The Safety-Critical Systems Club Newsletter

Safety Systems

Vol 33 No. 2 – May 2025

WHERE ARE ALL THE DRONES?
Enabling routine autonomous drone operations

CHANGING LANES
Adapting automotive standards for AI

HEAVY LIFTING
The path to autonomous off-road machinery

FEELING THE HEAT
Applying the Laws of Entropy to Human Society

SCSC

thescsc.org

SCSC Publication Number: SCSC-205

Front cover: Midjourney AI art adapted
In Brief images may be subject to copyright – contact the SCSC Newsletter Editor for details.

Contents


SCSC
For Everyone Working in System Safety
34th Safety-Critical Systems Symposium
10-12th February 2026
The Milner York, York, UK
SSS'26 Call for Abstracts
www.scsc.uk/sss

Editorial

Welcome to the May 2025 edition of Safety Systems!

A car I hired recently on a trip to Scotland came with Adaptive Cruise Control (ACC). I've driven with this feature before, but this vehicle went a step further by being able to read the speed signs and change the target speed accordingly while of course, slowing down if a vehicle was detected ahead. Entire journeys could be undertaken with steering alone; it really almost did 'drive itself'. There was certainly clear utility and in stop-start traffic liable to slow down unexpectedly, it added an element of safety especially with a tired driver at the wheel; it therefore certainly mitigates traditional hazards. My foot, however, always hovered warily near the brake pedal throughout – could I really *trust* this system? As a safety engineer, I am possibly more risk averse than most! Perhaps after months or years without mishap, that trust will increase and I may become complacent and so new and novel hazards will emerge. I wonder whether manufacturers could be more explicit in their reliability claims to help consumers judge, so a warning sign when you switch on ACC – perhaps a reliability percentage or number of likely journeys before a mishap. Certainly it should probably already state not to fully rely on the system. Perhaps our article in this edition on and how automotive standards can change to adapt to our emerging autonomous world will give some insight. Along this with we have a wide variety of articles from global considerations of the impact of the laws of thermodynamics on human societies, to drones and autonomous off-road machinery.

In February this year, the SCSC hosted another great Symposium in York with the event's twin themes being Artificial Intelligence (AI) and complexity & interconnectedness. There was a packed programme and a number of great new features such as workshop streams, new technical entertainment and 'armchair chats'! You can read my report of the event on page 31 and Wendy Owen reports on one of the workshops she led covering Change Management on page 41.

In May we held a fascinating seminar on Safe Agile Developments. I'll provide a report of this event in the next edition but we have some really great seminars coming up. Firstly, in London on 19th June we have "How Safety Culture has to Change With AI" (scsc.uk/e1156). After a hugely successful event last year on mainland Europe we are now also holding two further events: one in Brussels, Belgium covering compliance with the EU AI Act (scsc.uk/e5003) on the 9th October and we return to Munich, Germany on 4th December to cover new developments in Rail System Safety (scsc.uk/e5004). See the flyers in this newsletter or the SCSC website for further details of these events.

Talking of the SCSC website, if you've visited it recently, you'll see that we've now revamped the site significantly. The site still has all the previous great content but adds some new features to make the user experience even better. See page 47 for my brief introduction to the site and please try the site and feedback is more than welcome!

Our 60 second interview is with Graham Jolliffe. Graham will be known to many of us through his long career in the industry, much of which he covered in an entertaining after dinner speech as SSS'25. Find out what retired life is like for him on page 62!

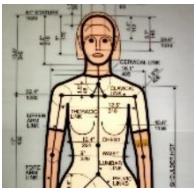
Paul Hampton
SCSC Newsletter Editor
paul.hampton@scsc.uk

In Brief






Cars aren't tested properly for women's safety



Women are 73% more likely to be seriously injured in a head-on car crash compared with men in the same crash. Female drivers and front-seat passengers are 17% more likely to be killed in a car crash than a male occupant of the same age, according to multiple studies conducted over the last five years.

The "She DRIVES Act" intends to raise the standards for car safety testing, promoting the use of "crash test dummies that reflect a woman's lighter frame" *nbcnews.com*

Ministry of Justice to Question the Presumption that 'the computer is always right'

Current principles on the use of evidence generated by computer software in criminal proceedings in simple terms state that, 'the computer is always right', unless someone can show it is not.

The government is now welcoming the views of all those with an interest in this area to provide insights to help ensure the criminal justice system is fair and effective, both now, and for years to come. *gov.uk*

The SCSC has provided a submission to this consultation here: scsc.uk/file/sg/SCSC Submission Call for Evidence.pdf

Six people killed after helicopter crashes into Hudson River in New York

A helicopter crashed into the Hudson River in New York on 10th April 2025, killing all six people onboard, including the pilot and a family of Spanish tourists with three children. The sightseeing helicopter broke apart in midair and crashed upside down into the Hudson River. *theguardian.com*

Disaster happened in 'world's most controlled airspace'

A US Army Black Hawk helicopter with a crew of three collided with an American Airlines jet carrying 64 people seconds before the passenger aircraft was due to land at Washington National airport in what is described as "the most controlled bit of airspace in the world". *bbc.co.uk*

All passengers survive crash landing as plane flips at Toronto airport

All 80 people on board a plane which crashed and overturned while landing in Toronto have survived, officials said.

