health advice from an AI chatbot?

Could your next diagnosis come from AI? A recent BBC report explores the booming trend of patients using AI chatbots for medical advice. With GP appointments harder to secure, many are turning to ChatGPT and similar tools for instant health answers; but is it safe?

AI's use seems appealing: it offers 24/7 access; it can simplify complex medical jargon, deal with minor queries and explain lab results. However, experts warn that AI lacks a "ground truth". It can confidently invent medical facts or suggest incorrect dosages – a phenomenon known as hallucination. *bbc.co.uk*

Artemis II crew 'happy and healthy' after completing historic mission to the Moon

The 10th April 2026 marks a historic milestone in human space exploration with the safe return of the astronauts, splashing down in the Pacific Ocean. The four-person crew were recovered safely and reported to be in good health.

Artemis II is significant for being the first crewed mission to travel beyond the Moon in over 50 years, since the Apollo era. NASA officials hailed the mission as a major success, confirming that the spacecraft handled the high-speed re-entry into Earth's atmosphere as expected. *bbc.co.uk*

Mass robotaxi malfunction halts traffic in Chinese city

A mass robotaxi outage in the Chinese city of Wuhan caused at least a hundred self-driving cars to stop mid-traffic, sparking renewed debate around the safety of driverless vehicles.

Local police said initial findings suggested a "system malfunction" caused multiple vehicles to stop in the middle of the road. *bbc.co.uk*

In Brief






AI firm Anthropic seeks weapons expert to stop users from 'misuse'

The US Artificial Intelligence firm Anthropic is looking to hire chemical weapons and high-yield explosives experts to try to prevent "catastrophic misuse" of its software. The company fears that its AI tools might tell someone how to make chemical or radioactive weapons, and wants an expert to ensure its guardrails are sufficiently robust.

But some experts are alarmed by the risks of this approach, warning that it gives AI tools information about weapons – even if they have been instructed not to use it. *bbc.co.uk*

Autonomous cars, drones cheerfully obey prompt injection by road sign

A new class of cybersecurity vulnerability has emerged, known as environmental indirect prompt injection, where physical road signs are used to hijack the decision-making processes of autonomous vehicles and drones.

Researchers from the University of California, Santa Cruz developed a method of attack that exploits Large Vision-Language Models that power "embodied" AI. Unlike traditional prompt injection, which occurs via text files or web pages, it uses visual cues in the environment. *theregister.com*

Officer reportedly leaks location of French aircraft carrier with Strava run

The French Ministry of the Armed Forces recently took "appropriate measures" after a naval officer inadvertently exposed the location of the nuclear-powered aircraft carrier Charles de Gaulle via the fitness-tracking app Strava.

The breach occurred while the officer was jogging on the carrier's deck with a GPS-enabled device. Strava's "Global Heatmap" feature, which aggregates user data to show popular exercise routes, displayed a distinct pattern of activity in the Mediterranean Sea. *bbc.co.uk*

100-Ton Weight Miscalculation By Pilots Caused LATAM Boeing 777 Accident In Milan

In July 2024, a LATAM Airlines Boeing 777-300ER scheduled for a flight from Milan to São Paulo suffered a severe tail strike during takeoff, an event recently reclassified as an accident by Italian investigators (ANSV). The root cause was a 100-ton weight miscalculation made by the crew during pre-flight performance planning.

The error originated when the line-training captain mistakenly subtracted the expected taxi fuel from the aircraft's zero-fuel weight. simpleflying.com

T-Time with the Editor!

I recently came across a 2020 Netflix series called "Zoe's Extraordinary Playlist", which you might call a jukebox musical comedy-drama, refreshingly featuring several women in senior IT positions and it also actually tackled serious issues of cultural discrimination in the work-place. One of the protagonists had an Ada Lovelace T-shirt with Ada's image and the text "Code like a girl". As my de-facto working uniform now, I am always on the lookout for new T-shirts, anything from the profound to the comical! My favourite ones that have appeared to me recently on social media are an animal, usually a cat but sometimes a racoon or even a penguin staring at its reflection in the mirror and saying:

"I do not think, therefore I do not am".

An amusing spin on Descartes' philosophy! I thought it would be fun to explore spinning another well-known quotation, perhaps even one from a female pioneer of engineering or indeed someone relevant to our safety domains. Ada has a good source of quotes but they tend to be long and not easily convertible into something short and punchy for a T-shirt. I then came across a quote from Marie Curie, the renown pioneering physicist and chemist, who stated around 1933.

"Now is the time to understand more, so that we may fear less".

I said I liked the comical, but I also like the profound and it struck me how acutely relevant this is today in our wild frontier of emerging AI technologies; opinions range from, "this is just a fad, it's just another knowledge system" to "AI will take over the world and enslave or exterminate all humans!". Only through considered and reasoned understanding will we truly know what is, or not, to be feared. I did actually cut Marie's quote short slightly, the first part said:

"Nothing in life is to be feared, it is only to be understood".

I might humbly suggest that this might need a new spin or modernisation and I'd propose:

"Life is to be feared if it is only understood".

Sorry, not the comical spin I originally set out to achieve but I think there's an important message here. There seems to be a relentless and unbridled pursuit to increasingly complex and sophisticated AI systems; we've seen humanoid robots on the battlefield, Claude Mythos potentially popping the lid on financial systems globally and the possibility of AI being used to design biological weapons. Possibly all hype I know, but the point is that understanding cannot exist in isolation; it needs to operate and evolve to inhabit our ethical and moral boundaries. We have only landed at the shore of this new AI frontier; the challenges ahead, like our space ambitions will be multi-generational and we also need to win the hearts and minds of the younger generations who will find themselves in the future wilderness.

I therefore leave you with this T-shirt. Let me know if you like the idea or even would like to pre-order this one. The SCSC is considering developing SCSC-related merchandise and so a range of safety-inspired T-shirts across a number of themes is one possibility. We would of course welcome your thoughts and inspirations!

Paul Hampton (SCSC Newsletter Editor)

Are software upsets really a cosmic mystery?

Last year, an Airbus A320 experienced an in-flight upset. It is suspected that a recent software update made the aircraft susceptible to disruption caused by cosmic radiation. Dewi Daniels investigates the issue, describing the software/hardware interactions and explores what regulations and standards exist to help mitigate these types of event.

On the 30th October 2025, a JetBlue Airways Airbus A320 experienced an in-flight upset while cruising at 35,000 feet [1]. Four flight attendants and 18 passengers sustained minor injuries.

The incident was notified to the National Transportation Safety Board (NTSB), who opened a formal investigation. The NTSB investigation is still ongoing [2].

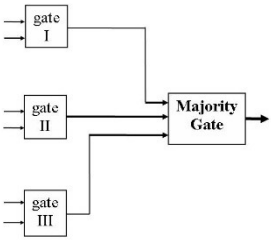
Airbus determined that a recent software release to the Elevator Aileron Computer (ELAC) was susceptible to Single Event Upsets (SEUs). An SEU occurs when a single, high-energy particle (like a cosmic ray or neutron) flips a bit of data (changing a 0 to a 1 or vice-versa) in a memory cell or a Central Processing Unit (CPU) register. The ELAC had been developed by Thales [2, 3].

Airbus issued an Alert Operators Transmission (AOT) A27N022-25 [3] on the 28th November 2025 requiring that all Airbus A319, A320 and A321 aircraft fitted with ELAC B standard L104 be reverted to ELAC B standard L103+.

The European Union Aviation Safety Agency (EASA) issued Emergency Airworthiness Directive (AD) No. 2025-0268-E [4] and the Federal Aviation Administration (FAA) issued Emergency AD 2025-24-51 [5] on the same day.

It may seem surprising that a software update would make an aircraft susceptible to SEUs. After all, an SEU is a hardware event. It's true that SEUs can be mitigated through hardware design – space satellites often use radiation-hardened microprocessors and memory devices. However, these are not used in airliners (and not even in some satellites) because radiation-hardened devices are bigger, heavier, slower and more power-hungry. Airliners do typically use Error-Correcting Code (ECC) memory, which helps to mitigate against SEUs, though ECC memory does not mitigate against SEUs that occur in the microprocessor itself, such as in cache memory and in registers.

The main mitigation against SEUs in avionic systems is using redundancy in system design. For example, consider triple modular redundancy (TMR). This is where three channels perform the same calculation and a voter is used to decide on a single output. An SEU will only affect one of the channels. The other two channels will produce the same, correct output and will therefore outvote the channel that suffered the SEU.



As an additional layer of defence, SEUs can be mitigated by software design. For example, I was one of the software developers on the Airbus A380 Landing Gear Extraction and Retraction System (LGERS) in the early 2000s [6]. While the main mitigation against SEUs was the fact that LGERS is a multiple redundant system, EASA also required that we mitigated against SEUs in our software design. We conducted a software hazard analysis to identify the critical data and we kept three copies of all critical data (one of the copies was the one's complement of the other two). This meant that we were able to detect when an SEU had corrupted one of the copies and restore the correct value from one of the other two copies. We recorded the number of data corruptions in non-volatile random-access memory (NVRAM). It would be interesting to know how often SEUs have occurred in practice – I suspect that SEUs occur quite often, especially at cruising altitude.

"I suspect that Single Event Upsets occur quite often, especially at cruising altitude"

EASA Certification Memorandum CM–AS-004 [7] provides guidance on how to consider the effects of Single Event Effects (SEEs) on aircraft systems and equipment. EASA has also published a Safety Information Bulletin (SIB) 2012-10R1 on SEEs [8]. Meanwhile, the FAA published Single Event Effect Mitigation Techniques Report DOT/FAA/TC-15/62 [9]. An SEE is the umbrella term for any measured change or failure in an electronic device caused by a single, high-energy particle (like a cosmic ray or neutron) hitting a sensitive spot on a chip. SEEs can either be soft errors, which are temporary glitches or hard errors, which cause permanent damage to the chip. An SEU is a specific type of soft error that occurs when a particle flips a bit of data, as described above.

RTCA DO-248C [10]/EUROCAE ED-94C [11] Discussion Paper (DP) #21 provides an explanation as to how SEUs can be mitigated in software. It explains that the most common protection mechanisms against SEUs are error detection and correction mechanisms, such as:

- Parity
- Cyclic redundancy code
- Hamming code
- Reed-Solomon code
- Convolutional codes
- Watchdog timers
- Voting
- Minimising the use of unprotected cache memory
- Periodically flushing the cache
- Storing triple versions of critical values
- Minimizing the use of non-ECC random access memory (RAM) on the processor
- Minimising stack and heap usage
- Using stack and heap overrun protection
- Minimising the use of variables whose corruption could significantly impact the behaviour of the software
- Periodically performing checksums on critical areas of memory
- Performing checksums on permanently stored data
- Providing a mechanism where the application can be reset

DP #21 also explains there are additional practices that can be used where appropriate, including:

- Repeated calculations to overcome transient errors
- Define constants in read only memory (ROM)
- Do not rely on RAM data to be accurate
- Write output discretes to hardware latches every frame
- Avoid using equality
- Continuously check the configuration state of devices that have been initialised by software
- Filter input data
- Whenever a built-in test equipment (BITE) or built-on test (BIT) detects a failure, rerun the test a second time to confirm the failure
- When using bi-directional I/O ports, re-assert the configuration of the I/O port often
- Where registers are used to define the CPU configuration, the configuration should be re-asserted often
- Pointers should be range checked when used.

SEE and SEU have been known about for a long time and are the topic of guidance from FAA and EASA. It is surprising that this software update resulted in an in-flight upset so soon after it was released. It suggests that SEU are relatively common but also that most avionic system and software designs are robust in the presence of SEUs.

The NTSB investigation is still ongoing and no further information has been released by Airbus. We can therefore only guess at the cause of the in-flight upset.

I suspect that ELAC B standard L104 introduced new functionality that was not cross-checked by the other channel(s) and that there was insufficient software mitigation (e.g. they did not keep triple versions of critical data).

Fortunately, the problem was resolved by reverting to the previous standard L103+. I assume that the intent is to develop a new software standard that re-introduces the new functionality in a manner that is not susceptible to SEUs.

"It is surprising that this software update resulted in an in-flight upset so soon after it was released"

References

[1] https://aviation-safety.net/wikibase/560989, retrieved 10 March 2026.

[2] Aviation Investigation Preliminary Report, Incident Number ENG26LA004, National Transportation Safety Board, https://data.ntsb.gov/carol-repgen/api/Aviation/ReportMain/GenerateNewestReport/201942/pdf, retrieved 10 March 2026.

[3] Airbus Alert Operator Transmission (AOT) A27N022-25 Rev 01, 28 November 2025, https://downloads.regulations.gov/FAA-2025-5395-0002/attachment_1.pdf, retrieved 10 March 2026.

[4] EASA Emergency Airworthiness Directive No. 2025-0268-E, 28 November 2025, https://ad.easa.europa.eu/blob/EASA_AD_2025_0268_E.pdf/EAD_2025-0268-E_1, retrieved 10 March 2026.

[5] FAA Emergency Airworthiness Directive # 2025-24-51, 28 November 2025, https://drs.faa.gov/browse/excelExternalWindow/DRSDOCID1701465859202511290342430001?modalOpened=true, retrieved 10 March 2026.

[6] Safety Aspects of a Landing Gear System, Dewi Daniels, Fourteenth Safety-critical Systems Symposium, Bristol, UK · Feb 1, 2006.

[7] Single Event Effects (SEE) Caused by Atmospheric Radiation, Certification Memorandum No. CM-AS-004 Issue 01, European Union Aviation Safety Agency, 8 January 2018, https://www.easa.europa.eu/sites/default/files/dfu/CM-AS-004%20Issue%2001.pdf, retrieved 10 March 2026.

[8] Single Event Effects on Aircraft Systems caused by Atmospheric Radiation, Safety information Bulletin No. 2012-10R1, European Union Aviation Safety Agency, 29 April 2021, https://ad.easa.europa.eu/blob/EASA_SIB_2012_10_R1.pdf/SIB_2012-10R1_1. Retrieved 10 March 2026.

[9] Single Event Effect Mitigation Techniques Report, DOT/FAA/TC-15/62, Federal Aviation Administration, February 2016, https://www.faa.gov/sites/faa.gov/files/aircraft/air_cert/design_approvals/air_software/TC-15-62.pdf, retrieved 10 March 2026.

[10] Supporting Information for DO-178C and DO-278A, DO-248C, RTCA, Inc., 13 December, 2011

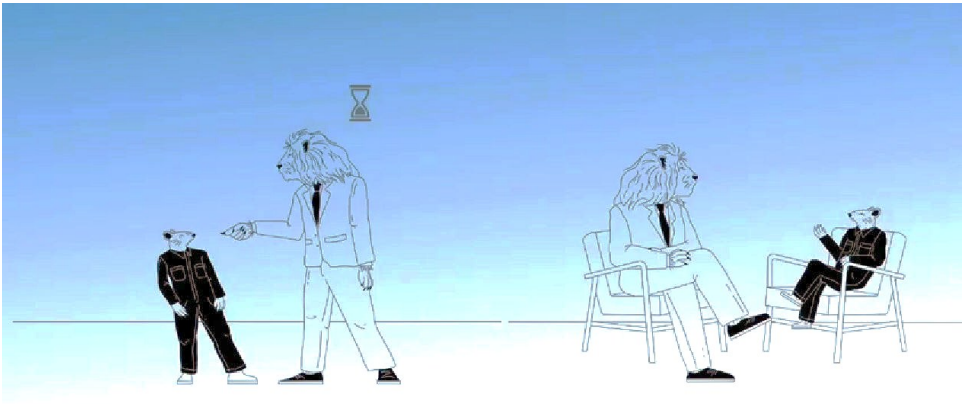
[11] Supporting Information for ED-12C and ED-109A, ED-94C, EUROCAE, January 2012

Image attribution:
top image: AI generated (Midjourney and Gemini)
Triple Modular Redundancy: IjonTichyIjonTichy, CC0, via Wikimedia Commons

Dewi Daniels, Software Safety Limited

Dewi is a Chartered Engineer with nearly 45 years' experience in the development and verification of safety-critical software. Dewi was one of the authors of DO-178C/ED-12C. He is currently a member of the RTCA/EUROCAE Forum on Aeronautical Software and one of the UK experts on the IEC 61508 committee.

From Power to Personhood



After experiencing a near-collision at sea, Dr Nippin Anand developed a lifelong passion for event investigation, focusing on how failure can be turned into opportunities for learning and change. Through his examination of the 2012 Costa Concordia accident, and his exclusive interview with the Captain who was vilified for the unfolding events, he asks if we are truly learning from accidents or whether scapegoating provides more comfort and certainty to society rather than learning. To promote better learning, should we not be taking a more transdisciplinary approach? Safety Sciences is inherently embedded in Material Ethics (i.e. Deontology, Behaviourism, Positivism and Empiricism), which reduces human beings to objects and hazards. In this article Nippin discusses the need to embrace the Ethics of Personhood.

Amongst the many theories that explain why we mock at others. I find the work of French Philosopher Henri Bergson's to be the most powerful of all.

We mock at others when we realise that we have reduced the spontaneous and organic nature of living and being into a mechanistic object. Bergson referred to this phenomenon as 'how the mechanistic encrusts upon the living.'

The picture opposite came from my own experience of working at sea nearly three decades ago. I see it as a beautiful example of the wisdom of Henri Bergson.

Humans are not objects to be measured or hazards to be controlled. Our being is fallible, mortal and whole. We must learn to relate with other human beings as whole persons if we want to learn from accidents. We can see people as "it", objects to measured, hazards to be controlled. When accidents are investigated the objectives are often "to extract data" or "to collect data" and there is a loss of being able to relate or connect to people (I -> it).

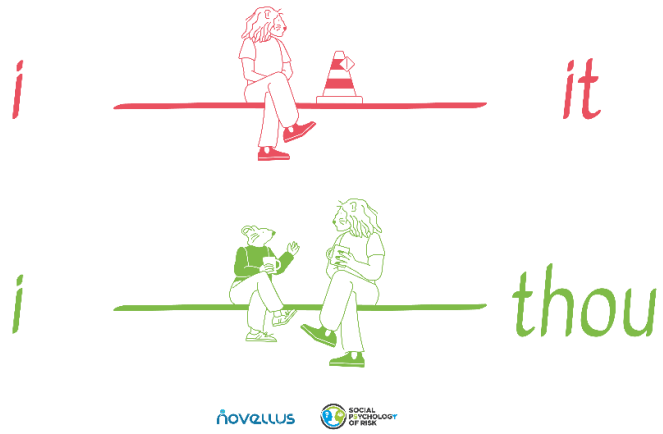


Image copyright to Novellus©

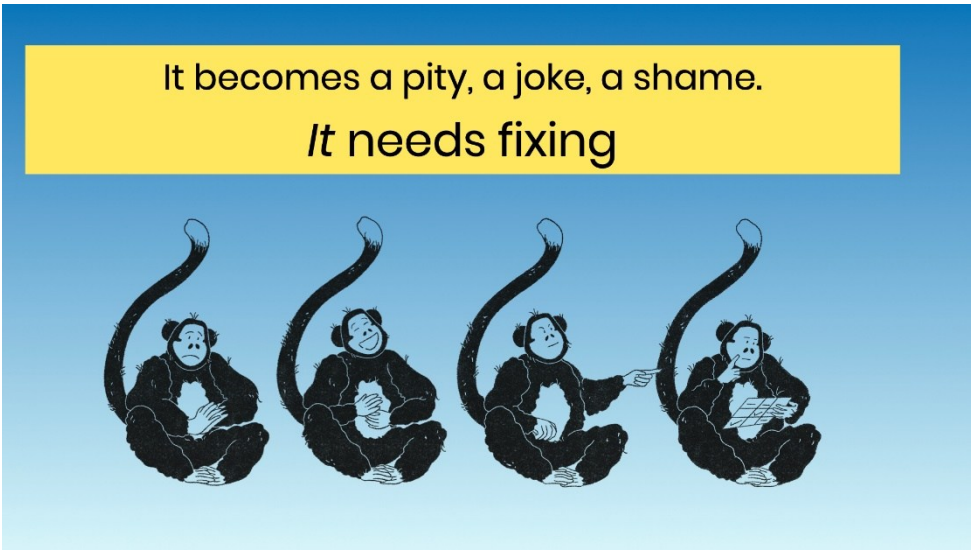
There is immense power in being able to look at people as a full person (I -> thou), to relate to them and being able to learn from them.

We can run away from our words but we cannot run away from our images. Notice the cover of the books in risk, safety and human factors. What do you notice?

Martin Buber was right. We treat everyone as an object to serve our agenda. We see everyone as *It*. It is so obvious that we don't even see *It*.

When *It* Goes Wrong

In January 2012, the passenger ship Costa Concordia ran aground off the coast of Italy. 32 people died in one of the worst accidents in passenger ship history. Coincidentally, the accident happened 100 years after the sinking of the Titanic.



Watching the Captain being vilified reminded me of Martin Buber: Human Factors and the culture of an entire industry in action. What happens when humans cannot be factored in the system? What happens when *It* does not serve the system?

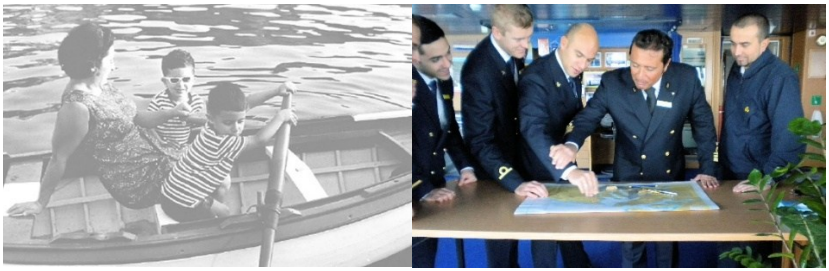
Seeing Beyond *It*

In March 2017, I contacted Francesco Schettino, the captain of the Costa Concordia. I requested a meeting with him to understand his perspective and what I could learn from him. Francesco agreed to meet me. At the time of our meeting, Francesco was under house arrest in his hometown Sorrento in Italy.

Those were his first few words when I met him in person. Imagine even after five years of the accident, no one from the industry ever spoke to him but every 'expert' had a view on the accident. More specifically, everyone had a view about 'Captain Coward' who ran away from the ship before all the passengers were evacuated.

What started as a casual conversation between us became an intense discussion. Francesco and I spent three days together and recorded more than 12 hours of video footage. He gave me many insights about what went wrong and how we can become better at managing passenger ship safety.

But I was more interested in understanding Francesco as a person. What did I learn about him?



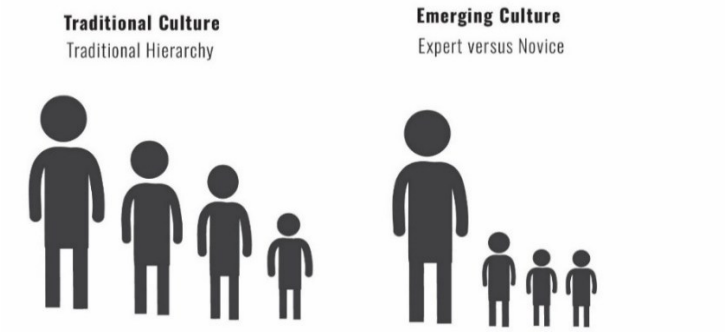
Francesco Schettino was born into a family of seafarers. His grandfather was a fisherman and his father was a marine engineer. His brother works as a first officer at sea. Fishing was his passion since he was a young boy. He had worked on tanker ships, ferries and gas turbines. He had been involved in building passenger vessels in shipyards in France; a staff captain for 6 years, a ship captain for 5 years and appointed as a safety representative for his company. Just this short biography should tell us he is not the 'Chicken of the Sea'.

Language of the Soul

I did not begin with investigating the accident. I started by relating with Francesco as a whole person. And in so doing, Francesco connected with me and gave the gift of his spirit. Galileo referred to this as the 'language of the soul'.

Throughout our three days of interactions, Francesco was highly critical of the quality of new recruits at sea. According to him, the junior officers lack the professionalism and the competence of a mariner.

The maritime industry has always been hierarchical but there is a new pattern of hierarchy we are noticing with there being an expert 'silo' surrounded by very junior novices. Despite there being five people on the bridge when the ship was heading towards rocks, none of them felt they could speak up and tell the Captain.



Why people don't speak up?

In one of our exchanges, the Captain revealed that when he asked his junior officers to put some salt tablets in the jacuzzi to turn the water saline, the officer added 'three salt tablets'. According to Francesco, someone who does not understand the basic principles of salinity and the Archimedes Principle of floatation and density does not deserve to be an officer at sea.

This story later became a turning point in my book, Are We Learning from Accidents [1], to dig deeper into systemic problems of training and competence in the maritime industry. The book, written after six years of contemplation and research into transdisciplinary areas, touches upon several aspects of risk and safety. I challenge the construct of 'soft skills'; 'non-technical skills' and 'psychological safety'. Deep and systemic issues of competence and expertise are often masked under a multi-million dollar industry that is inclined to reframe systemic problems as dearth of 'soft skills' or a 'lack of psychological safety'.

Several learnings surfaced during our deep discussions. Francesco, during his house arrest, was undertaking rigorous research to question everything from design, operations, company and regulatory standards of passenger ships. He was asking fundamental questions about fire safety, passenger evacuation, ship construction and stability. The systemic failures following the accident have led to many policy interventions in the maritime industry, but it has also given a new meaning to Francesco's quest for truth.

For a more detailed overview, here is the video link [2].

What is 'normal work'?

I also found how experts, on a daily basis, walk the difficult line between satisfying different competing and conflicting needs of the organisation, but it only takes a couple of hours to turn an expert into a criminal. The seemingly reckless close-pass of Giglio Island that led to the grounding is known as a "Salute" in the industry, and it is common practice to promote the image and commercial interests of the cruise industry.

Every day we are fed with meaningless jargon – 'learning from normal work'; 'learning from what goes well'; and 'learning from success'.

We should learn to slow down, pause and reflect on these constructs. Do we care to understand what is good, normal and successful from the perspective of the others?

Prior to the capsizing of Costa Concordia, sailing close to islands was considered a normal practice. How many risk and safety managers would be comfortable calling it 'normal work?' One person's normal is another person's catastrophe.

Such words have no meaning if we don't care to understand the subjective and hermeneutic nature of risk. Where do we discuss risk perception in risk and safety books, models, methods and methodologies? The industry lacks the ethics of personhood.

"Where do we discuss risk perception in risk and safety books, models, methods and methodologies? The industry lacks the ethics of personhood"

What is missing in emergency processes and contingency plans?

Emergency procedures are written in a very logical systematic and analytical way and fail to address the chaos and messiness that follows during an accident. Not only do these procedures belie an unrealistic fantasy of expected behaviours of pressurised and traumatised individuals but are actually used as the basis to criminalise participants.

Can there be a no-blame culture?

Francesco Schettino was also accused of leaving the ship before everyone was rescued. This is a baseless story that begs critical thinking and questioning. Several researchers and authors, including my own work, have questioned these allegations.

During evacuation, he was forced to jump once the ship started to list heavily towards one side. His presence of mind to land on a lifeboat that was stuck under the ship whilst instructing the coxswain to ease on the engine throttle to release the boat hook attached to the ship saved hundreds of people from being crushed under the boat. But this story never made it to the press. Instead, our quest for a scapegoat following an accident, led to the 'Captain Coward myth'. But such a myth is not uncommon when humankind seeks meaning in misfortune.

In Francesco's scapegoating lies the redemption of the cruise industry. Imagine what would happen if there was no one to scapegoat on that night?

Be careful when you hear the word, 'Blame fixes nothing'. Humans have not evolved to get rid of scapegoating. It is how we have always found meaning in accidents and disasters.

Long live scapegoating, who cares to learn from accidents?

The Ethics of Personhood

Once we turn people into 'objects' their state of mind, anxiety, distress and trauma hardly matters. What matters is extracting data, writing reports and releasing safety alerts. We call it 'lessons learned.'

It is no surprise that people involved in accidents often say this to me: going through the investigation was far worse than the actual experience of the accident. Many don't come out of their trauma for the way they were treated as part of the investigation process.

There is no humanistic ethics in investigation or for that matter in the safety industry; there need not be because that is not important. What is important is preventing harm. The end justifies the means.

In pursuit of Zero Harm human beings are brutalised and reduced to *It*.

The real question therefore is not the why, the what or the how? The question is: Who needs to learn from accidents?

That is where I spend a lot of time educating the investigators, auditors and safety inspectors. Unless we acknowledge the hidden dogma and indoctrination within the risk and safety industry there is no way we can learn from accidents.

Unless we learn to see another person as a whole person, there is no way we can learn from accidents.

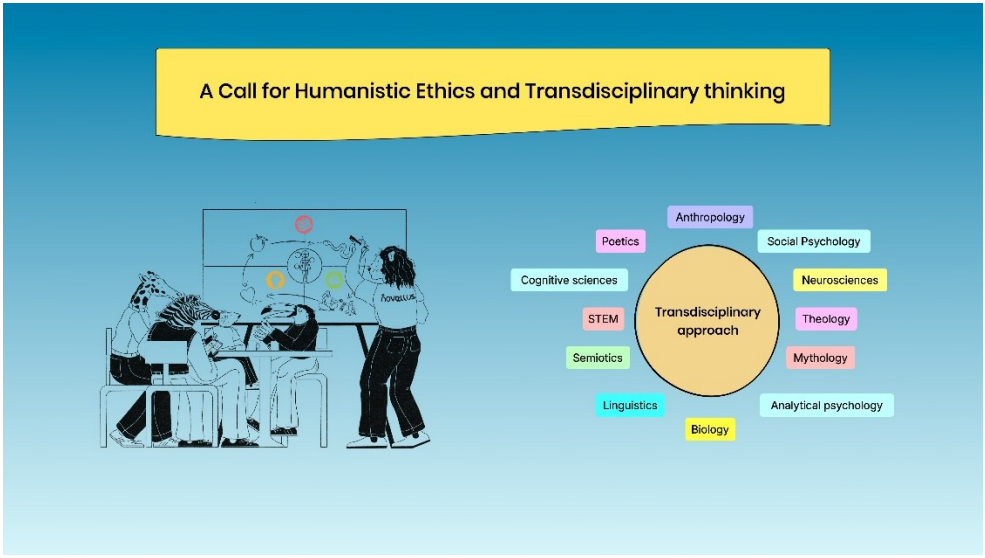
Embracing Fallibility

Several insights came out of our interactions, but more importantly, meeting with Captain Francesco Schettino has transformed me as a person. This is my most profound learning from accidents.

I don't look for perfection anymore; I am at ease with imperfection and fallibility. This inner journey has helped me to live a more fulfilling life. I see every day as a gift and every social interaction as a unique opportunity to learn about myself and others.

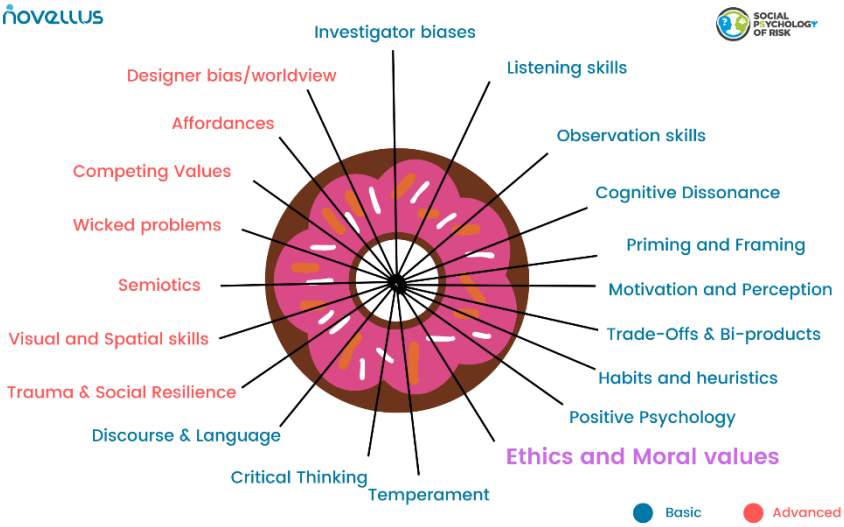
Transdisciplinary methods beyond STEM Sciences

Broader questions about human behaviour require broadening our understanding. These questions cannot be answered within the realms of Science, Technology, Engineering and Mathematics (STEM). We must learn to embrace other disciplines both academic and otherwise. That is where the future of learning needs to go.



For that we need to embrace the Ethics of Personhood and semiotic methods to learn from another human person.

At Novellus we encourage semiotic methods within Social Psychology of Risk (SPoR) – a Transdisciplinary body of knowledge developed by Dr Robert Long in Canberra, Australia. One such method for investigations is called the iCue engagement process. These methods bring in not only the rational and logical analysis of a human but also incorporates decision making from experience-based heuristics as well as automatic non-rational 'gut thinking' intuition. (You can view several examples of the iCue method by visiting this link [3].)



SEEK (SOCIAL EVENT EXPLORATION KNOWLEDGE)

Accident Investigation Programme

These use visual (semiotic) tools to help organisations learn from events, improve decision making and achieve culture change. I invite you to watch my talk (Keynote at EU Rail Safety days) [4] for my personal presentation on the topics covered in this article.

References

[1] "Are We Learning From Accidents, A quandary, a question and a way forward", Novellus, 25th April 2024, ISBN: 978-1738560301

[2] Why don't people speak up? The Power of Framing (Learning from Accidents Ep.1), https://www.youtube.com/watch?v=JJ5E95nuR9E, accessed May 2026

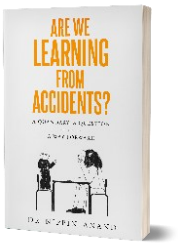
[3] The iCue engagement program™, https://www.youtube.com/playlist?list=PLUmJhx2rt4T01AuD3x-5vXM5lE6mtQ0dl, accessed May 2026

[4] Learning from accidents: a call for humanistic ethics (Keynote at EU Rail Safety days), https://www.youtube.com/watch?v=QGXL2Pq2F1A, accessed April 2026.

Dr. Nippin Anand, Founder and CEO of Novellus Solutions

Nippin is a consultant specialising in human-centred approaches to learning, risk and social decision making. He is a former master mariner with an MSc in Economics and a Ph.D. in Social Sciences and Anthropology. Nippin brings a Transdisciplinary lens to the challenges of work and organising spanning: the humanities, social psychology, mythology, semiotics, anthropology and philosophy.

As a former subject matter expert at DNV, Nippin asks challenging questions about the role of ethics, care, helping, moral meaning, emotions and trauma in the discourse of risk and safety. In so doing, he seeks to help the industry to become more person-centric and ethical when it comes to risk management.



Dr Anand is the author of three books 'Are We Learning from Accidents?', 51 Stories in Culture and Three Semiotic Walks. He is also the host of the podcast Embracing Differences, and a frequent writer, well known for transforming complex ideas into practical insights accessible and actionable for safety-critical industries.

SSS'27 – New Venue!