The Delta Air Lines flight from Minneapolis skidded along the runway with flames visible and it came to a halt upside down as firefighters came to the rescue. *bbc.co.uk*

On-Board Safety Monitoring for Drones

Nick Tudor discusses some of the issues which have to be resolved before we see routine on-demand, commercially viable fully autonomous drone operations in our skies. He provides an overview of the regulations, their current means of compliance, and proposes an approach to help unblock the technical challenges being experienced in the industry.

There are a number of reasons why Unmanned Air Systems (UAS), Unmanned Air Vehicles (UAVs), Remotely Piloted Air Systems (RPAS), or 'drones', have yet to really deliver the vision of autonomous flight. Apart from the multiple labels for the same thing[1] , these range from legal and technological to regulatory and there have been numerous false starts. This paper will describe and touch on some of the issues which have to be resolved in order to enable on-demand, commercially viable fully autonomous operations. The focus of this article, however, is on a proposed approach to the resolution of some of the technological issues that could then lead to changes in the law that, in turn, might enable a change in regulatory policy and possibly affect insurance premiums for drone operations.

The Three Questions

While many in the autonomous systems world focus on capabilities, when it comes to engineering a solution (and from a regulatory perspective) showing what it does is only one part of the three-question set that have to be satisfactorily answered.

[1] Some might say that a UAV is only the aircraft, some might say that there has to be a 'pilot' and hence RPAS, some might say that there has to be a ground station and hence UAS; they're all correct to a greater or lesser degree, so it's not really a useful difference except perhaps in perception by different groups of people.

The questions are:

- What will it do?
- Can we give assurance that it won't do the things we don't want it to do?
- Can we describe what happens, when [not 'if'] things go wrong?

Largely it is accepted that developers can do the functions that they claim, otherwise they wouldn't be in the business in the first place. It is therefore relatively easy to answer the first question: what does it do? Most developers, however, do not focus on the other two questions. While current systems require a human to supervise autonomous operations, a human operator is limited in what they can do by the design of the vehicle, its ground system and the specifics of the environment in which the actual task is being conducted.

International Civil Aviation Organization (ICAO)

Role

Internationally, the driving agency for regulations is the International Civil Aviation Organization (ICAO). It is a United Nations specialised agency set up originally as a result of the Convention on International Civil Aviation (also known as Chicago Convention), that was signed on 7 December 1944 by 52 States.

While it is implicitly part of the ICAO Business Plan 23-25, there is only one specific mention of unmanned aircraft and that is in the message from the Secretary General. However, there is an annual ICAO Remotely Piloted Aircraft Systems Symposium/Drone Enable Symposium that seek to understand the latest developments and thinking in uncrewed aviation. There is also an ICAO RPAS Panel (RPASP), which includes representatives from the UK.

Safety

Managing and improving the safety of the global air transport system is ICAO's guiding and most fundamental Strategic Objective. One of the major initiatives of ICAO is the 'No Country Left Behind' initiative. This is to try to assist member States with implementation of globally harmonized, safe practices; this will apply to autonomous systems. Within aerospace, safety can largely be split into two broad topic areas: the airspace and the aircraft.

Airspace

Views on what the future holds vary significantly. Some think there will only be a small increase in the amount of air traffic by the introduction of uncrewed vehicles, restricted to niche use cases in remote areas. Others, however, think there will be a massive increase, including over dense population centres.

In remote areas, even with small numbers, there are significant impacts on existing air users and, particularly if there is a larger increase in numbers, the fundamental principles of Air Traffic Management (ATM) are being challenged. This is why there are significant initiatives on Unmanned Traffic Management (UTM). The thinking is that UAS are different and have to be treated differently, but they still have to be integrated into existing ATM as other air users need to be aware and be able to react to advice and direction from ground-based services – as well as using information from other aircraft, such as conspicuity devices. Simply segregating airspace for the sole use of UAS is not tenable in the medium term but is currently the only accepted approach for trials.

'Ground Control to Major Tom'[2]

While there are grand proposals, plans and in some cases, actual trials for lots of likely very expensive ground-based systems that purport to provide the safety backstop for the aircraft, ultimately, the decision for what the aircraft will actually do must reside with the aircraft. When, (not 'if') the communications fail, there is not a lot a now 'not-in-control' controller can do. They may be able to alert the authorities to the possibility of a vehicle being out of that person's control, but where it will be and what it's going to do is entirely in the gift of the aircraft; Major Tom is off on his own!

"When, (not 'if') the communications fail, there is not a lot a now 'not-in-control' controller can do"

Airworthiness of Aircraft

Developed by ICAO are the Standards and Recommended Practices (SARPS) contained in the nineteen Technical Annexes to the Convention on International Civil Aviation are applied universally and produce a high degree of technical uniformity.