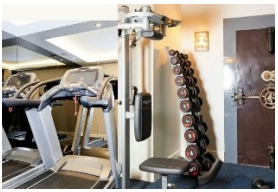
The SCSC is returning to Bristol for our annual Symposium in February 2027 and is hugely excited to be able to host the event in a new location – the luxurious Harbour Hotel. The hotel is housed within two grand, former 19th century bank buildings, blending its opulent historical architecture with vibrant, contemporary designs. This is a fantastic new location for the club in the heart of Bristol and here are a few highlights of the venue!

The Harbour Hotel is in Corn Street in Bristol less than 10 minutes' walk from the Royal Marriott where we've previously held the Symposium for many years. Corn Street is one of the oldest and most historically significant thoroughfares, forming the heart of Bristol when it was a walled medieval city.

Many of the luxury rooms in the hotel feature eclectic interiors that nod to the building's history, with some suites located in former high-ranking bank offices.

The main symposium will be held in the hotel's centrepiece – the Sansovino Hall with spectacular skylight and ornate period facades. This was built in 1850 inspired by Venetian architecture and was originally the main banking hall for Lloyds Bank.

One of the unique features of the hotel is its spa, which has been ingeniously built into the bank's former subterranean vaults. Guests can swim in both the indoor and hydrotherapy pools that sit behind the original, heavy iron vault doors.



As well as a well-equipped gym, the spa also includes a sauna, steam room, and treatment rooms offering a range of holistic therapies. One hour of free spa treatment is included for all residents every day!

For SSS'27 there will be a choice of accommodation packages, so there will be opportunities to upgrade to larger rooms. Here is a selection of some of the rooms the hotel has to offer.




There are also amazing locations for dining and socialising with the Harbour Kitchen and other lounges such as the Blue Room and Red Lounge.



The call for abstracts for SSS'27 is now open so please join us for this amazing event next year! Please book soon as there are some great early bird discounts and spaces will be limited for the premium rooms in the main hotel.



See scsc.uk/sss for more details about the Symposium and we are looking forward to seeing you there at this great new venue!

Human factors in the age of AI

Artificial Intelligence (AI) based technology is rapidly evolving and will have major implications for how humans and technology collaborate in workflows and operations. Dorthea Mathilde Kristin Vatn and Thor Myklebust use a traditional sociotechnical Human, Technology, Organization (HTO) framework to provide a theoretical introduction to the important implications for specialists working with Human Factors (HF) and suggest how the framework can be extended in the context of AI, highlighting three main implications for HF specialists in the age of AI.

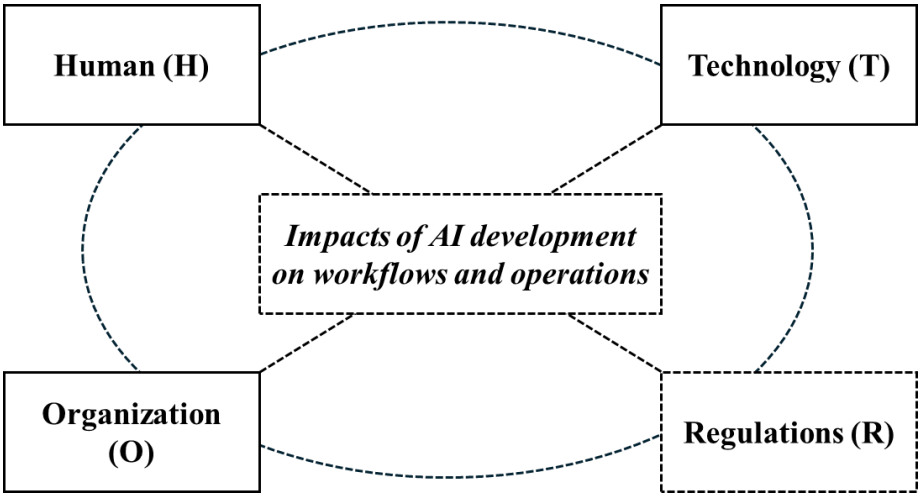
From a sociotechnical perspective, understanding how AI impacts workflows and operations requires a consideration of human, technological, as well as organizational aspects [1]. By providing equal emphasis on all aspects and the interactions amongst them, we are in a better position to understand how work is performed and the outcomes of it [2].

This idea underpins the "HTO concept" [1] highlighting that work activities can be described, analysed and understood by exploring the interactions between three sub-systems including Human (H), Technology (T), and Organization (O).

- The Human component encompasses a description of humans at four levels covering the human as a biological energy processing system, as a cognitive information processing system, as an individual with a unique history, and as a member of social groups and cultures.
- The Technology component refers to the technology itself, including specific procedures and methods tied to the use of the technology in the organizational context.
- The Organizational component refers to both the formal arrangements and informal social structures of an organization, including the structural dimensions tied to different organizational roles and hierarchies [1].

While the sociotechnical HTO concept encompass several facets that all are important to understand how AI impacts workflows and operations within organizational settings, we also believe that understanding AI in this context requires a careful consideration of regulations (R) that both affect how AI systems are developed, implemented and used in the organizational setting [3].

The figure below presents the components considered from a sociotechnical perspective when examining the impact of AI on workflows and operations, using the HTO concept [1] and incorporating regulations (R) as an additional element. We next explore how this extended HTO framework offers valuable insights into how AI is transforming organizational workflows and operational practices.



Technological aspects

Although AI systems should not be considered "novel" technologies in themselves, modern data-driven, machine learning-based systems introduce several new challenges. One first major challenge is the complexity of these systems, which often makes their inner workings opaque. As a result, many AI solutions are difficult to interpret, leaving human stakeholders unable to fully understand how these systems operate or how they arrive at their decisions [4].

This concern has led to an increasing interest in Explainable AI (XAI) as a research field [4], that from the technical perspective encompass technical tools and methods that provides insight into the inner workings of AI systems [5]. A second challenge relates to the inherently dynamic nature of modern data-driven AI systems, that are continuously evolving as they are retrained on new data. This aspect challenges the traditional view of technology development as a discrete activity, separate from its practical application in various contexts [6]. This technological challenge calls for the usefulness of complementing a model-centric view on AI development with a data-centric view on AI development.

Human aspects

While AI systems are often introduced as tools to automate tasks previously performed by humans, they frequently do not eliminate human operators but instead transform existing workflows. This shift underscores the need to consider how AI systems align with human cognitive processes, addressing concepts such as situational awareness, attention, expertise, and learning [7,8].

Accidents involving modern cars operating in autopilot mode underscore the importance of ensuring that AI-enabled features are designed to align with human cognitive capabilities. Similarly, research in the medical domain shows that reliance on AI can lead to a decline in human performance, emphasizing the risk of deskilling [9]. In addition, studies on Explainable AI (XAI) reveal that understanding how AI systems function requires careful consideration of the intended audience of explanations [4]. Although there may be a technical explanation for how an AI system operate and generate decisions, these explanations might not be understandable for certain user groups.

Organizational aspects

Beyond the technical and human aspects that need to be considered, several organizational aspects should be considered as well. While, from an organizational perspective, there are several aspects that could be discussed, we highlight two central aspects that follows from the technical and human considerations above.

"Although there may be a technical explanation for how an AI system operate and generate decisions, these explanations might not be understandable for certain user groups"

The first relate to the dynamic nature of AI systems that requires organizations to approach AI development and AI use as inseparable activities. This emphasizes the need for organizations to explore how development teams and users should work together, and how such work should be organized and structured.

The second relate to the importance of having an organizational capability to provide explanations of AI systems' operations and decisions to different stakeholders in the organizational setting [10]. Developing such a capability requires investments not only in specific XAI tools, but also people and processes [11].

Regulatory aspects

The EU Artificial Intelligence Act (AI Act, EU 2024/1689) establishes the first comprehensive and binding regulatory framework for AI, based on a risk classification that distinguishes between unacceptable, high, limited, and minimal risk systems. High-risk AI systems are subject to extensive requirements, many of which explicitly address Human Factors related issues (e.g. Article 14 – Human Oversight). The requirements cover risk management, data governance, technical documentation, human oversight, post-market monitoring, and conformity assessment prior to market access. The AI Act is embedded in the EU New Legislative Framework, linking compliance to CE marking, notified bodies, and harmonized standards, thereby integrating AI regulation into existing product safety regimes [3].

Beyond Europe, AI regulation is developing globally. Several jurisdictions, including the United States, China, Canada, the United Kingdom, Japan, and Australia, have introduced AI-related legislation, executive orders, or binding sectoral rules. These initiatives reflect increasing regulatory focus on safety, transparency, accountability, and risk management, although implemented through different legal approaches and levels of prescriptiveness.

A key implementation mechanism of the AI Act is the development of harmonized European standards. Once cited in the Official Journal of the EU, these standards provide presumption of conformity. An example is prEN 18286, a forthcoming harmonized standard defining a quality management system tailored to AI Act requirements that operationalizes Article 17 – Quality Management System by specifying organizational processes for documentation, traceability, risk management, and lifecycle governance of AI systems.

Implications of the HTOR-framework for HF Specialists

By providing examples of how AI impacts workflows and operations through the lens of the HTOR-framework we have elucidated that modern data-driven AI systems have implications covering technological, human, organizational, as well as regulatory aspects. Next, we discuss practical implications that follows our theoretical discussion above.

We need to rethink how user-centred design is performed

The dynamic nature of modern data-driven AI systems underscores the need to reconsider established approaches to user-centred design. Whereas the development of rule-based systems could adhere to traditional cycles of iterative user testing, culminating in a clear endpoint where the system is ready for deployment, determining such an endpoint is far more challenging in the context of machine learning-based systems.

From an organizational perspective, this necessitates the sustained involvement of AI expertise that collaborates closely with end users and domain specialists throughout the entire lifecycle of AI systems. These requirements, in turn, have significant implications for how work is structured and how resources are allocated to support the ongoing collaboration essential for effective AI development and integration within organizational settings.

Insight into human cognition is more relevant than ever

Both in the context of AI systems that are supposed to partly assist or take over certain work tasks, paying careful attention to human cognition when end users are introduced to new tools is increasingly important. In safety-critical systems, where human operators are retained to maintain controllability and intervene if the technical system fails or an unforeseen event occurs, it is essential to design equipment and workflows that preserve situational awareness, thereby enabling effective human oversight [3].

Furthermore, when designing tools that is supposed to assist highly skilled expertise, we need to pay careful attention to how such tools affect expertise development and learning, to avoid deskilling. This calls for the importance of using insight from fields such as psychology that can provide insight into how human learning and expertise development unfolds.

We need new standards covering human aspects

The existing set of international standards addressing Human Factors in relation to safety and AI is currently limited, representing an unresolved standardization gap.

While the next edition of IEC 61508 for functional safety introduces clearer references to AI (e.g. IEC TR 5469 and ISO/IEC TS 22440-1) and cybersecurity (e.g. the IEC 62443 series), its treatment of Human Factors remains limited and largely implicit. This is problematic as Human Factors should be addressed at a level comparable to AI and cybersecurity, with explicit normative references and lifecycle considerations in safety-related systems increasingly characterized by AI-driven behaviour.

"However, the absence of Human-Factors-specific standards relevant to the development and assessment of modern AI systems highlights a significant and unresolved standardization gap"

There are some standardization approaches that can be used, for instance ANSI/HFES 400 [12] can be used to perform a systematic assessment of human readiness and performance across the system lifecycle. However, the absence of human-factors-specific standards relevant to the development and assessment of modern AI systems highlights a significant and unresolved standardization gap.

References

[1] Karltun, A., Karltun, J., Berglund, M., & Eklund, J. (2017). HTO–A complementary ergonomics approach. Applied ergonomics, 59, 182-190.

[2] Hollnagel, E. (2017). The ETTO principle: efficiency-thoroughness trade-off: why things that go right sometimes go wrong. CRC press.

[3] Myklebust, T., Stålhane, T., & Vatn, D. M. K. (2025). The AI Act and The Agile Safety Plan (p. 156). Springer Nature.

[4] Arrieta, A. B., Díaz-Rodríguez, N., Del Ser, J., Bennetot, A., Tabik, S., Barbado, A., ... & Herrera, F. (2020). Explainable Artificial Intelligence (XAI): Concepts, taxonomies, opportunities and challenges toward responsible AI. Information fusion, 58, 82-115.

[5] Gunning, D., Vorm, E., Wang, J. Y., & Turek, M. (2021). DARPA's explainable AI (XAI) program: A retrospective. Applied AI Letters, 2(4).

[6] Waardenburg, L., & Huysman, M. (2022). From coexistence to co-creation: Blurring boundaries in the age of AI. Information and Organization, 32(4).

[7] Lee, J. D., Wickens, C. D., Liu, Y., & Boyle, L. N. (2017). Designing for people: An introduction to human factors engineering. (3ed). Create Space.

[8] Endsley, M. R. (1995). Toward a theory of situation awareness in dynamic systems. Human factors, 37, 85-104.

[9] Budzyń, K., Romańczyk, M., Kitala, D., Kołodziej, P., Bugajski, M., Adami, H. O., ... & Mori, Y. (2025). Endoscopist deskilling risk after exposure to artificial intelligence in colonoscopy: a multicentre, observational study. The Lancet Gastroenterology & Hepatology, 10(10), 896-903

[10] Vatn, D. M. K. & Mikalef, P. (2025). XAI Capabilities as a lens to theorize XAI in organizations. R&D Management conference, 2025, Pisa, Italy.

[11] McKinsey & Company. (2024). Building AI trust: The key role of explainability. Accessed 6th of Jan at: https://www.mckinsey.com/capabilities/quantumblack/our-insights/building-ai-trust-the-key-role-of-explainability

[12] ANSI/HFES 400-2021 (2021). Human Readiness Level Scale in the System Development Process. Accessed 6th of Jan at: https://www.hfes.org/Portals/0/Documents/DRAFT%20HFES%20ANSI%20HRL%20Standard%201_2_2021.pdf

Dorthea Mathilde Kristin Vatn, Research Scientist, SINTEF Digital

Dorthea is a research scientist within Human Factors, Psychology, & Information Systems at SINTEF Digital. She holds a MSc in Work and Organizational Psychology and is currently combining her role as a research scientist in SINTEF with pursuing a PhD in Information Systems. She works with questions at the intersection of people and technology, exploring how novel technologies impacts people and organizations both in a safety perspective and a business perspective.

Thor Myklebust, Senior Research Scientist, SINTEF Digital

Thor is a senior researcher in Safety and Reliability at SINTEF Digital. Since 1987 he has been involved in research, assessment and certification of products and systems. He has worked for the National Metrology Service, Aker Maritime, Nemko, and SINTEF. Thor has extensive experience in participating in several international committees and he has written four Springer books and more than 300 papers and reports.

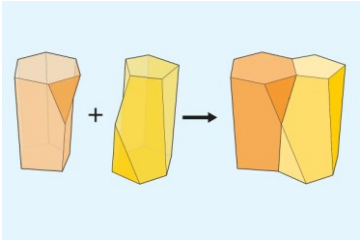
The shape that didn't want to be a box!

One of the fantastic features of this year's Symposium were the containers used to hold treats for delegates. These are based on the "Scutoid" shape that was only discovered in recent years, and has been cleverly designed into a foldable box by Mitali and Divya Atkins, the founders of Scutoid Design. Mitali and Divya Atkins provide a fascinating insight into this object and their journey in evolving the shape into a container that doesn't want to just be a box!

What is a Scutoid, who discovered it, and why is it important?

Not a term you've come across? Not surprising as it was coined less than ten years ago! Think of a Scutoid as the unsung geometric hero of your own body. It's a shape that mathematicians didn't even have a name for until 2018, yet it is a key feature of human and animal bodies, and thought to be in plants too.

The Scutoid is a geometric solid. It is characterised by having a different polygon at each of its two parallel ends (most commonly a pentagon at one end, and a hexagon at the other). The ends are connected by an additional triangular face that emerges partway along one of the lengths. This extra face is what makes the Scutoid unusual: it means the shape is not the same from top to bottom, and technically rules it out as a true polyhedron, since not all of its faces are flat.



In reality, Scutoids are not a single shape, but a family of shapes. The number of sides at each end can vary, giving rise to different members of the same geometric family, all sharing that characteristic mid-level transition.

In 2018, it was discovered that the Scutoid is the shape all our epithelial cells adopt when tissues bend during development. Epithelial cells form the lining of skin, organs, and body cavities, and as an embryo develops, these cells must curve and pack tightly together to build complex three-dimensional structures. The discovery of the Scutoid solved the long-standing conundrum about tissue packing: How do cells tile both surfaces of a curved tissue without gaps or overlaps, while minimising the energy cost of maintaining contact with their neighbours?

This discovery came through computational modelling. The research was a US-EU collaboration led by Javier Buceta, associate professor of bioengineering at Lehigh University, and Luis M. Escudero of Seville University in Spain. Using Voronoi diagramming – a mathematical tool for understanding geometric organisation – their model predicted that as tissue curvature increases, cells cannot be accommodated by columns or bottle-shapes alone. The model was pointing to a shape that, as Buceta put it, "didn't even have a name in mathematics" [1]. The team then verified the prediction by examining cell packing in real tissues from zebrafish and fruit flies, and found the shape was already there. The results were published in Nature Communications [2].

“Not a term you’ve come across? Not surprising as it was coined less than ten years ago!”

The name for the new shape was chosen for the shape's resemblance to the scutellum – the triangular part on the back of a beetle's thorax. The word Scutoid also traces back to the Latin “Scutum”, meaning Shield – fitting for a shape that nature uses to protect the lining of living tissues.

Beyond its biological significance, the Scutoid has implications for tissue engineering and regenerative medicine. Understanding how epithelial cells pack in three dimensions could inform the design of tissue scaffolds – the biodegradable structures used to help cells regenerate – and may eventually help researchers grow artificial organs that more accurately replicate how nature builds them.

From cell shape to cardboard container

Scutoid Design was incorporated in 2023 as a product and industrial design firm. With a passion for innovation, Mitali and Divya Atkins picked up their next challenge: to make Scutoid-shaped packaging, inspired by the name they had chosen for the company.

The Scutoid box began as an exploration of an extraordinary and unique shape. We were intrigued by how the Scutoid's dual geometry could offer something aesthetically and functionally different for packaging. A pair of Scutoids would create two perfectly tessellating compartments. Each would be a complete box within itself, seamlessly integrated into the pair. This offers a unique way to present a product and its accessory, or a gift and its companion piece, two flavours, two samples or two halves of a set for gifting at events.

The most challenging task was to create a net. A net is the flat template that folds up to form a three-dimensional box, and designing one for a Scutoid is considerably harder than it sounds.

The faces between the two polygonal ends of a Scutoid are not flat in the strict geometric sense – they curve subtly as they bridge the transition between the hexagon and pentagon. Treating them as ordinary planar faces, as you would in a conventional box, leads quickly to a geometry that simply won't fold correctly. The angles don't resolve. The edges don't meet. The box refuses to close. The process was entirely iterative: fold, assess, adjust, repeat.

"A net is the flat template that folds up to form a three-dimensional box, and designing one for a Scutoid is considerably harder than it sounds"

However once the basic net existed, we discovered that it was not a single solution, but a starting point. The geometry of the Scutoid allows for many different net configurations – different ways of folding a flat sheet into the Scutoid shaped pairs of containers.

Of everything that came out of this project, for us, one detail stands above the rest. We were able to design the Scutoid pair to be a single net, folded, that becomes two complete Scutoid boxes. One net in; one pair out.

We were honoured to provide The SCSC with the first 150 of these packages customised for the Symposium, filled with sweets for delegates! Perhaps you can think of a use in your company or event where these might help deliver gifts and act as a great talking point!

The Scutoid packaging is UK Design Registered, number 6496179.

References

[1] J. Buceta and L.M. Escudero, "Learn About the Scutoid," P.C. Rossin College of Engineering and Applied Science, Lehigh University, Bethlehem PA, https://engineering.lehigh.edu/bioe/research/learn-about-scutoid, accessed May 2026

[2] P. Gómez-Gálvez et al, "Scutoids are a geometrical solution to three-dimensional packing of epithelia", Nature Communications, vol. 9, article no. 2960, Nature Publishing Group, 27 July 2018. ISSN 2041-1723.

Dr Divya Atkins

Divya Atkins has a background in Computer Science, and has conducted research in formal methods, high-integrity and real-time systems and software metrics. Her experience includes safety-critical development, and project management, and she is interested in computer and network security. Aside from her technical expertise, she has a passion for sustainability, design and craft, which led her to co-found Scutoid Design with Mitali.

Mitali Atkins

Mitali is a product designer by training, having graduated from Central Saint Martins, University of the Arts London. She co-founded Scutoid design with Divya while still completing her BA degree in 2023.

SSS'26 Event Report

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

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

Staying safe from flying killer robots

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

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

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

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

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

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

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

Armchair Chat

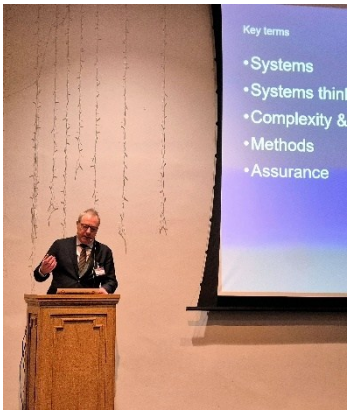
Our first Armchair Chat was with Karin Rudolph (Founder of Collective Intelligence UK) interviewing Mikela Chatzimichailidou (Professor of System Safety and Innovation at University College London).

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

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

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

Complexity and Assurance



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

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

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

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

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

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

Technical Entertainment

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

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

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

Exhibition and Drinks

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

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

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

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

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

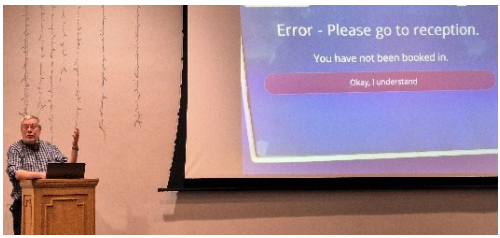
She examined three pairings:

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

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

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

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



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

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

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

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

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

Armchair Chat

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

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

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

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

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

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

Streams

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

Experience of static analysis

Possibility Analysis

Building Systems in Rust

Sensitivity Analysis

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

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

Scutoids!

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

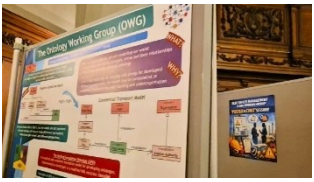
Social Events

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

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

Poster Session

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



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

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

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

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

Banquet

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

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

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

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

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

Effective and reflective assurance for AI-based autonomy

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

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

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

These models enable:

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

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

Armchair Chat

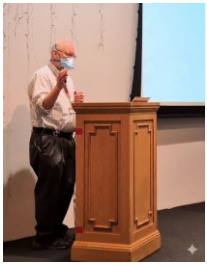
Our final armchair chat was Tim Kelly being interviewed by Tom Anderson. Tom introduced Tim, noting his background as a former professor at the University of York who worked on safety-critical systems and later became a rector in the Anglican Church, serving four parish churches in the East Riding and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

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

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

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

Overview of Embodied AI Safety



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

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

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

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

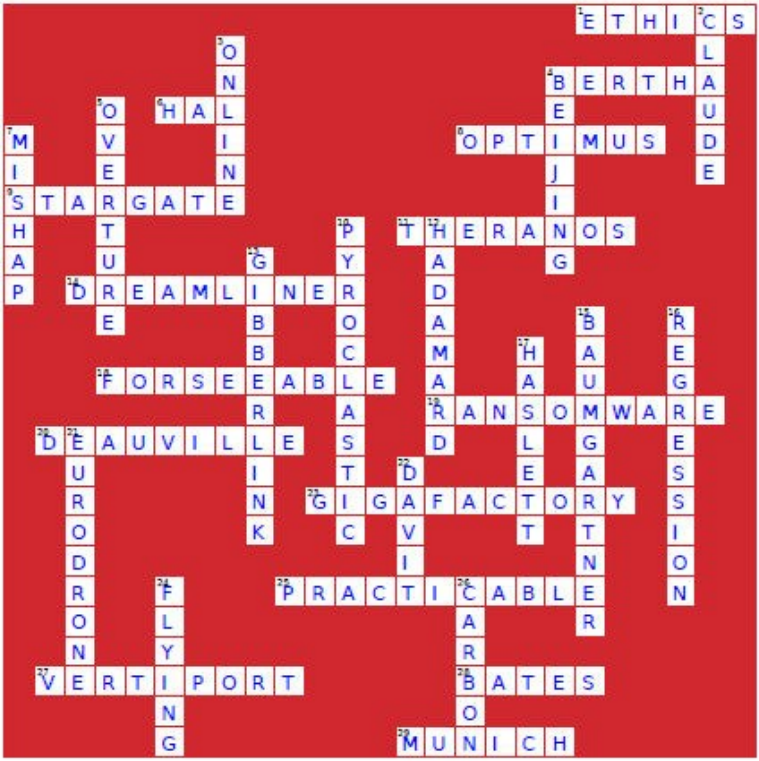
He discussed how humans are terrible supervisors of automation (known since the 1950s), with issues like perception-response time, automation bias and skill degradation with high-quality automation.

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

Crossword Competition

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

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



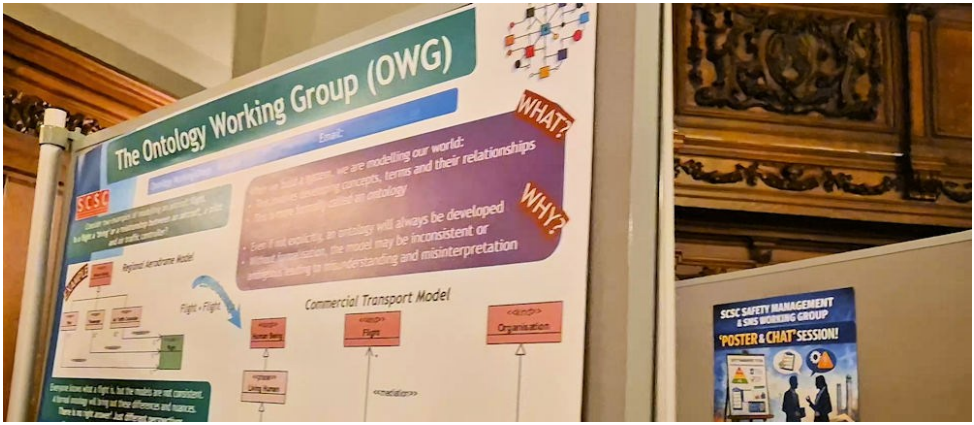
Across

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

Down

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

SSS'26 Posters



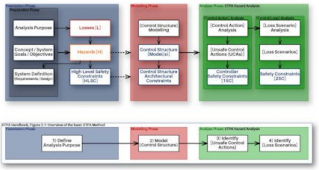
The following pages provide snapshots of most of the posters presented at SSS'26. If viewing via the pdf of the newsletter, SCSC Members can click on the poster to see a full-size pdf version of the poster.

Addressing Complexity using STAMP Control Structure Models and STPA Hazard Analysis

34th Safety Critical Systems Symposium (10th February 2026)

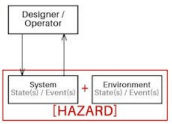
Mr Simon P.P. Whiteley BEng (Hons) MSc
Whiteley Aerospace Safety Engineering & Management Limited
https://www.whiteley-safety.co.uk/

STPA Hazard Analysis Process



[Hazard] & Control Structure Concept

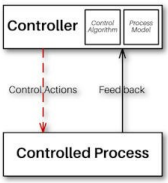
- "[Hazard]: A System state or set of conditions that, together with a particular set of worst-case environmental conditions, will lead to an accident (loss)."
  - State (condition), or
  - Event (time limited)



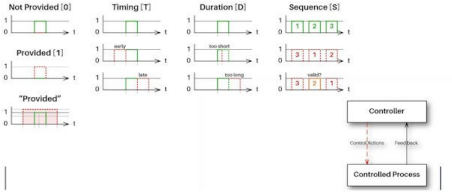
[Control Action] basic structure:

[unique.ID] <Source Controller> <[Control Action Type]> <[Control Action]> <Context> <Hazard Link [H]>

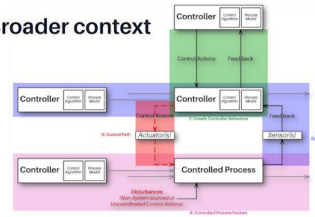
- <[Control Action Type]>
  - Not Provided [0]
  - Provided [1]
  - Timing [TE / TL]
  - Duration [DS / DL]
  - Sequence [S]
  - Magnitude [<M / >M]
- <[Context]>



[Unsafe / Contributory Control Actions]: Types



Broader context

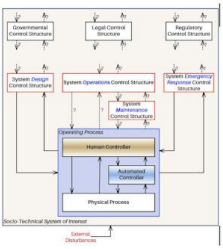


[Control Structure]

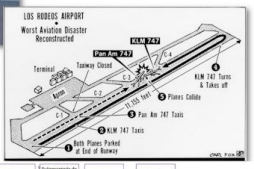
Thinking in terms of *Control Structures*:

- organises your thinking and understanding;
- provides a natural path to follow / a structure to work to.

Key to why STAMP-based assessments are so powerful.

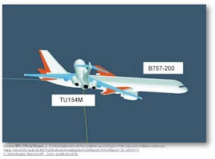


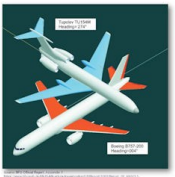
27/3/1977

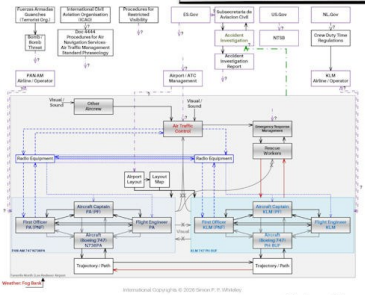


1/7/2002

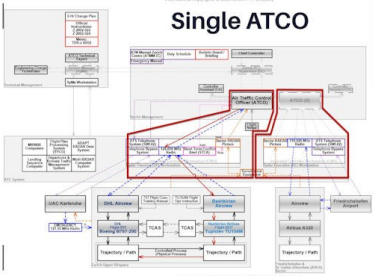
Collision Angle







Single ATCO



Towards Understanding the Benefits, Challenges and Limitations of using AI in the Design and Implementation of Safety Related Systems

POSITION PAPER SCOPE AND PURPOSE

- Overview of the current state of play in this fast-evolving field
- Insight into how a balance should be achieved between taking advantage of AI's transformative capabilities and the risks posed

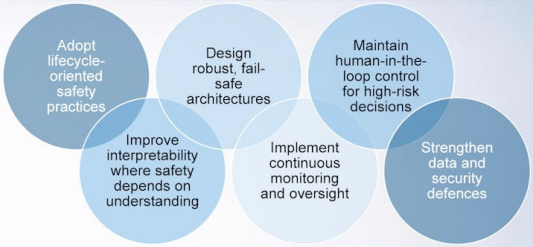
TYPICAL AI DEVELOPMENT LIFECYCLE

COMMON RISKS IN AI USAGE

- AI failures differ from traditional systems
- Different AI technologies present different risk profiles
- Data limitations are a dominant risk
- Poor generalisation and concept drift undermine reliability
- Opacity increases safety risk
- Edge cases and adversarial inputs remain critical vulnerabilities
- Agentic AI amplifies these risks

AI USE CASE SCENARIOS

POTENTIAL MITIGATION STRATEGIES



EXAMPLE AI RISKS vs OPPORTUNITIES

Opportunities	Enhancement of current design, VV&T, assurance and auditing processes	Enhanced design solutions Revolutionary new designs	Advanced system features Improved system performance Improved safety Enhanced decision making
Risks	Over dependence on AI Hidden mistakes Infringement of IPR Fabrication of evidence	Hidden flaws Increased design complexity Designs not well adapted to the real world	Catastrophic system failure Unintended behaviour
Mitigations	Checks and balances Competence in AI	Enhanced checks and balances Competence in AI	Regulation Safeguarding Assurance governance and rigour

FUTURE DIRECTIONS & CHALLENGES

Future progress must keep the primary focus on overall system safety, not AI technology in isolation. This requires advancing explainable and interpretable AI, evolving AI-specific regulation, and strengthening lifecycle management via continuous monitoring and operational control. Organisations must address the hidden technical issues in data dependencies, model coupling, and system evolution, while improving data stewardship and quality assurance. Emerging risks from generative and frontier AI—such as hallucinations, deepfakes, and unintended emergent capabilities—must be actively managed, with greater resilience to edge cases and rare events. Effective human–AI collaboration remains essential, supported by upskilling to meet the growing complexity of assuring safety-related systems that use AI

OVERVIEW OF CURRENT STATE

- Using AI not always considered in the context of the safety of the system
- AI is already embedded in safety-related systems development
- AI safety assurance is evolving into a lifecycle-oriented discipline
- Key challenges persist in emergent behaviours, data bias and dark data, limited explainability, adversarial vulnerability, and regulatory gaps
- Mitigation requires layered controls such as model transparency, robust and hybrid architectures, defensive data practices, adversarial testing, strong human-in-the-loop oversight, etc.
- Standards and governance are evolving, and sector-specific assurance frameworks are still emerging
- Responsible progress depends on collaboration and caution

SCSC For Everyone Working in System Safety

Safe AI Working Group (SAIWG)

SAIWG KEY AIMS

- Ongoing development of Autonomous Systems WG work
- Review of research in AI usage in the development (testing, V&V, et al) and implementation of Safety related systems

STAKEHOLDERS

Broad spectrum of professionals and stakeholders involved in safety-related systems

- Safety engineers, systems engineers, software engineers, and managers directly involved in the development, verification, and validation of safety-related systems
- Regulators, auditors, and policymakers who play a vital role in shaping the standards and regulations governing AI safety
- Business managers who oversee the strategic implementation of AI systems
- Owners, maintainers, and operators responsible for the long-term deployment and maintenance of these technologies

SAIWG PLANS FOR 2026

- Consolidate high volume of research captured
- Publish high-level working group position paper
- Develop draft guidance incorporating principles and objectives for the safety assurance of systems with AI

Safe AI Working Group, SCSC
WG Chair: alan.simpson@ebeni.com

TOWARDS DYNAMIC SAFETY CASES FOR COBOTS
LEVERAGING STANDARDS, INDICATORS, AND DIGITAL TWINS

Laure Buysse, Mohammed Tloul, Dries Vanoost, Davy Pissoort

Safe Autonomous Systems through Dynamic Assurance Cases

MPRO

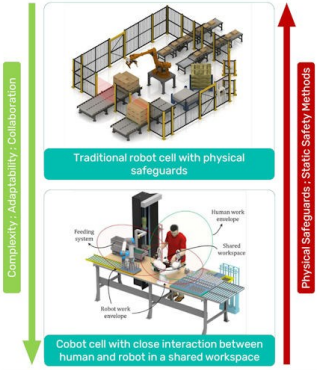
TD7 System-of-System Technologies

GOAL

Operationalize **runtime assurance for collaborative robots** through a standards-aligned framework that connects safety arguments to runtime **safety performance indicators** and supports continuous monitoring, assessment, and update using dynamic safety cases.