Airworthiness

Airworthiness is the measure of an aircraft's suitability for safe flight. Certification of airworthiness is initially conferred by a certificate of airworthiness from a national aviation authority, and is maintained by performing the required maintenance actions. The application of airworthiness defines the condition of an aircraft and supplies the basis for judgment of the suitability for flight of that aircraft, in that it has been designed with engineering rigour, constructed, maintained and is expected to be operated to approved standards and limitations, by competent and approved individuals, who are acting as members of an approved organisation and whose work is both certified as correct and accepted on behalf of the State.

It is for each State to ensure that their aircraft have a certificate of airworthiness and that these certificates are recognised as valid by other states. For large aircraft (such as an Airbus or Boeing), within Europe there is Certification Specification 25 and similar documents have been developed for helicopters, smaller aircraft, gliders, etc, but until recently, there has been no guidance on and no equivalent for UAS; with Europe there now is JARUS CS-LUAS and EASA CS-LUAS.

Acceptable Loss

Flying aircraft presents a number of hazards which, through the design process of the aircraft, are expected to be mitigated in some way. There is a limit to what can be achieved to design, build and maintain an aircraft, so the approach is based upon the probability of a failure and the impact of that failure on the ability of the aircraft to continue to be operated. Loss of an aircraft/life is a defined as 'Catastrophic' and per aircraft Type (eg Airbus A320); this has been agreed to be $1x10^{-6}$, or one in a million flying hours as the overall hull loss

[2] This reference is to a David Bowie's 1969 song "Space Oddity". The lyrics tell the story of an astronaut named Major Tom who is informed by Ground Control that a malfunction has occurred in his spacecraft; but the astronaut does not get the message.

accident rate for an individual aircraft. An aircraft is built from various equipment, systems and installations and all are assessed to determine their contribution to safety. Figure 1 is a diagram that outlines the probability vs severity of failure principle of aircraft components and is used as part of the design process in order to mitigate hazards.

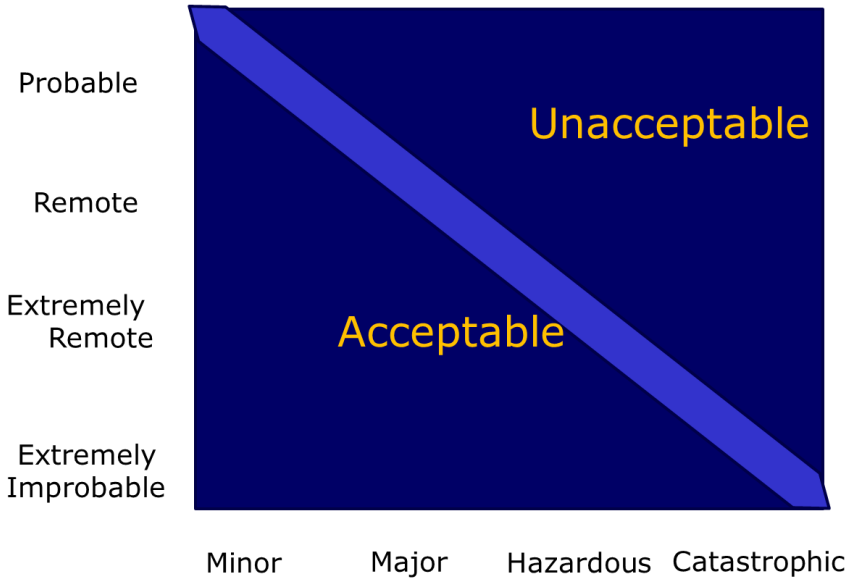


Figure 1 - Probability vs Severity

This is encapsulated in CS-25.1309 where not only must all components perform their intended functions in foreseeable operating conditions, but also that:

"The aeroplane systems and associated components, considered separately and in relation to other systems, must be designed so that -

(1) Any **catastrophic** failure condition

(i) is **extremely improbable**; and

(ii) does not result from a single failure; and

(2) Any **hazardous** failure condition is **extremely remote**; and

(3) Any **major** failure condition is **remote**.

Information concerning unsafe system operating conditions must be provided to the crew to enable them to take appropriate corrective action."

Extremely Improbable Failure Conditions for systems are those having an Average Probability Per Flight Hour of the order of $1x10^{-9}$ or less[3].

[3] This is the contribution per failure condition to the overall aircraft loss rate. More details on how this is calculated can be found at AMC 25.1309.

European Union Aviation Safey Agency (EASA) has issued Special Condition RPAS.1309 [1], which applies to any RPAS:

- for which a type certification is requested,
- for which the kinetic energy assessment in accordance with section 6 of the EASA policy E.Y013-01 results in an initial certification basis according to CS-VLA or CS-VLR, and
- with no occupant on board.

For this instantiation of paragraph 1309, it uses almost exactly the same wording in CS25.1309 for the treatment of likelihood and impact and hence acceptable loss (see Figure 1).