MOTIVATION

- Traditional industrial robots rely on physical separation (e.g., fences and cages) for safety, whereas collaborative robots operate in shared workspaces where such safeguards are infeasible.
- As tasks, layouts, and human behavior change, safety approaches developed at the design stage no longer reflect operational reality.
- Maintaining continuous safety without diminished performance or constrained collaboration requires runtime safety assurance methods, motivating the use of dynamic safety cases for cobot systems.



APPROACH

(1) Patterns (Assurance Structure)

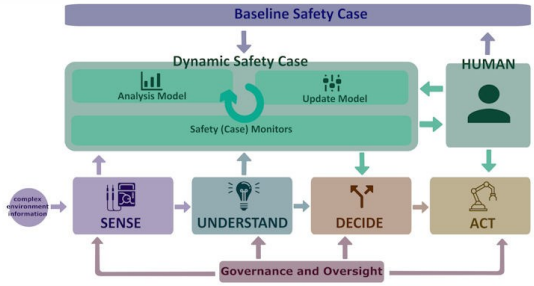
Instantiate standards-aligned assurance case patters based on the collaboration mode(s) (intervention, teaching, interaction, physical collaboration)

(2) Safety Performance Indicators (SPIs)

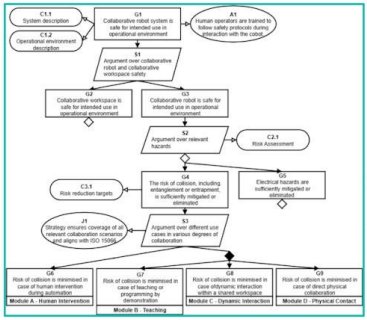
Select relevant SPIs and map to runtime data streams. Consider criticality levels and minimum dimensions

(3) Digital Twin

Improve coverage and reduce uncertainty through virtual sensing, predictive checks, and what-if simulations of rare events



RESULTS



Argument Link	SPI Metric	Criticality
G2	Workspace occupancy	Medium
G4	Number and extend of changes to path planning	Low

Argument Link	SPI Metric	Criticality
G6.1	Frequency of (safety-rated monitored) stops	High
G6.2	Separation distance between all operators and the cobot (incl. violations, average …)	Mandatory
G6.3	Tool centre point velocity	Mandatory
	Location of the operator(s)	Low

Argument Link	SPI Metric	Criticality
G7.5	Tool centre point velocity	Mandatory
G7.6	Cobot position within (restricted) space	Low
E7.1	Trend on tool centre point velocity data with respect to the defined limit	Medium
E7.2	Trend separation distance cobot and operator with respect to the defined limit	High

Collaboration Mode	Monitorability	Assessibility	Updateability
Human Intervention	2	1	1
Hand Guiding	2	2	2
Shared Workspace	2	2	2
Physical Collaboration	3	3	3

KEY TAKE-AWAYS

- Static safety cases are insufficient for collaborative robots operating in dynamic, human-centred environments.
- Dynamic safety cases enable runtime-adaptive, standards-aligned safety assurance for cobots by linking assurance case patterns, runtime indicators, and digital twins.

FURTHER READING

- Buysse, L., Habli, I., Vanoost, D., Pissoort, D. (2025). *Safe autonomous systems in a changing world: Operationalising dynamic safety cases.* Safety Science, 191, Art.No. 106965. doi: 10.1016/j.ssci.2025.106965
- Buysse, L., Tloul, M., Vanoost, D., Pissoort, D. (2026). *Towards Dynamic Safety Cases for Cobots: Leveraging Standards, Indicators, and Digital Twins.* Safety-Critical Systems Symposium 2026 (accepted)

laure.buysse@kuleuven.be

Part of this research has received funding from the Research Foundation Flanders (FWO) under grant no. 1S17123N. Part of this research has received funding from the European Union's Horizon Europe research and innovation program under the Marie Skłodowska Curie grant agreement No 101169797 [AERIALIST]. This publication reflects only the author's view exempting the European Union from any liability.

Information Systems: Advisory to Assured

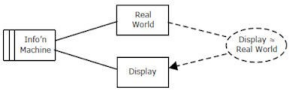
Information systems are increasingly relied upon in a safety related context. However, standards and guidance are limited for how to assure their safety.

NOT TO BE RELIED UPON FOR SAFETY

Paul Ensor MSc MRAes CEng
Jade Edwards BEng

Introduction

Information systems and their databases often support safety-related, task-oriented decision making. Although guidance addresses data safety, equivalent guidance and standards for the safety assurance of information systems are lacking. Existing safety standards focus on Functional Safety, resulting in safety cases that are frequently caveated by with "advisory only or "not to be relied upon". This undermines the utility of information systems in safety-related contexts.



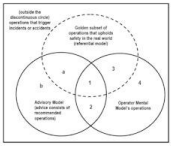
Michael Jackson's Problem Frames [1]

The Information Display Problem:

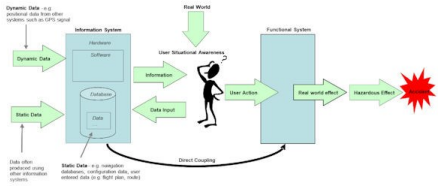
Jackson's problem frames describe the information machine problem. The challenge is to make the information display equivalent to the real world. The supporting databases, software integrity and complexity of the real world make this challenging.

Human Operator and Advisory Systems

In his paper on Advisory Systems Safety, Oliveras describes the relationship between the user and system model of the real world in relation to safe states. The ideal state is where all 3 agree as in case 1. Oliveras describes different cases where there is a disconnect between safety in the real world, the advisory model and the user's mental model.



Oliveras's Human operator and advisory system cases [2]



P. Ensor, Safety Context of Data within Information Systems [3]

Safety Context of Information Systems

The safety context of Information systems is based on the user receiving information from the system and the real world and making decisions. These decisions can result in user action in a functional system that could have a direct real world safety effect. Information systems often indirectly contribute to safety through the accident chain.

Endsley's Model of Situational Awareness

Endsley model of situational awareness uses Goal Directed Task Analysis, which can help to define the safety context of the information based on his 3 levels of situational awareness:

- Level 1 - Perception of elements in the environment
- Level 2 - Comprehension of the current situation
- Level 3 – Projection of the future situation

This model can help identify is where the information system is the sole source of safety related information.

Goal			
-	Subgoal		
	-	*Decision*	
		-	Projection (SA Level 3)
		-	Comprehension (SA Level 2)
		-	Data (SA Level 1)

Endsley's Model of Situational Awareness [4]

Information System Safety Assurance

Once the safety context of the information system is understood, there is very little guidance or standards for how to provide the necessary safety assurance. There are many types of information systems used in different industries and some industry specific standards exist. However, most safety standards are focused on functional safety and do not address the unique requirements of assuring the safety of information systems.

Have you used caveats in safety cases such as "for situational awareness only" or "not to be relied upon for safety" knowing this is a sticking plaster? Want to get involved in developing guidance and exploring the topic further, then please contact us using the details below.

Data is an important component of most information systems

References

1. M. Jackson. Problem Frames: Analysing and Structuring Software Development Problems, Boston, MA: Addison-Wesley, 2001
2. C.S. Oliveras, Systems, Advisory Systems and Safety, Dept. Comput. Sci., University of Newcastle upon Tyne, UK, 2002
3. P. Ensor, "Safety Analysis of Navigation Data," MSc Thesis, Dept. Comput. Sci., Univ. York, UK, 2009
4. Endsley, M. R. "Designing for situation awareness in complex systems" in Second int. workshop on symbiosis of humans, artifacts and environment, Kyoto, Japan 2001.

Further Reading

1. HSE CONTRACT RESEARCH REPORT 419/2002, Developing advisory software to comply with IEC-61508HSE Books (2002).
2. C. Carvalho, E. Borycki and A. Kushniruk, "Ensuring the Safety of Health Information Systems: Using Heuristics for Patient Safety" in healthcare Quarterly, Vol. 12 Special Issue, Patient Safety, 2009
3. ED-109A | Software Integrity Assurance Considerations for Communication, Navigation, Surveillance and Air Traffic Management (CNS/ATM) Systems

Contact:
Paul Ensor and Mike Parsons @ mike.parsons@scsc.uk

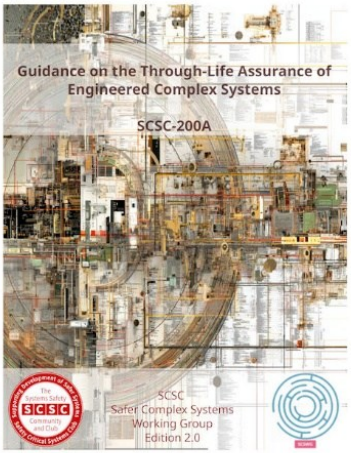
The Systems Safety SCSC Community and Club — Supporting Development of Safer Systems — Safety Critical Systems Club

SCSC For Everyone Working in System Safety

SCSC: Safer Complex Systems Working Group

Guidance Document

Edition 1 of the WG Guidance was published at SSS'25. Edition 2 is now available.



WG Chair: Mike Parsons
Guidance Editor: Chris Hobbs

Analysis of Incidents

- R.101 Airship (1930)
- Herald of Free Enterprise (1987)
- Clapham Junction Railway Crash (1988)
- Boeing 737 Max 8 (2018/2019)
- CrowdStrike Software Update (2024)

A Complex Engineered System is a Socio-Technical system that exhibits:

- emergent behaviour: system behaviour that could not have been predicted by examining its components individually.
- whole/part interactions: bidirectional non-separability between the identities of the parts and the identity of the whole. Not only is the identity of the whole determined by the constituent parts, but also the identity of the parts are determined by the whole.
- non-linearity of effect: a small change to part of the system can cause a disproportionately large change in the system's behaviour.
- coupled feedback: one element of the system feeds back positively to other parts which then affect the original element.
- multiscale behaviour: the system's structure exists on many scales and characteristics are not reducible to only one level of description.
- indeterminate boundaries: boundaries are intricately woven with their environment and other interacting systems, particularly during accident investigation.

Approach

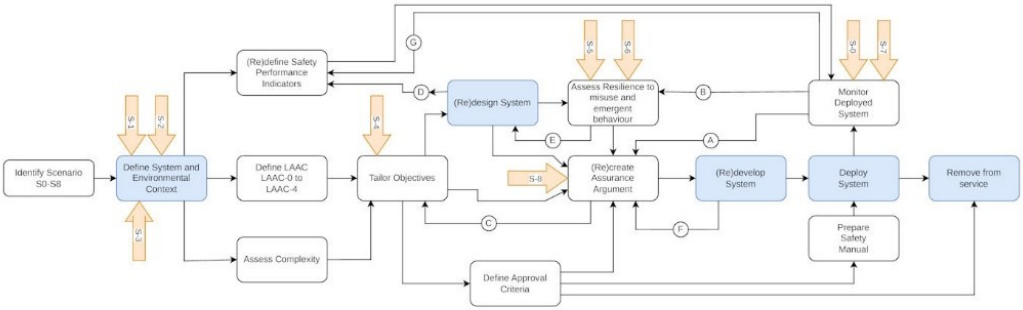
It can be difficult deciding whether a system is complex (unexpected emergent behaviours may arise later): we take the approach that the guidance can be applied in any case.

The Guidance introduces 7 principles and related objectives to define assurance of a complex system. The table below shows Principle 4. Compliance with the objectives then provides an assurance position.

Id	Principle
4	**P-4: The SCS SHALL be resilient to emergent, unintended and unanticipated behaviours of its elements and their interactions, including those caused by accidental or deliberate misuse.**
	Objectives
4.a	Unintended behaviours arising from the SCS SHALL be considered.
4.b	Unintended behaviours resulting from fault-free cases SHALL be considered.
4.c	Emergent behaviours of the SCS SHALL be considered.
4.d	Behaviours due to design decisions SHALL be considered.
4.e	Resilience measures to deal with unknowns of the SCS SHALL be considered.
4.f	SCS behaviours due to potential non-linearities SHALL be considered.
4.g	SCS behaviours due to potential whole/part interactions SHALL be considered.
4.h	SCS behaviours due to deliberate or accidental misuse SHALL be considered.
4.i	Degraded and contingency modes of the SCS SHALL maintain a defined subset of these objectives to a specific level.
4.j	Resilience to SCS behaviours SHALL be considered as part of sign-off/approval.

Outstanding Question

Unexpected conditions will occur in a complex system's environment, so it is essential that it be resilient. What techniques are suitable for providing resilience in a complex system?



IEC 63187

Systems engineering — System safety Complex systems in defence programmes

"A speciality engineering view of ISO/IEC/IEEE 15288"

IEC 63187-1 is currently at the Committee Draft for Vote development stage. Publication as an international standard is planned in 2026, subject to international approval.

IEC TR 63187-2 is being drafted as a Technical Report to support implementation of IEC 63187-1.

Motivation for a new standard

The market is evolving towards:

- More **complex** systems with **complex** functions and **complex** architectures
- **New technologies** and new applications of existing technology
- **Fewer humans in the loop** to handle safety
- **Dynamically evolving risks**

Existing safety standards do not:

- Align with **system engineering**
- Address **multi-layered systems** recursively
- Capture **emergent properties** at system level (without failure)
- Fully allow interaction with other **engineering domains**

Objectives

Safety:

- Propose a comprehensive approach for **adapting safety requirements to risk**
- Propose an approach for **risk control** across the layers of a system
- Propose an approach to control situations of **dynamic risk**
- Maintain an open approach towards activities and assurance **outcomes**
- **Account for traditional approaches**, in particular quantitative, for **realised system elements**

Systems engineering:

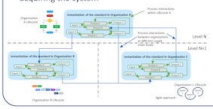
- Propose a way to **embed safety engineering** in systems engineering (ISO/IEC/IEEE 15288)
- Propose an approach enabling **instantiation between system layers** and between supply chain levels **without limitations**
- Distinguish the system conceptual activities from the realisation of the system physical and logical elements
- Propose a seamless **interface to existing safety standards** for realising physical and logical system elements

Fundamental principles

- **Risk-based** (ISO 31000): focus on hazards and their consequences rather than quantitative probability; risk is the effect of uncertainty on objectives
- **Systems-based** (ISO/IEC/IEEE 15288): recursively applying systems engineering principles at multiple levels in the systems hierarchy and supply chain
- **Systems theory** and **control theory**: considering interacting system elements that can lead to detrimental effects without component failure
- **Integrating safety into systems engineering** as a fundamental part of engineering the system, with the flexibility to trade requirements
- **Appropriateness of approach:** addressing threats to safety from sources with different types of characteristic
- **Supply chain considerations**: addressed to apply proportionately over organisational boundaries
- **Solution independent**: regardless of the origin or lifecycle stage of realised system elements
- **Goal-based:** providing a framework to identify and achieve safety objectives, rather than a prescriptive set of rules or specifications

Acquisition viewpoint

- Defence applications are subject to dynamic risks: detriments (harms), safety objectives and compromises depend on the operational context (CONOPS)
- Risk acceptability can only be determined on a case-by-case basis, by the organisation acquiring the system



- Definition of detriments from the acquirer's own viewpoint (i.e. "what is important")
- Convergence and control of Measures of Importance (MoI) through schemes agreed between parties (i.e. "how important is that?")
- IEC 63187 is applied by organisations across the supply chain, giving a consistent approach
- Each organisation defines its own suitable life cycle on the basis of the generic ISO/IEC/IEEE 12207 life cycles
- Organisations agree on interface arrangements, allowing consistent and traceable engineering

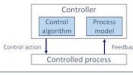
Systems engineering viewpoint

Control theory:

- Detriments from all domains of interest (mission, safety, security, ...) can be considered in decision making
- Centred on the Perception–Interpretation–Decision–Action loop.
- Safety viewed as the robustness of control under internal and external perturbations
- Modelling control structures allows scenarios that lead to undesired system states to be identified
- Humans are integrated in the control structures

IEC 63187 considers all the system life cycle processes from a safety viewpoint:

- Implementing a "Safety View" (as an aspect of speciality engineering, as per ISO/IEC/IEEE 24748-1:2024 annex D4)
- Supplementing ISO/IEC/IEEE 15288 process outcomes with specialised requirements, criteria and informative notes, to clarify what is needed from the safety viewpoint



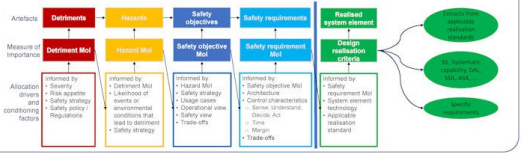
Implementation viewpoint

- The actual production of system elements is not in the scope of IEC 63187. The standard is limited to their specification and acceptance, not the detail of their realisation
- The requirements of IEC 63187-1 do not interfere with the prescriptive standards for the production of system elements (e.g. for E/E/PE: DO178C, IEC 61508-3, IEC 61508-2)
- Inputs to realisation work will be defined based on the detriments, hazards, safety objectives and safety requirements; and the design constraints will integrate the elements necessary for the realisation

	Visibility of design and configuration	No visibility of design and configuration
Controllability of the design	Route to realisation 1_A	Route to realisation 3_A
No controllability of the design	Route to realisation 2_A	Route to realisation 4_A

Safety engineering viewpoint

- No split imposed between the system under control and the safety functions, as is the case with IEC 61508
- The IEC 63187 approach remains compatible with the fundamental principles of IEC 61508 and MIL-STD-882E
- The Measure of Importance (MoI) concept allows classifying various artefacts according to associated criteria/parameters and moderation factors to reflect how much they matter to the stakeholder
- Defining a MoI makes it possible to avoid the saturation of integrity levels that can occur when allocating requirements mechanically



Takeaway points

Systems engineering
- No mandated safety deliverables; safety outcomes are embedded in the systems engineering outcomes, open life cycle adaptable by each stakeholder organisation

Hazards, risks and detriments
- Principles of control theory
- Based on a unique concept to express objectives from all specialities and allow arbitration when necessary

Safety objectives and safety requirements
- Dissociation of constraints on the system of interest (objectives) from the solutions satisfying them (safety requirements) and allows identification of emerging aspects

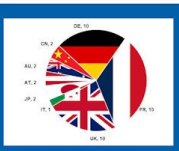
Measures of Importance
- No predefined index (no equivalent to SIL, DAL, ASIL, etc.)
- Definition of normative requirements to allow stakeholders to define ad hoc Measures of Importance in a consistent global framework

Safety performance
- Accounts for the fact that the system safety performance, if expressed only quantitatively as the sum of the realised system element failures, cannot represent the overall system safety

Safety assurance
- Accounts for the fundamental difference between the necessary means to deliver system safety and the necessary means to guarantee their effectiveness

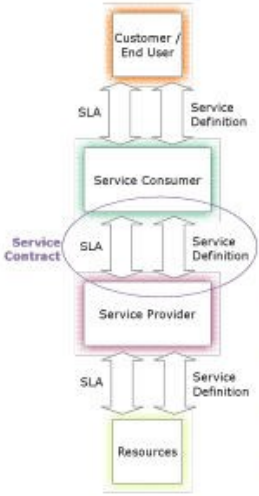
IEC 63187 development ecosystem

50+ Participants from 11 contributing nations



IEC 63187 is being developed by Working Group 18 of the IEC's TC65/SC65A technical subcommittee: Industrial-process measurement, control and automation – Systems Aspects. Members of the international working group are experts nominated by the national standards organisation of each country that takes part.

For more information, contact james.inge@scsc.uk



Service Definition - describes the Services available for consumption which may include technical and/or commercial aspects. It may include deliverables, prices, contact points, availability, ordering and processes to request Services. This may include a service catalogue.

Service Level Agreement (SLA) - the agreement between the Service Provider and Consumer that defines the level of service that the Consumer will receive. It usually specifies responsibilities of both parties and defines the penalties in the event the specific targets in the SLA are not met

Service Contract - The contractual agreement between Service Provider and Service Consumer. Note that the Service Consumer may not be involved in defining the service or the SLAs at the outset; they may be provided pre-defined and pre-packaged by the Service Provider on a take-it-or-leave-it basis.

A **Service Based Solution (SBS)** comprises the systems, organizations, processes and resources to deliver and manage the services through life. It may consume other services. An SBS delivers capabilities to its customers via a set of collaborating services.

Service Assurance Principles

The intent of the service assurance requirements shall be maintained through the service definitions, service levels, the service architecture and the agreements made at service interfaces

Unintended behaviours of the service-based solution shall be identified, assessed and managed

These principles shall be established and maintained throughout the lifetime of the SBS, resilient to all changes and re-sourcing

1. Requirements shall be defined to address the service-based solution's (SBS) contribution to both desirable and undesirable behaviours
2. Service assurance requirements shall be satisfied
3. The confidence established in addressing these principles shall be commensurate with the level of risk posed by the service-based solution
4.
5.
6.

Service Assurance Working Group

"To produce clear and practical guidance on how services should be managed in a safety related context, to reflect emerging best practice"

Members 31
Meetings 47

https://scsc.uk/gs
contact: mike.parsons@scsc.uk

Level of Service Assurance	Definition (Service Consumer View)
LSA 0	No safety aspects at present in service
LSA 1	Minor safety aspects with little impact of failures (minor injury possible but unlikely)
LSA 2	Safety aspects with some impact of failures (several injuries possible)
LSA 3	Significant safety aspects with service with major impact (could indirectly lead to single death or multiple injuries)
LSA 4	Service is safety-critical: service failures could have catastrophic impact (could directly lead to multiple deaths)

SCSC

Data Safety Initiative Working Group (DSIWG)

Started: January 2013 | 96 Meetings | 109 Members

SCSC-127K

Mission Statement:
"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."

SSS'26 poster sponsored by

www.scsc.uk/gd

mike.parsons@scsc.uk

New Principle added

Principle 1: data safety requirements shall be defined to address the data contribution to system hazards

Principle 2: the intent of the data safety requirements shall be maintained throughout requirements decomposition

Principle 3: data safety requirements shall be satisfied

Principle 4: Hazardous system behaviour arising from the system's use of data shall be identified and mitigated

Principle 5: The confidence established in addressing the data safety assurance principles shall be commensurate to the contribution of the data to system risk

Principle 6: All principles SHALL be established and maintained through all changes, reuse, re-deployment and re-purposing.

Recent Data Safety accidents

Tandem Insulin Pump

Excessive Bluetooth data downloads caused battery failure.

Data property lost: ***Goldilocks***

Poncheon Bombing

Incorrect entry of target coordinates during a live-fire exercise led to the bombing of a civilian area.

Data property lost: ***Integrity***

A320-214 Catania incident

Failure to enter takeoff parameters into the flight management system (FMS) contributed to an unexpected loss of altitude on takeoff.

Data property lost: ***Completeness***

New guidance: Version 4.0 released at SSS'26:

Major re-write of the guidance, split into 3 volumes

Volume 1 contains the normative material. It describes the "what" of the guidance and states what is needed to ensure conformance with this guidance, if required. It should be of use to those establishing processes and procedures for data safety assurance and for those doing the actual assurance.

Volume 2 contains the informative material. It describes the "how" of the guidance and should be of particular value to data safety practitioners.

Volume 3 contains the discursive material. It describes the "why" of the guidance and gives background and supporting material intended to improve practitioner's understanding of the data safety management processes and of issues relating to data safety management.

Selected Objectives

Id	Objectives
1.a	System context and intended use SHALL be established.
1.b	Legal and regulatory obligations and requirements SHALL be incorporated.
1.c	Applicable standards and relevant guidance SHALL be incorporated
1.d	Existing data quality and data assurance requirements and constraints SHALL be identified

Id	Objectives
6.a	All changes that impact these principles and objectives SHALL be assessed and managed.
6.b	Assurance artefacts SHALL be maintained.
6.c	Measures SHALL be in place to monitor the behaviour of the SCS at appropriate intervals throughout its life.
6.d	Use SHALL be monitored for change and an assurance impact analysis undertaken where necessary.
6.e	Evolution and incremental change SHALL be considered.
6.f	Longevity and obsolescence of data SCS SHALL be considered.

New Properties added

Property	Abbreviation	Description
Analysability	Z	The data (including any metadata) is of a suitable size, type and format to enable it be usefully analysed
Explainability	X	The data can be meaningfully explained by a suitable mechanism, to those who need to understand it
Clarity	K	The data is visible, unmasked, not hidden or obscured and not camouflaged
Goldilocks	G	The data is just the right size – not too much and not too little

Example Data Problem Storyboard - Tandem Insulin Pump

This relates to the Goldilocks property as the failure was caused by excessive data downloads.

A Safety Case Report Format

Follow us on LinkedIn

Buy now at Amazon

Helping people to understand your safety case
www.barker-eaton.co.uk

"Very experienced authors – definitely worth a read"
Professor John McDermid, University of York

"If the book is consulted, digested and followed it should render considerable assistance; even if read and not followed, a reader should acquire much valuable insight."
Professor Tom Anderson, Newcastle University

"Excellent, well written and presented. Every Safety Manager should have a copy of this book."
John Stelfox, Nanaimo Search and Rescue Vancouver Island (retired)

"... the book is as much about what needs to be in the safety case itself as it is about the corresponding SCR. Why not use the book at an early stage in a project to help design a convincing safety case... "
Steve Kinnersly, B.Sc. D.Phil. MRSC ISA

"It is a useful resource that can also serve as a check on the completeness of your safety case; if the Safety Case Report format asks for something you don't have in your safety case, can you write a compelling justification as to why it is not needed, or did you miss something?"
John Spriggs, Editor of the SCSC eJournal

To register an interest in workshops on the derivation of the format contact mail@barker-eaton.co.uk

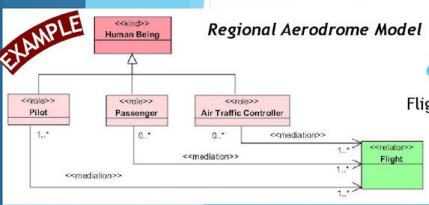
The Ontology Working Group (OWG)

SCSC — For Everyone Working in System Safety

Ontology Working Group - Website: https://scsc.uk/owg - Email: ontology@scsc.uk

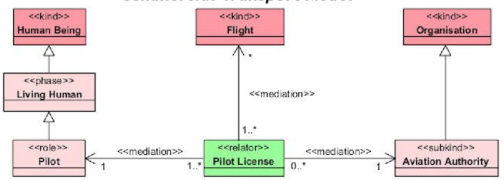
Consider two examples of modelling an aircraft **flight.**
Is a flight a 'thing' or a relationship between an aircraft, a pilot and air traffic controller?

EXAMPLE



Flight ≠ Flight

Consistent?



Everyone knows what a flight is, but the models are not consistent.
A formal ontology will bring out these differences and nuances.
There is no right answer! Just different perspectives.

WHAT?

When we build a system, we are modelling our world:
- This involves developing concepts, terms and their relationships
- This is more formally called an *ontology*

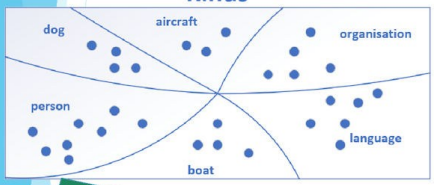
WHY?

- Even if not explicitly, an ontology will always be developed
- Without formalisation, the model may be inconsistent or ambiguous leading to misunderstanding and misinterpretation

The Unified Foundation Ontology (UFO)
A formalised and consistent foundation model for developing ontologies.
Implemented as stereotypes in a modified UML notation: **OntoUML**

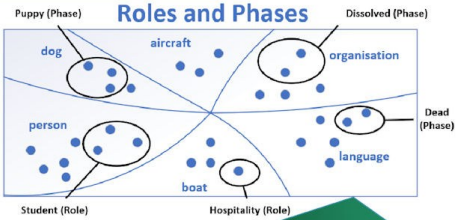
Examples of UFO foundation classes: **Kinds, Roles & Phases and Mixins:**

Kinds



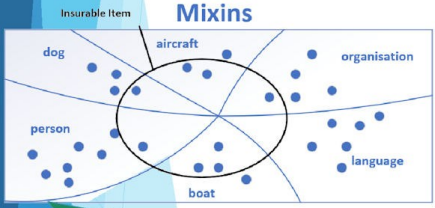
"Kinds" endure, are countable and share "identity principles" - (common properties whose values distinguish specific individuals)

Roles and Phases

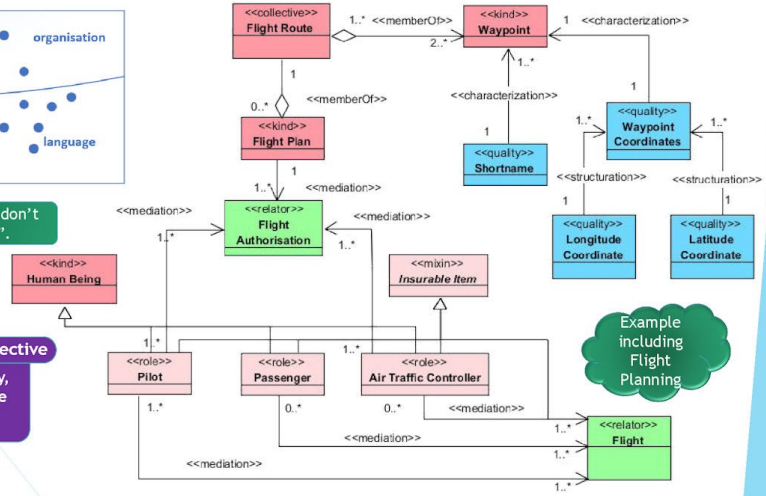


Roles and Phases are specialisations of kinds that are transitory. A dog is always a dog but goes through a "phase" of being a puppy.

Mixins



Mixins are properties that span kinds so don't share the same "identity properties".



Example including Flight Planning

The Ontology Working Group Objective

"Develop a clear, systematic terminology, and unambiguous model of risk and value concepts and their relationships"

Meet by using

- the Unified Foundation Ontology (UFO)
- visual modelling tools (Visual Paradigm)
- ontologically consistent modelling notations (OntoUML)

and monitoring work of other working groups (eg. ISO & IEC)

Current projects

- An Ontology of Risk and Value for Safety and Security Engineering
- Data Safety Guidance: Data Properties Model
- SCSC Newsletter Serialisation (now on Episode 3!)

Revision 2026/1.0

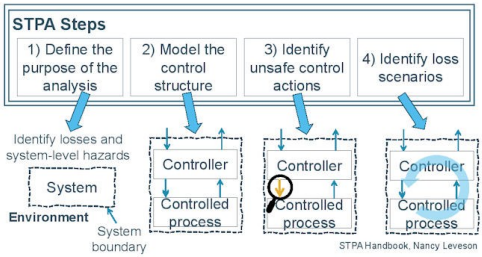
M.Tloul, L. Buysse, D. Vanoost, and D. Pissoort
Department of Electrical Engineering (WaveCore), M-Group, KU Leuven, Bruges, Belgium Flanders Make@KU Leuven, Leuven, Belgium
Email: mohammed.tloul@kuleuven.be

STPA analysis for a wheelchair with a head-foot steering system

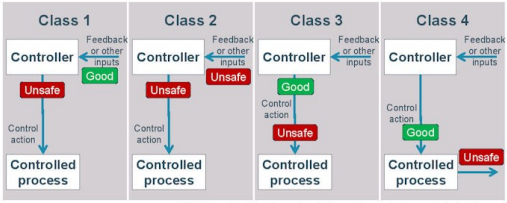
GOAL

This work aims to enhance **safety assurance for a powered wheelchair equipped with a head-foot steering system** designed for individuals with severe motor impairments. It seeks to apply **System-Theoretic Process Analysis (STPA)** as an initial step to identify hazards and improve system design.

APPROACH



- In step 1, identify losses related to **safety and mission**.
- In Step 2, divide the control structure into **two primary control loops**: one representing the user and the other representing the technology.
- In Step 3, identify **all unsafe control actions**.
- In step 4, follow the **formal approach for defining the loss scenarios** (using the following four classes).



STPA Step 4 Building Scenarios - A Formal Scenario Approach, John Thomas

KEY TAKE-AWAYS

- **STPA** goes **beyond component failures**. It addresses unsafe interactions among **software, hardware, and humans**.
- It is **challenging** to account for users' **different physical and cognitive abilities** during the analysis.
- **Control structure division** helps focus on either **human** or **technology aspects**.
- The **formal approach** in step four identifies potential loss scenarios in a structured manner, requiring **more resources** but enabling **future automation**.

Part of this research has received funding from the European Union's Horizon Europe research and innovation program under the Marie Skłodowska-Curie grant agreement No 101169197 (AERIALIST). Part of this research has received funding from the Research Foundation Flanders (FWO) under grant no. 1S17123N. This publication reflects only the author's view exempting the European Union from any liability.

MOTIVATION

Traditional hazard analysis methods focus on component failures and do not adequately address the **interaction between the system components** and the **human–machine interaction**, especially in **assistive technologies used by children with severe disabilities**. Ensuring safety in such systems is critical to prevent injuries, wheelchair damage, or loss of mobility.

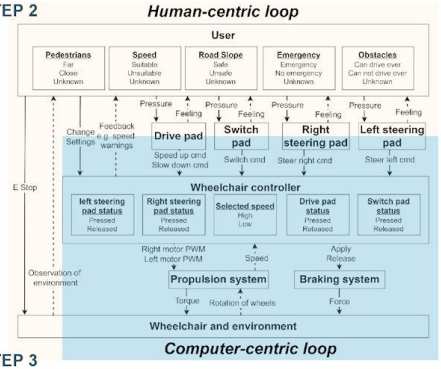
RESULTS

STEP 1

ID	Loss
L1	Loss of a human life or injury to people.
L2	Loss or damage to the wheelchair.
L3	Loss of mission (wheelchair becomes faulty and stops moving).

ID	Hazards	Link to losses
H1	Unintended acceleration or deceleration of the wheelchair.	[L1, L2].
H2	Wheelchair drives over other people's feet or bumps into other people.	[L1].
...	...	...

STEP 2



STEP 3

ID	Unsafe Control Action (UCA)	Link to hazards
UCA2.1	The wheelchair controller provides PWM cmd to drive when the Drive_Pad is released.	[H1, H2, H3]
...	...	...

STEP 4

UCA2.1	Class 1	Class 2	Class 3	Class 4
Example - Provide causing hazard	1. <The wheelchair controller> provides <PWM to drive> when <Drive_Pad is released>. 2. <The wheelchair controller> receives feedback (or other inputs) that indicates <Drive_Pad is released>.	1) Feedback received by <the wheelchair controller> does not adequately indicate <Drive_Pad is released>. 2) <Drive_Pad is released> is true	1) <The wheelchair controller> does not provide <PWM to drive> when <Drive_Pad is released> 2) <The wheelchair> receives <Drive cmd> when <Drive_Pad is released>.	1) <PWM to drive> is not received by <the wheelchair> when <Drive_Pad is released> 2) <Wheelchair> responds by <Driving>
Causal factors	-Physical fault within the wheelchair controller. -Algorithmic fault within the wheelchair controller. -...	-Weather conditions (e.g., rain, sun) causing the pad's sensor to generate a signal without being pressed. -...	-Physical fault in the propulsion system. -Communication delay. -...	-Using the wheelchair on a slippery road surface. -Physical failure of the braking system. -...