New EASA Policy – SAIL V and SAIL VI

The CAA has tended to mirror EASA policy since Brexit, which is why this new policy is interesting from a market perspective. There are three categories of UAS under the EASA approach to RPAS authorisation: Open (broadly light, very short range, Visual Line of Sight, etc ...), Specific (broadly getting heavier, Beyond Visual Line of Sight (BVLOS), operating closer to larger groups of people, etc..) and Certified (broadly: everything else). EASA have recently published "MOC Light-UAS High Risk.2510-01" [2] which apply to the upper end of the Specific category. This is targeted at UAS that are likely to be heavier, will be BVLOS and closer to people. The objective of Light-UAS.2510 is to ensure an acceptable safety level for equipment and systems as installed as part of the UAS. The safety objectives for each failure condition are reproduced from para 8.1 Safety Objectives per SAIL(Specific Assurance and Integrity Level) in the following table:

	Failure Condition Classification		
	Major	Hazardous	Catastrophic
	Allowable Qualitative Probability		
	Remote	Extremely Remote	Extremely Improbable
	Allowable Quantitative Probability and Functional Development Assurance Level (FDAL)		
SAIL VI	$\leq 10^{-4}$ FDAL D	$\leq 10^{-6}$ FDAL C	$\leq 10^{-8}$ FDAL B
SAIL V	$\leq 10^{-4}$ FDAL D	$\leq 10^{-5}$ FDAL C	$\leq 10^{-7}$ FDAL B

In the notes for this table, EASA make it clear that the quantitative safety objectives are expressed per flight hour and that an average flight profile (including the duration of flight phases) and an average flight duration should be defined. Furthermore, in a recognition that the drone industry does not use the same components/systems that might be used for manned aviation, it states that: "*component failure rate data may not be precise enough to enable accurate estimates of the probabilities of failure conditions.*" The resultant uncertainty must therefore be safely accounted for when calculating the estimated probability of each failure condition. There is quite a lot of guidance in the document which is a significant

enhancement on previous UAS.1309, especially as this now effectively requires use of ARP4754B/4761A and DO-178C for SAIL V/VI aircraft and changes the allowable quantitative probability numbers to be more stringent than previously defined.

The UK

The Civil Aviation Authority (CAA) provides the regulatory services for RPAS in the UK. The major problem all authorities have to deal with is how to authorise on-demand use of fully autonomous capable aircraft. While airspace can be segregated, Transponder Mandatory Zone (TMZ) and the like may provide at least a partial solution with conspicuity and even 'detect-and-avoid' systems being required on board aircraft, there still remains the question over trust: what will these aircraft actually do?

The Answer is On-Board

The decision for what the aircraft will actually do must reside with the aircraft. This is the case for manned aviation and the pilot is responsible for the safety of the aircraft (and passengers). While, for example, Air Traffic Control may direct a pilot to do something, ultimately the decision as to whether to comply resides with the pilot . However, there needs to be assurance that whatever the aircraft is going to do in the apparently wide plethora of possible circumstances, it will always behave as another air-user would expect it to behave.

"The decision for what the aircraft will actually do must reside with the aircraft."

DO-178C Section 2.4.3

Fortunately, DO-178C[4] has at least partially solved the issue of dealing with untrusted functionality (eg AI[5]). At section 2.4.3, Safety Monitoring, "...is a means of protecting against specific failure conditions by directly monitoring a function for failures that would result in a failure condition. Monitoring functions may be implemented in hardware, software, or a combination of hardware and software." The approach is to provide an independent safety monitor that covers the ability to detect system faults at the required integrity level.

Systems Architecture

The systems architecture has to be developed to defend against failure and inaccuracies in sensors; otherwise from the point of view of the software, it's garbage in, garbage out. As noted earlier, many of the systems and material used in UAS are not of manned aviation standards, so failures are more likely. Figure 2 is an overview of a possible systems architecture. Sensors have to cover the spectrum, there has to be sufficient redundancy and this includes off-board data systems such as GPS as well as monitoring on-board systems health. The safety monitor cannot simply block actions, it has to provide an alternative, safe action. This aspect takes a considerable amount of thought and this behaviour has to be accessibly described so that all stakeholders can understand. Although the UAS components may be

[4] The section reference and wording has not changed since the issue of DO-178B in 1992.

[5] Artificial Intelligence (AI) has its place; it is not in safety critical systems without a safety monitor. Indeed, the approach we have in civil aerospace is typically no single point of failure, so why rely upon something that can only ever be around, maybe 95% confident?

built using commodity components, a monitor assured to a manned aircraft standards keeping eye on proceedings provides sufficient protection against failures. However, developing to aviation standards is generally considered expensive and time-consuming.

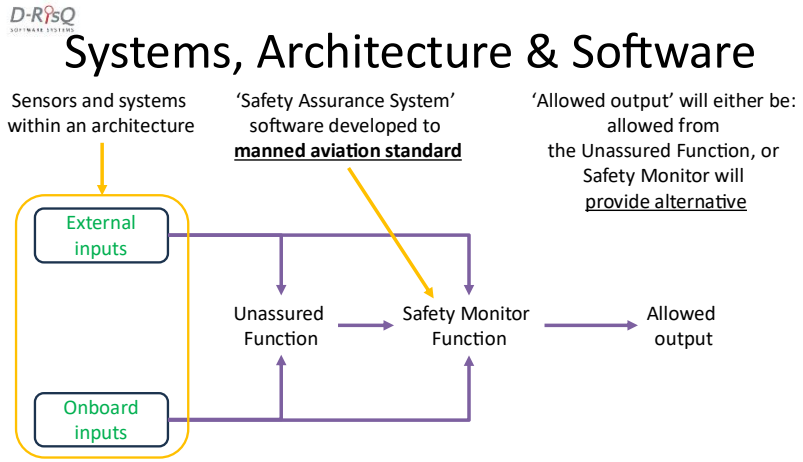


Figure 2 – Safety Monitoring High Level Architecture Overview

Software Development Processes

It is often thought that, in order to develop software to meet aerospace standards, one needs deep pockets. However, the D-RisQ tools have been shown to be highly productive and can dramatically reduce such costs [3]. The software development process is pretty much as usual with the exception that standards compliance includes DO-333, the Formal Methods Supplement to DO-178C. The tools in the process are outlined in Figure 3.

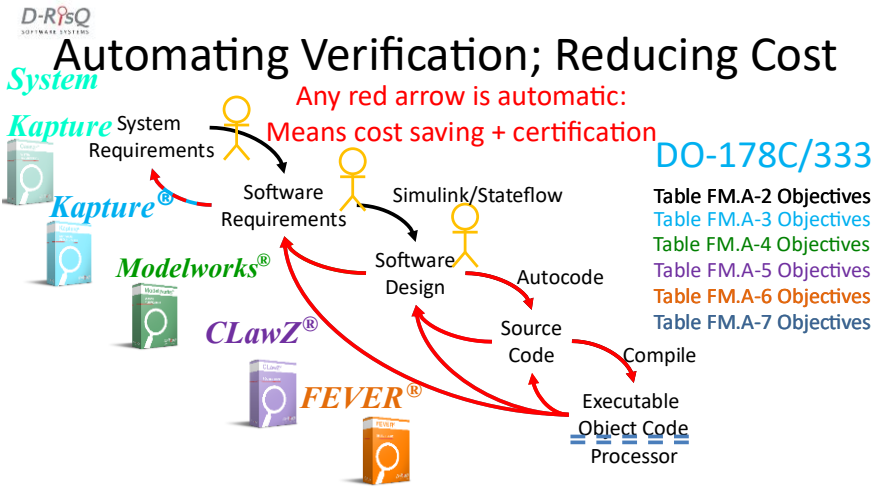


Figure 3 - The D-RisQ Tools in Software Development and Verification

Where is this Happening?

The Digital Tethering project spearheaded by Drone Major Group for Network Rail [4] is exploiting this approach. It has independent safety assurance software developed by D-RisQ with processes designed to meet DO-333. The described behaviour of the aircraft vested in that software assumes that, at some point, the operator will lose communications, have on-board failures, etc and hence we have to build a safety argument that allows safe operation; we have to be able to satisfactorily answer the three questions. All the principles outlined in this article have been implemented and exploits novel navigation and communications systems with redundancy built in, but if things go wrong, the software will continue to behave as described in order to keep the aircraft safe. For example, should the flight control system take the aircraft off track, it will intervene; should one of the navigation systems be insufficiently accurate, the battery be low, the communications be interrupted, etc, the software system will safely intervene.

Conclusion

If the approach for an independent, highly assured safety monitoring system outlined in this article becomes accepted, then there is a potential basis for accepting that drones, in air, land and sea, may be able to operate unsupervised. This supposes that software can be adequately trusted, can be developed at an affordable price and that the many other aspects of systems reliability can also be tackled. This might then provide an impetus to change the law and develop suitable regulation with the resultant impact on insurance premiums for operators and developers alike.

References

[1] EASA, https://www.easa.europa.eu/sites/default/files/dfu/SC-RPAS.1309-01_Iss02.pdf

[2] EASA, https://www.easa.europa.eu/en/document-library/product-certification-consultations/light-uas-2510-01-sail-v-and-vi

[3] D-RisQ, https://www.drisq.com/case-study-steam-boiler-exemplar

[4] Network Rail, https://www.networkrailmediacentre.co.uk/news/network-rail-trials-revolutionary-approach-to-aerial-operations-with-british-drone-companies, accessed April 2025

Nick Tudor, D-RisQ

Following a full career as an RAF Officer Engineer, Nick has been working in software and high integrity systems for the past two decades. As co-Founder of D-RisQ, he has worked in multiple sectors including aerospace, defence, automotive, rail, autonomous systems in air, land, sea, nuclear decommissioning and cyber-security. Perhaps the only claim to fame he might have is as one of the key authors of DO-333, the Formal Methods Supplement to DO-178C (the aerospace software standard).