Transforming Formal Verification Insights from MALPAS

Formal methods use mathematical techniques to improve software reliability and safety in critical domains like nuclear, aerospace, and defence. Despite proven benefits, adoption remains limited due to complexity and skill gaps. While standards and regulations (e.g., IEC 60880, DO-178C) encourage their use, many emerging areas such as autonomous systems lag behind. The cost of poor software quality —$2.41 trillion in the US (2022)—underscores the need for robust verification.

MALPAS, a suite of static analysis tools, bridges theory and practice by providing rigorous code analysis for compliance and error detection. Planned enhancements aim to improve usability and efficiency, making formal verification more accessible and cost-effective across industries.

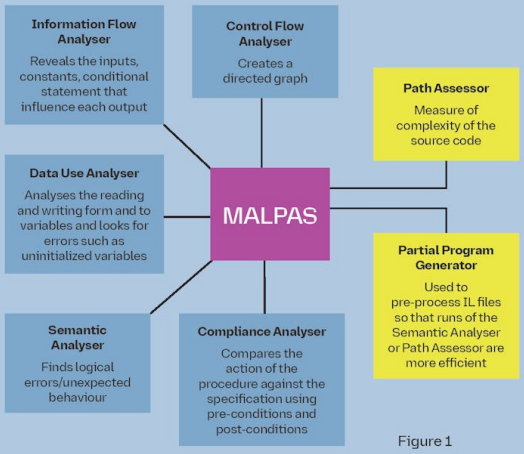


Figure 1

Old Programs vs New Programs

One could apply FMs to the new system specification and new code; however, whatever was in the old software program may be difficult to apply FMs to. If you had the source code of the old software program, some static analysis could possibly be applied, but if there isn't a specification, you would not be able to verify the code against the specification.

Formal Verification of the future

Automated Formal Methods Evolving from Model Based System Engineering is a key for future technology. Possible evolutions to make MALPAS more future proof include:

- Ensure it's developed in modern, fully supported languages.
- Enhance its features so it is easier to use and needs less intervention, making it more user-friendly.
- Consider human factors and human-system interaction to improve user-friendliness.
- Increase efficiency in run time.
- Open up MALPAS to other markets, such as defence, aerospace, cyber security, etc., in addition to supporting the nuclear sector.

MALPAS Past and Present

The MALPAS static analyser has demonstrated a strong track record across several large-scale projects, primarily within the defence and nuclear sectors. Notable applications include extensive nuclear reactor projects, smart devices, and flight control systems.

MALPAS' toolset is modular (shown in figure 1): one can analyse their code using the full suite of analysers or a subset, depending on the rigour required.
Because of its usage in ongoing nuclear programs MALPAS will still be relevant for the next 60 years and more, as it will need to be used to check the code for any updates and maintenance made to the Nuclear protection systems.

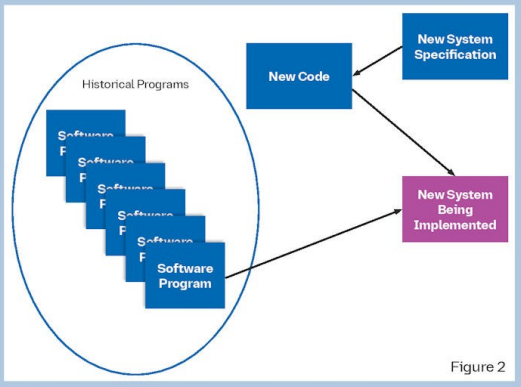


Figure 2

References

- Maurice H. ter Beek, R. C. (2024). Formal Methods in Industry. Association for Computing Machinery.
- WARD, N. J. (1989). The Static Analysis of Safety Critical Software Using MALPAS. IFAC SAFECOMP. Vienna, Austria.
- ter Beek, M. H. (2024). Formal Methods in Industry. Association for Computing Machinery.
- Wassyng, M. L. (2012). Formal verification of nuclear systems: Past, present, and future. 1st International Workshop on Critical Infrastructure Safety and Security, (pp. 43--51).

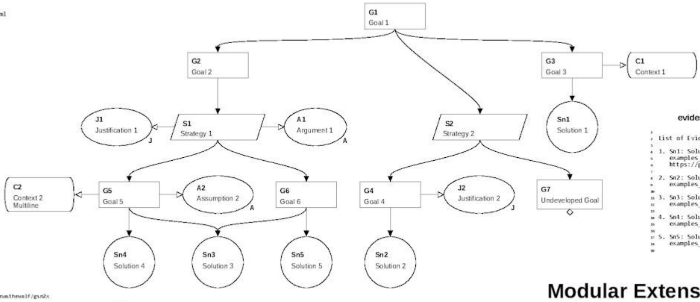
E-mail:
Lavinia.Burski@atkinsrealis.com

gsn2x

Goal Structuring Notation made easy

examples/example.gsn.yaml

```yaml
G1:
 text: Goal 1
 supportedBy: [G2, G3, S2]

G2:
 text: Goal 2
 supportedBy: [S1]

G4:
 text: Goal 4
 inContextOf: [J2]
 supportedBy: [Sn2]

G3:
 text: Goal 3
 supportedBy: [Sn1]
 inContextOf: [C1]

C1:
 text: Context 1

S1:
 text: Strategy 1
 supportedBy: [G5, G6]
 inContextOf: [A1, J1]

G5:
 text: Goal 5
 inContextOf: [C2, A2]
 supportedBy: [Sn3, Sn4]

C2:
 text: |
  Context 2
  Multiline

G6:
 text: Goal 6
 supportedBy: [Sn3, Sn5]

A1:
 text: Argument 1

Sn1:
 text: Solution 1
 url: https://github.com/jonasthewolf/gsn2x

Sn2:
 text: Solution 2
 layer1: Additional information on layer 1
 layer2: Additional information on layer 2

Sn3:
 text: Solution 3
 layer2: Additional information on layer 2

Sn4:
 text: Solution 4
 horizontalIndex:
  relative: -1

Sn5:
 text: Solution 5

J1:
 text: Justification 1

J2:
 text: Justification 2

A2:
 text: Assumption 2
 classes: [mycssclass, anotherclass]

S2:
 text: Strategy 2
 supportedBy: [G4, G7]
 rankIncrement: 1
 horizontalIndex:
  relative: -1

G7:
 text: Undeveloped Goal
 undeveloped: true
```



evidence.md

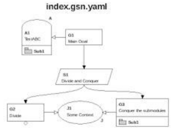
```
List of Evidence

1. Sn1: Solution 1
   examples_example_gsn_yaml
   https://github.com/jonasthewolf/gsn2x

2. Sn2: Solution 2
   examples_example_gsn_yaml

3. Sn3: Solution 3
   examples_example_gsn_yaml

4. Sn4: Solution 4
   examples_example_gsn_yaml

5. Sn5: Solution 5
   examples_example_gsn_yaml
```

Usage

```
gsn2x [OPTIONS] [INPUT]…

Arguments:
  [INPUT]...  Sets the input file(s) to use. [default: index.gsn.yaml]

Options:
   -h, --help     Print help
   -V, --version  Print version

CHECKS:
   -c, --check                        Only check the input file(s), but do not output graphs.
   -x, --exclude=<EXCLUDED_MODULE>    Exclude this module from reference checks.
       --warn-dialectic               Emit a warning if Dialectic Extension is used.
       --extended-check               Perform additional checks.

OUTPUT:
   -N, --no-arg                         Do not output of argument view for provided input files.
   -f, --full=<COMPLETE_VIEW>           Output the complete view to file with name <COMPLETE_VIEW>. [default: complete.svg]
   -F, --no-full                        Do not output the complete view.
   -a, --arch=<ARCHITECTURE_VIEW>       Output the architecture view to file with name <ARCHITECTURE_VIEW>. [default: architecture.svg]
   -A, --no-arch                        Do not output the architecture view.
   -e, --evidence=<EVIDENCE>            Output list of all evidence to file with name <EVIDENCE>. [default: evidence.md]
   -E, --no-evidence                    Do not output list of all evidence.
   -o, --output-dir=<OUTPUT_DIRECTORY>  Emit all output files to directory <OUTPUT_DIRECTORY>. [default: .]
       --statistics[=<STATISTICS>]      Output statistics on inputs to <STATISTICS> file or standard output.
       --dump-yaml[=<YAMLDUMP>]         Output parsed YAML files to single <YAMLDUMP> file or standard output.

OUTPUT MODIFICATION:
   -l, --layer=<LAYERS>              Output additional layer. Can be used multiple times.
   -s, --stylesheet=<STYLESHEETS>    Links a stylesheet in SVG output. Can be used multiple times.
   -t, --embed-css                   Embed stylesheets instead of linking them.
   -G, --no-legend                   Do not output a legend based on module information.
   -g, --full-legend                 Output a legend based on all module information.
   -w, --wrap=<CHAR_WRAP>            Define the number of characters after which a line of text is wrapped.
```

Modular Extension

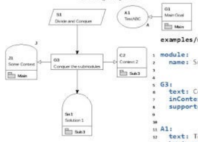
index.gsn.yaml



examples/modular/index.gsn.yaml

```yaml
module:
  name: Main
  uses: [sub1.gsn.yaml, sub3.gsn.yaml]

G1:
  text: Main Goal
  supportedBy: [S1]
  inContextOf: [A1]
  horizontalIndex:
    absolute: last

S1:
  text: Divide and Conquer
  supportedBy: [G2, G3]

G2:
  text: Divide
  inContextOf: [J1]
  undeveloped: true

J1:
  text: Some Context
```

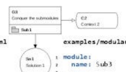
sub1.gsn.yaml



examples/modular/sub1.gsn.yaml

```yaml
module:
  name: Sub1


G3:
  text: Conquer the submodules
  inContextOf: [J1, C2]
  supportedBy: [Sn1]


A1:
  text: TestABC
  horizontalIndex:
     absolute: 0
```

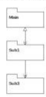
sub3.gsn.yaml



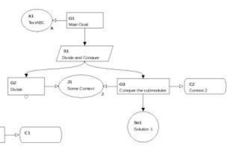
examples/modular/sub3.gsn.yaml

```yaml
module:
  name: Sub3

C2:
  text: Context 2

Sn1:
  text: Solution 1
```

Architecture View



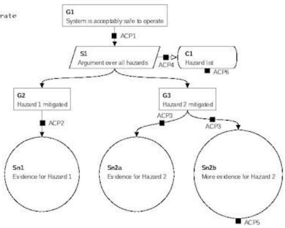
Complete Argument View



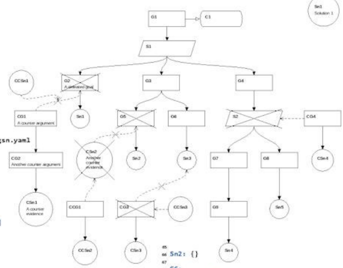
Confidence Argument Extension

examples/modular/index.gsn.yaml

```yaml
G1:
  text: System is acceptably safe to operate
  supportedBy: [S1]
  acp:
    ACP1: S1

S1:
  text: Argument over all hazards
  supportedBy: [G2, G3]
  inContextOf: [C1]
  acp:
    ACP4: C1

C1:
  text: Hazard list
  acp:
    ACP6: C1

G2:
  text: Hazard 1 mitigated
  supportedBy: [Sn1]
  acp:
    ACP2: Sn1

Sn1:
  text: Evidence for Hazard 1

G3:
  text: Hazard 2 mitigated
  supportedBy: [Sn2a, Sn2b]
  acp:
    ACP3: [Sn2a, Sn2b]

Sn2a:
  text: Evidence for Hazard 2

Sn2b:
  text: More evidence for Hazard 2
  acp:
    ACP5: Sn2b
```

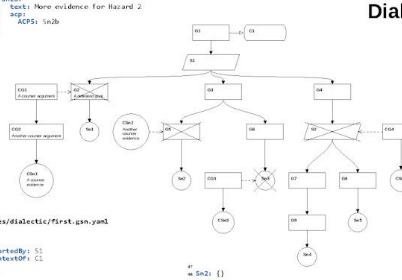


Dialectic Extension



examples/dialectic/second.gsn.yaml

```yaml
G1:
  supportedBy: S1
  inContextOf: C1

C1: {}

S1:
  supportedBy: [G2, G3, G4]

G2:
  text: A defeated goal
  supportedBy: Sn1
  defeated: true

Sn1: {}

CG1:
  text: A counter argument
  supportedBy: CG2
  challenges: G2
  defeatedRelation: G2
  horizontalIndex:
    relative: -1
  rankIncrement: 1

CCSn1:
  nodeType: CounterSolution
  challenges: G2 -> CG1

CG2:
  text: Another counter argument
  supportedBy: CSn1

CSn1:
  text: |
     A counter
     evidence

G3:
  supportedBy: [G5, G6]

CSn2:
  Text: |
     Another
     counter
     evidence
  challenges: G5
  defeated: true
  defeatedRelation: G5
  RankIncrement: 1

CCG1:
  nodeType: CounterGoal
  supportedBy: CCSn2
  challenges: CSn2
  rankIncrement: 1

CCSn2:
  nodeType: CounterSolution

G5:
  supportedBy: Sn2
  defeated: true

Sn2: {}

G6:
  supportedBy: Sn3

Sn3: {}

CG3:
  challenges: Sn3
  supportedBy: CSn3
  defeated: true
  defeatedRelation: Sn3
  rankIncrement: 1

CSn3: {}

G4:
  supportedBy: [S2]

S2:
  supportedBy: [G7, G8]
  defeated: true

G7:
  supportedBy: G9

G9:
  supportedBy: Sn4

Sn4: {}

G8:
  supportedBy: Sn5

Sn5: {}

CG4:
  challenges: S2
  supportedBy: CSn4
  horizontalIndex:
    absolute: last

CSn4: {}

CCSn3:
  nodeType: CounterSolution
  challenges: CG3
  horizontalIndex:
    relative: +1
```



examples/dialectic/first.gsn.yaml

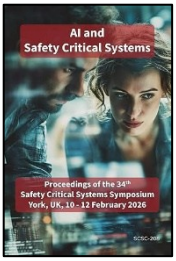
```yaml
G1:
  supportedBy: S1
  inContextOf: C1

C1: {}

S1:
  supportedBy: [G2, G3, G4]

G2:
  text: A defeated goal
  supportedBy: Sn1
  defeated: true

Sn1: {}

CG1:
  text: A counter argument
  supportedBy: CG2
  challenges: G2
  horizontalIndex:
    relative: -1

CG2:
  text: Another counter argument
  supportedBy: CSn1

CSn1:
  text: |
     A counter
     evidence

G3:
  supportedBy: [G5, G6]

CSn2:
  Text: |
     Another
     counter
     evidence
  challenges: G5

G5:
  supportedBy: Sn2
  defeated: true

Sn2: {}

G6:
  supportedBy: Sn3

Sn3:
  defeated: true

CG3:
  challenges: Sn3
  supportedBy: CSn3

CSn3: {}

G4:
  supportedBy: [S2]

S2:
  supportedBy: [G7, G8]
  defeated: true

G7:
  supportedBy: G9

G9:
  supportedBy: Sn4

Sn4: {}

G8:
  supportedBy: Sn5

Sn5: {}

CG4:
  challenges: S2
  supportedBy: CSn4
  horizontalIndex:
    absolute: last

CSn4: {}
```

Element Type	Prefix
Goal	G
Assumption	A
Justification	J
Solution	Sn
Context	C
Strategy	S
Counter Goal	CG
Counter Solution	CSn

Get it on github:
https://github.com/jonasthewolf/gsn2x
MIT License

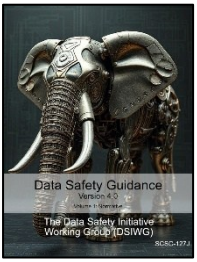
gsn2x

Recent Safety Publications

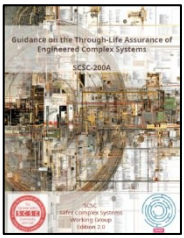


Proceedings of the 34th Safety-Critical Systems Symposium
scsc.uk/scsc-208

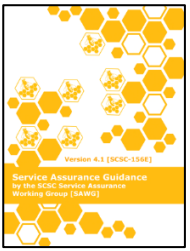
Safety-Critical Systems eJournal vol.4 no.2
Winter Issue 2025
scsc.uk/scsc-210



Safety-Critical Systems Data Safety Guidance v4.0
Parts 1, 2 and 3
scsc.uk/scsc-127K



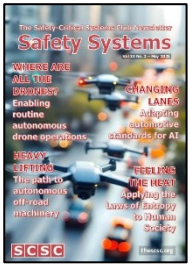
Guidance on the Through-Life Assurance of Engineered Complex Systems v2.0
scsc.uk/scsc-200A



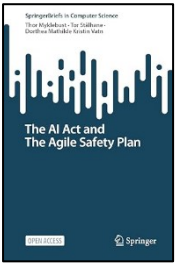
Service Assurance Guidance v4.1
scsc.uk/scsc-156E

The Safety-Critical Systems Club Newsletter, Volume 33, Number 3
scsc.uk/scsc-206

Safety-Critical Systems eJournal vol.4 no.1
Spring Issue 2025
scsc.uk/scsc-204



The Safety-Critical Systems Club Newsletter, Volume 33, Number 2
scsc.uk/scsc-205



The AI Act and
The Agile Safety Plan
amazon.co.uk/dp/3031805038

60 Seconds with ... Mikela Chatzimichailidou

Mikela is a Professor at University College London (UCL); a leading researcher of all things technical and a consulting engineer bringing together experience and expertise from across healthcare, transportation and infrastructure in the fields of systems engineering and integration, safety assurance, complexity management, product design and innovation.

She has been leading research and consulting assignments for more than a decade both in academia for some of the world's top universities, and in industry for world-class built environment consultancies.

During her career she has worked in both hands-on R&D roles, consultancy and design roles and as a project and engineering manager, leading others to deliver client objectives and cutting edge academic research. Mikela therefore brings experience of both the academic and industrial worlds, bridging the gap and drawing the best from each.