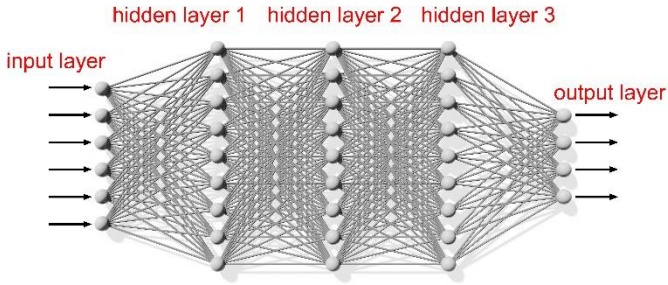
Bridging Gaps in ISO 26262 for Testing Machine Learning (ML) Systems

Integrating Machine Learning (ML) into safety-critical automotive systems presents new challenges. As automotive technologies evolve, standards like ISO 26262, which regulate the functional safety of electrical and electronic systems in vehicles, must be updated to address the complexities of modern ML systems. Drawing on a recent peer-reviewed IEEE Access publication co-authored with Emil Gracic and Gregor Pawelke, Padma Iyenghar outlines a systematic approach to enhancing ISO 26262 by introducing ML-specific life cycle phases and testing methods to ensure the safety and reliability of ML-driven systems.

While ISO 26262 [5] has effectively guided traditional software, it falls short in ensuring the safety and reliability of ML-driven systems due to the unique challenges posed by ML, such as non-determinism, interpretability issues, and the difficulty of comprehensive testing. As ML is increasingly embedded in automotive applications, adapting functional safety standards is crucial to address these challenges.

Gaps in ISO 26262 for ML

ISO 26262 is a solid standard and framework for ensuring the safety of automotive systems that includes structured guidelines for development, testing, and certification. However, the growing use of ML in safety-critical systems reveals significant gaps. These gaps mainly involve the life cycle phases of ML systems, their safety or desired properties, and the testing methods used to validate them.



deep neural network

1. Absence of ML-Specific Life Cycle Phases

While ISO 26262 covers software life cycle processes, it doesn't address the unique aspects of ML systems. ML involves stages like data preparation, model training, and deployment, each needing specific safety and verification measures. ISO 26262 does not guide these stages, leading to inconsistency and uncertainty in industry practices.

2. Lack of Safety Properties for ML Models

ML systems must meet certain safety properties that are not covered under traditional software safety requirements. For example, robustness, uncertainty handling, and interpretability are critical for ML models, particularly in scenarios where the systems interact with humans or make safety-critical decisions. These properties ensure that ML models operate safely under unpredictable conditions. However, ISO 26262 lacks provisions for their integration into the safety assurance process.

3. Insufficient Testing Methods

ISO 26262 provides specific recommendations for traditional software testing methods that vary based on the Automotive Safety Integrity Level (ASIL) assigned to each component or system. The rigour and depth of testing increase with each ASIL level, reflecting the higher risk and safety requirements.

"While existing standards like ISO/IEC 29119-11 and ISO PAS 8800 address some aspects of AI and ML testing, they do not comprehensively cover the full life cycle of ML models in automotive contexts"

This comprehensive approach ensures that systems meet their safety goals and function reliably under various conditions. However, ML testing introduces new challenges. ML models are often treated as "black boxes," complicating their interpretability, testing, and validation.

While existing standards like ISO/IEC 29119-11 [2] and ISO PAS 8800 [3] address some aspects of AI and ML testing, they do not comprehensively cover the full life cycle of ML models in automotive contexts. As a result, there is a lack of systematic, clear, and uniform development procedures that provide critical guidance for expert assessment and independent certification, ensuring reliable recommendations.

Proposed Framework: A systematic approach

To effectively integrate ML into the ISO 26262 framework for safety-critical automotive systems, our proposed solution in [1] outlines necessary enhancements that are required to bridge current gaps.

These enhancements are centred around the introduction of three new ML-specific life cycle phases: preparation of data, training of ML models, and deployment of ML models. Each of these phases necessitates defined inputs, rigorous testing methods, and the management of outputs that meet specified safety properties, such as robustness, explainability, and uncertainty handling. These properties are meticulously selected based on expert judgment to ensure they address the most critical aspects of ML system development.

ML-Specific Life Cycle Phases

To address the lack of ML-specific guidance in ISO 26262, three dedicated life cycle phases are proposed.

- **Preparation of Data:** This initial phase demands quality-assured data and metadata as inputs, which are critical for training robust ML models. The existing ISO 26262 framework does not specify these requirements; hence our proposal includes rigorous data handling measures to maintain the quality of ML-specific data.
- **Training of ML Model**: Post-data preparation, the ML model undergoes training. This phase's output often serves as a prototype and not the final deployed product. Thus, it's critical to apply stringent test methods during this phase to ensure the quality and reliability of the model before it advances to deployment.
- **Deployment of ML Model**: In the final phase, the trained ML model is refined and adapted to meet operational demands and hardware limitations, culminating in the deployment of the ML model. This version, which will be utilised in real-world applications, integrates with other software units and requires additional deployment-specific test methods to ensure its functionality and safety.

Definition of Desired Safety Properties

In the integration of ML into safety-critical automotive systems, defining desired properties for each life cycle phase is essential. These properties are critical non-functional requirements that ensure high-quality results throughout the development and testing of ML models. For instance, the trained ML model, a key outcome of one phase, becomes a foundational input for the deployment phase.

Selected based on expert judgment, desired properties such as completeness, consistency, robustness, explainability, and uncertainty handling are prioritised to ensure that ML models are fully developed and operate reliably under various conditions.

"The proposed framework aims to improve current practices in ML model development and testing, addressing gaps in existing standards"

By focusing on these key attributes, the proposed framework aims to improve current practices in ML model development and testing, addressing gaps in existing standards and laying the groundwork for the systematic testing of ML models, thereby contributing to the development of more reliable and safe automotive systems.

Definition of Test Methods

Several standards that provide robust test methods for developing and testing ML models were considered, each contributing valuable insights and methodologies. ISO 29119 (Part 11) and ISO PAS 8800 were selected based on expert judgment, recognising that many of these test methods are complementary and enhance their effectiveness in ensuring safety.

In the initial step, the test methods in these standards were thoroughly analysed for their applicability to the ML life cycle phases. This analysis resulted in a detailed mapping of test methods to specific phases of the ML life cycle. For each test method, a concise definition was developed, and a concrete and pragmatic description was provided to ensure clarity and ease of implementation.

It is important to emphasise that while specification and design are crucial activities within the life cycle phases discussed, the primary focus was placed on refining testing methodologies. These methods are essential in ensuring the robustness, reliability, and safety of ML models. By leveraging the comprehensive guidelines and methodologies from ISO 29119-11 and ISO PAS 8800, a solid foundation for the systematic testing of ML models was aimed to be established, ultimately contributing to the advancement of safety-critical automotive systems.

The systematic framework presented in [1] employs a rigorous evaluation framework inspired by IEC 61508 (Part 3, Annex C) [4], which assesses the effectiveness of methods for ASIL A and B conformance. This includes assigning rigour levels (R1 and R2) to categorise methods, ensuring that ML models meet essential safety properties, thereby enhancing product safety. The framework involves creating mapping tables that align desired safety properties with specific test methods, promoting a structured approach to their application.

Outputs and Recommendations

The framework establishes well-defined inputs, methods, and objectives for each life cycle phase, mirroring the structure used in ISO 26262. Through rigorous evaluations, it provides recommendations for methods that achieve ASIL A/B compliance. These enhancements aim to refine the testing and certification processes for ML-driven systems in the automotive industry, significantly boosting their safety and reliability.

Impact on the Industry

The proposed extension of ISO 26262 will have a significant impact on the automotive industry, particularly in the integration of ML into safety-critical systems. By defining clear life cycle phases and testing methods, the framework will:

- Provide clarity on ML model development and testing in compliance with functional safety requirements
- Streamline the certification process with a well-defined testing methodology
- Enhance the safety and reliability of ML systems through rigorous testing and alignment with key safety properties

This approach will be invaluable to automotive manufacturers, suppliers, and certification bodies, as it addresses the challenges of integrating ML into safety-critical systems while reducing ambiguity and enhancing overall system integrity.

Conclusion

The integration of ML into automotive systems is becoming increasingly prevalent, making it imperative to evolve ISO 26262 to address these modern complexities. Our proposed enhancements help bridge the current gaps, contributing to safer, more reliable ML-driven automotive systems. Future work will aim to extend this framework to higher ASIL levels and explore additional ML techniques, ensuring that safety standards keep pace with technological advancements.

For more detailed information and insights into our methodology and findings, please refer to our publication in [1].

References

[1] P. Iyenghar, E. Gracic and G. Pawelke, "A Systematic Approach to Enhancing ISO 26262 With Machine Learning-Specific Life Cycle Phases and Testing Methods," in IEEE Access, vol. 12, pp. 179600-179627, 2024, doi: 10.1109/ACCESS.2024.3506333.

[2] ISO/IEC TR, 29119-11:2020, "Software and Systems Engineering—Software Testing—Part 11: Guidelines on the Testing of AI-based Systems", 2020.

[3] ISO Std. ISO/DPAS, 8800, "Road Vehicles—Safety and AI", 2023.

[4] IEC 61508-1:2010, "Functional Safety of Electrical/electronic/programmable Electronic Safety Related Systems", 2010.

[5] ISO, 26262, "Road Vehicles—Functional Safety", 2018.

Dr. Padma Iyenghar (innotec GmbH)

Padma Iyenghar is a senior Functional Safety and Cybersecurity Consultant at innotec GmbH–TÜV Austria Group, with a strong background in AI, academia, and industry. From 2020 to 2024, she also served as Development Professor at the University of Applied Sciences, Osnabrück, and continues to take on selected teaching assignments. She holds a Ph.D. from the University of Osnabrück and has over 14 years of R&D and 8 years of teaching experience, contributing actively to academic and professional communities. She is also an active member of the standards committee DKE/AK 914.0.11 – Functional Safety and AI.