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

I've always been fascinated by people; how we make decisions, take risks, and interact with one another. System Safety offered me the chance to help people on a larger scale, to understand human behaviour in complex environments, and to make systems safer not just technically, but for the humans who rely on them every day.

What aspect of your career are you most proud of?

I'm proud of working at the crossroads of academia, industry, and policy. It's where research meets practice, and where insights turn into action that genuinely protects people. Being able to bridge these worlds and see ideas make a tangible difference is incredibly rewarding.

Tell us one interesting unusual fact about yourself!

When I was five, someone asked me what I wanted to be when I grew up, and I said "Prime Minister." Even though I didn't take that exact path, it reflects a mindset I've carried ever since: aim high, dream boldly, and don't shy away from challenges that seem bigger than you. That was back in the early 90s – not sure how well our politicians do today...

What advice would you give to yourself age 12?

I'd tell my younger self: never stop dreaming. Focus on the bigger picture, not just what's right in front of you. Being a dreamer isn't naïve, it's essential. The key to a fulfilling career is holding onto your curiosity, imagination, and willingness to pursue what may seem impossible.

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

We need to embrace change and complexity rather than resist it. Complexity isn't the enemy, it's the world we live in. The challenge is to navigate it thoughtfully, adapt quickly, and find ways to work with systems rather than against them. That mindset is no longer optional; it's essential for shaping a safer future.

What's your most favourite quote or motto?

"*Insanity is doing the same thing over and over again and expecting different results.*" (A. Einstein) It's a reminder to keep questioning, try new approaches, and never settle for doing things just because *"that's how they've always been done"."*

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

I'd study forensics. I've always been fascinated by puzzles, mysteries, and uncovering how events unfold or why accidents happen. There's a strong connection to safety: understanding human behaviours helps us prevent risks or encourage good practices, and the detective mindset sharpens your ability to spot patterns and connections that others might overlook.

"The key to a fulfilling career is holding onto your curiosity, imagination, and willingness to pursue what may seem impossible"

If you could be any fictional character, whom would you choose?

Popeye for his determination, resilience, and unshakable optimism. There's something inspiring about a character who faces challenges head-on, never gives up, and still finds joy along the way. A little spinach-powered optimism never hurts!

How do you see the rise of Artificial Intelligence affecting the future of safety engineering?

AI is just the latest in a long line of disruptive technologies. The question isn't whether AI will change our work – it will – but whether we remain critical thinkers, creators of value, and socially responsible engineers. We do, as long as we resist shortcuts, use AI thoughtfully, and remember that insight and judgement still comes from people, not algorithms.

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


Security Informed Safety


Assurance Cases


Service Assurance


AI / Autonomous Systems


Data Safety Initiative


Safer Complex Systems


Multicore


Safe System Architecting


Safety Culture


Ontology


Safety Futures Initiative


Systems Approach to Safety of the Environment


Safety Management & Safety Management Systems

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.

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.

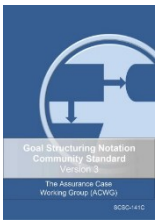
Last year, the working group published its first piece of guidance: Co-Assurance of Safety and Security.

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

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



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. This includes a library scsc.uk/library of relevant papers previously published by Tim Kelly, which are now hosted on the SCSC website.

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

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

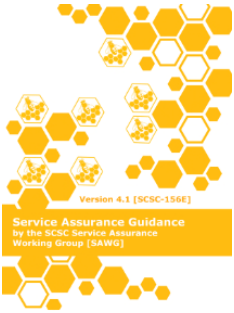
Lead **Jane Fenn** jane.fenn@baesystems.com with support from **Phil Williams** phil.williams@scsc.uk

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 is working on an update to the guidance v4.1 hopefully to be published in 2026.

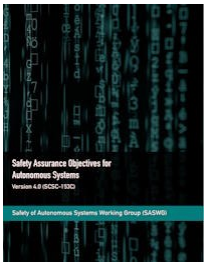


Lead **Kevin King** kevin.king@baesystems.com

Safety of AI / Autonomous Systems

It is clear that AI and 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 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.

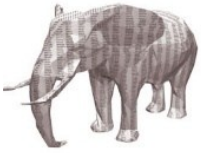


The working group was kicked-off at SSS'24 and is led by Alan Simpson. The SAIWG will conduct regular meetings, workshops, and publications to share knowledge and experience on various topics related to AI and safety systems, such as coordination of safety with other disciplines, evaluation of risk,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

The group builds on the earlier work of the Safety of Autonomous Systems Working Group (SASWG) that culminated in production of the 4th version of its guidance: Safety Assurance Objectives for Autonomous Systems, in Feb 2024 scsc.uk/scsc-153C

Lead Alan Simpson alan.simpson@ebeni.com

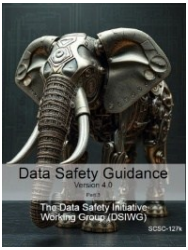
Data Safety Initiative



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.



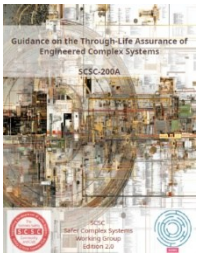
An update to the guidance (v4.0) was published in Jan 2026: scsc.uk/scsc-127K This was a major release for the guidance and saw the original document reorganised into three separate parts that can be upissued independently.

Lead Mike Parsons mike.parsons@scsc.uk

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 problem statement:

- 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

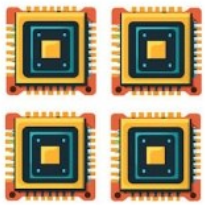


The group produced the second edition of Guidance on the Through-Life Assurance of Engineered Complex Systems (scsc.uk/scsc-200A) in January 2026. Note that the title now includes the word "Engineered" to be specific about the types of system in scope.

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

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

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

Safe System Architecting

The SCSC Safe 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.

The working group meets 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.

Co-chairs: Siyuan Ji s.ji@lboro.ac.uk and **Jane Fenn** jane.fenn@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. scsc.uk/r2995

A seminar was held 19th June 2025 in London and focussed on how Safety Culture practices need to change to accommodate Artificial Intelligence. SCSC members can access the seminar presentations and videos here: scsc.uk/e1156

Lead Anne Seldon anne.seldon@wae.com

Ontology

The Ontology Working Group (OWG) develops ontologies that will form the basis of SCSC guidance, as well as having wider industrial and academic applications.

During system development, and especially with Model-Based Systems Engineering (MBSE), it is essential to build a model of the world that the system will inhabit, and this involves developing and structuring concepts, terms and their relationships. An ontology is an explicit specification of such a conceptualization and provides the foundation for MBSE and architectural descriptions in general. Ontologies are also increasingly important, if not essential, for explainable Artificial Intelligence (AI), enterprise knowledge systems and the standards that underpin them.

The OWG is currently working on the definition of an ontology of risk and value for application in guidance for risk-based decision making – notably safety and security. The framework for modelling is the Unified Foundation Ontology (UFO) and OntoUML, a domain-specific language (DSL) for modelling in UML tailored for ontological modelling based on UFO.

The OWG has also embarked on a series of SCSC Newsletter articles to gently explain ontological concepts and notations. The aim is to provide an accessible introduction to the domain so readers can be more informed and to help demystify a topic that may have a perception of being quite academic. The third article in the series can be found in this edition.

Lead **Dave Banham** ontology@scsc.uk

The Safety Futures Initiative

The Safety Futures working group meets once a month to bring together fresh perspectives, innovative ideas and insights.

The Safety Futures is diligently working on developing a comprehensive roadmap to guide new safety professionals in exploring career paths across various industries. To supplement this, they have an upcoming initiative to create a University 'League' Table to rank universities based on their safety engineering courses and the career pathways they support.

They are also looking to start a reverse mentoring programme where we can match more experienced people with new professionals for information exchange.

The group encourages anyone to get involved to help shape the future of safety engineering careers.

Lead **Giles Howard** giles.howard@scsc.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

Safety Management and Safety Management Systems

This new working group aiming to cover Safety Management and also Safety Management Systems (SMSWG) is now in full swing with almost 60 members.

Safety Management can be a difficult challenge with many different stakeholders with their own objectives pulling in different directions, perhaps one might draw parallels with the equally challenging task of herding cats! This analogy has given rise to the group's icon as shown.

Being an effective Safety Manager requires a balance of technical knowledge, regulatory understanding, soft skills, and leadership. Yet many are asked to lead safety without prior experience or clear support. This group will explore challenges such as overcoming organisational resistance, gaining senior buy-in, building trust across the workforce, and creating a positive safety culture where reporting is safe and encouraged. The group will also explore regulatory frameworks, going beyond compliance to fully understand the intent behind the rules.

The group is led by Si Hays so get in touch with him if you want to find out more about the group.

Lead **Si Hays** si.hays@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 and access to papers presentations and other resources from events.

See scsc.uk/membership for more details.

	Public	Registered	Individual	Corporate
Access to the SCSC Newsletter	✓	✓	✓	✓
Access to the E-Journal	✓	✓	✓	✓
Receive monthly e-flyer	×	✓	✓	✓
Attend SCSC 1-day Seminars	×	×	✓	✓
Attend the annual Symposium	×	×	✓	✓
Access to Proceedings of the Symposium	×	×	✓	✓
Participate in SCSC Working Groups	×	×	✓	✓
Access to publications	×	×	✓	✓
Access to video recordings and presentations	×	×	✓	✓
Reduced membership costs	×	×	×	✓
Free full-page spread in SCSC Newsletter	×	×	×	✓
New members announced on website	×	×	×	✓
Share promotional material at 1-day events	×	×	×	✓
Sponsored content in SCSC monthly e-flyer	×	×	×	✓
Company logo on footer of SCSC website	×	×	×	✓

Individual Membership

Individual Membership is essential for engaging with the SCSC, and in particular, attending Seminars, Symposia and other events run by the club. It also gives access to over three decades of papers and presentations from some of the leading experts in system safety.

To become an individual member of the SCSC please register on the SCSC website using the Home->Register menu option. Complete and save your account registration and then verify your email address. Once registered and logged in, select the Membership menu option and pick the membership package you would like to sign up for.

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

Corporate membership affords all the benefits of individual members at discounted rates, plus some other great benefits for promoting your company. These are:

- A free full-page spread in the SCSC Newsletter, which goes out to thousands of system safety practitioners worldwide
- The ability to share promotional material at SCSC 1-day Seminars
- Sponsored content in the SCSC's monthly e-Flyer that goes to everyone registered on the SCSC website
- Your company's logo on the footer of the SCSC website

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 2026 for new and renewing members:

- 1 year Individual Membership: £159
- 2 year Membership: 7% discount: £295
- 3 year Membership: 17% discount: £395
- 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

Contact Alex King using office@scsc.uk

The SCSC Steering Group

Current Members


Stephen Bull
stephen.bull@scsc.uk


Carmen Carlan
carmen.carlan@scsc.uk


Dewi Daniels
dewi.daniels@scsc.uk


Dai Davis
dai.davis@scsc.uk


Jane Fenn
jane.fenn@scsc.uk


Paul Hampton
paul.hampton@scsc.uk


Giles Howard
giles.howard@scsc.uk


James Inge
james.inge@scsc.uk


Brian Jepson
brian.jepson@scsc.uk


Graham Jolliffe
graham.jolliffe@scsc.uk


Alex King
alex.king@scsc.uk


Kate McDougall
kate.mcdougall@scsc.uk


Mark Nicholson
mark.nicholson@scsc.uk


Yvonne Oakshott
yvonne.oakshott@scsc.uk


Wendy Owen
wendy.owen@scsc.uk


Mike Parsons
mike.parsons@scsc.uk


Davy Pissoort
davy.pissoort@scsc.uk


Rudi Redford-Brown
rudi.redford-brown@scsc.uk


Karin Rudolph
karin.rudolph@scsc.uk


John Spriggs
john.spriggs@scsc.uk

Note that honorary SCSC membership has replaced honorary Steering Group membership.

Club Positions

The current holders of club positions are as follows:

Managing Director

Mike Parsons 2019-

Steering Group Chair

Dewi Daniels 2024-

Programme & Events Coordinator

Mike Parsons 2014-

Manager

Alex King 2019-

Newsletter Editor

Paul Hampton 2019-

University of York Coordinator

Mark Nicholson 2019-

Honorary Solicitor

Dai Davis 2022-

Website Editor

Paul Hampton 2025-

eJournal Editor

John Spriggs 2021-

Administrator

Alex King 2016-

Diversity, Equity and Inclusion (DE&I) Lead

TBC

Safety Futures Initiative Leads

Giles Howard 2025-

Calendar

May '26

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 '26

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 '26

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 '26

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 '26

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				

October '26

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 '26

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 '26

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			

January '27

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 '27

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 '27

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				

April '27

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

14 May 2026
Working Group Meeting
DSIWG #106

Online

scsc.uk/events-diary/working-groups/dsiwg-98

19 May 2026
Working Group Meeting
OWG #106

Online

scsc.uk/events-diary/working-groups/owg-106

19 May 2026
Working Group Meeting
SCSWG

Online

scsc.uk/events-diary/working-groups/scswg

25 Jun 2026
SCSC Seminar
How to Make the Most of AI: A Workshop for Safety Engineers

Hilton London Euston, UK

scsc.uk/e5101

22-25 Sep 2026
Conference
The 45th International Conference on Computer Safety, Reliability and Security (SafeComp 2026)

Universitat Politècnica de València (UPV), Spain

www.his-conference.co.uk

23-24 Sep 2026
Convention
Centre for Humanistic Ethics in Risk Management Scandinavia (CHERMS)
Towards Human-Centred Organising

Svendborg, Denmark

novellus.solutions/mec-events/cherms26

18-20 Nov 2026
Course
Accident investigation program

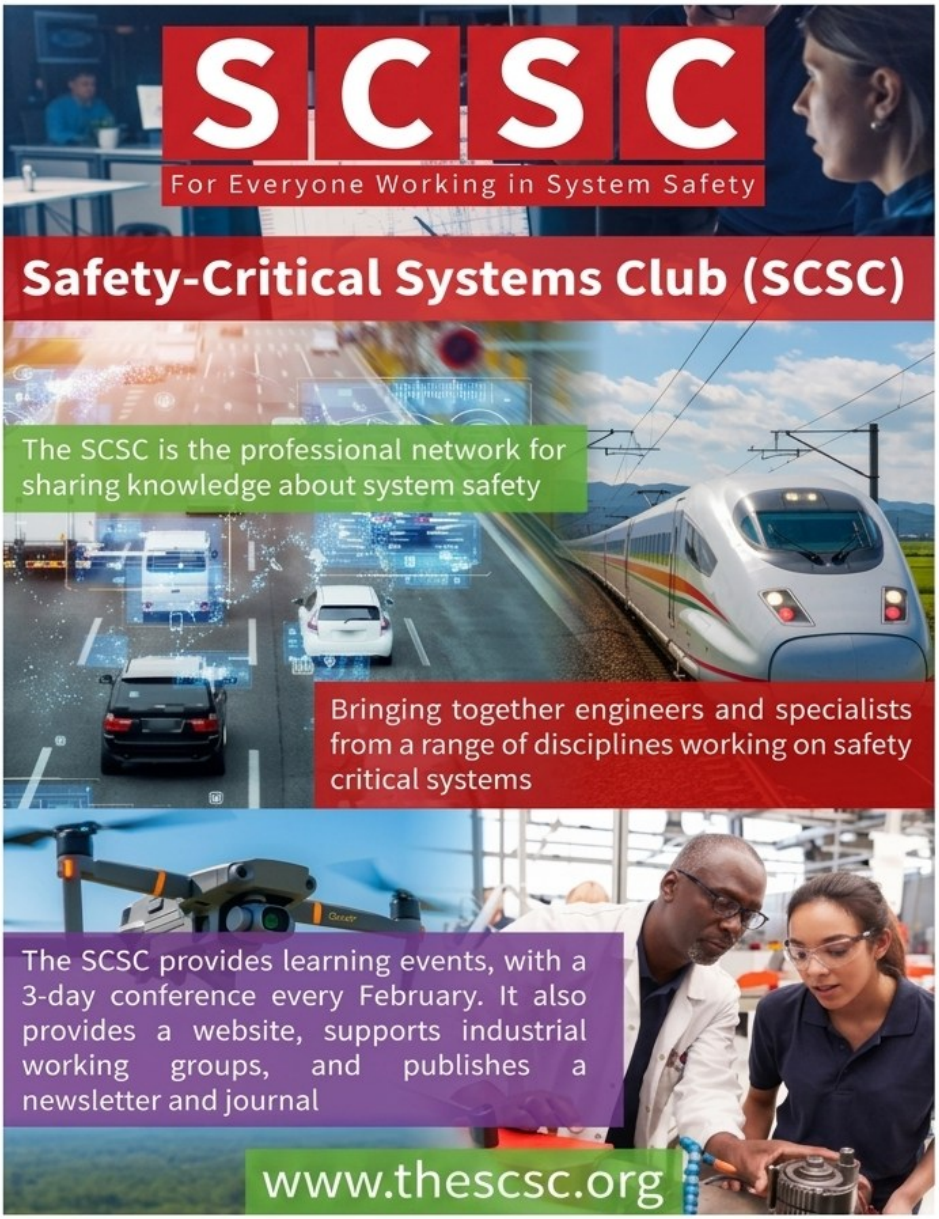
Heathrow Marriot Hotel, London, UK.

novellus.solutions/mec-events/accidentinvestigationlondon-459

9-11 Feb 2027
SCSC Symposium
Safety Critical Systems Symposium SSS'27

Harbour Hotel, Bristol, UK

scsc.uk/sss'27



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