Web: https://sites.google.com/site/piyengha/

https://scsc.uk

SCSC

For Everyone Working in System Safety

Safety-Critical Systems Club (SCSC)

How Safety Culture has to Change With AI

Thursday 19 June, 2025

Hilton London Euston Hotel, London

This 1-day seminar looks at how an organisation's safety culture has to change when systems including AI are introduced. The emergent application of artificial intelligence in safety critical systems raises many questions for safety culture.

This seminar is for all of those involved in introducing AI into the workplace, especially in a safety critical situation. It will be useful for safety engineers, programme and change managers, and operational staff.

Ben Fulford, Safety Consultant, BMT
Merging human expertise with AI for better safety management

Paul Leach, Head of Human Factors, Rail Safety and Standards Board
Human factors principles for the design and operation of AI systems in rail

Kathy Syfret, Deputy MilCAM for A400M RAF platform
AI and Aircraft Maintenance

Ben Wright, Coventry University
TBA

Michael Wright, Wright Human Factors Ltd
Artificial Intelligence: Emergent safety culture issues

Safety and Highly Automated Machinery

Tampere, Finland – often referred to as the "Manchester of the North" and aptly nicknamed "Manse" – is a centre for research into the automation of off-road mobile machinery. This research is being conducted at the University of Tampere in close collaboration with the R&D departments of local machinery manufacturers. There, for the past four years, Marea de Koning, has been conducting research into the safety of highly automated off-road mobile machinery. In this article, Marea provides a summary of her research, where it started and ended.

My initial findings and concerns have been summarised and discussed in a previous publication of this newsletter ("The Innovative Hydraulics and Automation Lab", *Safety Systems* Vol 31 Nos 2 May 2023). Meanwhile, several years later the research – published across five articles (one of which remains in review at the time of writing) – in the form of a PhD dissertation has come to an end.

The objective of my research was threefold:

- To enhance the understanding of where, when, and how automation in off-road mobile machinery exceeds the scope of the Machinery Directive
- to evaluate the implications of forthcoming legislative changes; and
- To identify potential pathways and roadblocks towards safer highly automated off-road mobile machinery

Where the research starts

Off-road mobile machinery, such as those deployed in the construction, mining, forestry, and agricultural sectors, are essential to numerous industries worldwide. Currently, the EU is a world leader in the manufacturing of such machinery, with a turnover of approximately €740 billion annually [1]. This success can be attributed, in part, to the strict safety requirements for machinery entering the market. Manufacturers must demonstrate compliance with the Essential Health and Safety Requirements (EHSR) documented in the Machinery Directive (MD) (Directive 2006/42/EC) via a 'Conformité Européenne' (CE) declaration, which guarantees a baseline level of safety for EU citizens and workers. This protection is vital, as harm – defined as the risk of physical injury, damage to health, or property – is a major concern in workplace safety.

"These higher levels of automation not only introduce new risks, challenging workplace safety assurance, but have also prompted a change in the machine safety regulatory landscape"

The MD defines machinery as a collection of linked parts or components, at least one of which moves, powered by a non-human or non-animal energy source, and designed for specific functions. The introduction of new digital technologies, such as Artificial Intelligence (AI), Machine Learning (ML), and the Internet of Things (IoT), facilitates higher levels of automation in off-road mobile machinery. These higher levels of automation not only introduce new risks, challenging workplace safety assurance, but have also prompted a change in the machine safety regulatory landscape.

As of January 27th, the MD is to be superseded by a Machinery Regulation (MR) (Regulation 2023/1230). This change broadens the scope of the ESHR and expands the definition of machinery.

One of the most significant amendments is the inclusion of software within the overall definition of machinery. More specifically, the definition of machinery has been extended to include "*... including those that only lack the software upload intended for the manufacturer's envisioned use*"[6]. This update formally acknowledges the role and importance of software in machinery design and operation. Furthermore, the MR specifies that when software performs a safety function and is independently placed on the market, it is classified as a safety component. Such amendments reflect the growing influence of digital solutions on safety, particularly as the level of automation in off-road mobile machinery increases.

Despite existing regulations, fatal and non-fatal accidents in the workplace remain prevalent. In 2022 alone, the EU recorded approximately 3,286 fatalities and 2.97 million non-fatal accidents. Most fatal and non-fatal accidents occur in areas such as mining, manufacturing, forestry/agriculture, or construction sectors. These accidents are often attributed to a loss of control of machinery (e.g., unexpected start-up of an off-road mobile machine or unexpected overextension of a mobile elevating work platform). Human errors such as falling, stumbling, or slipping typically come second [2] [3].

There is a growing concern that accident patterns seen in other fields which integrate higher levels of automation in their systems – such as (mobile) robotics and automotive vehicles – could translate to highly automated off-road mobile machinery. This could potentially exacerbate existing accident rates rather than mitigate them, as is often expected. This concern is one of the reasons the MD has been superseded by the MR.

Nevertheless, adjusting the scope of EHSR to encompass the potential risks of highly automated off-road mobile machinery does not necessarily solve the safety challenges manufacturers now face. Instead, it can be said that it has made the journey to safer highly automated off-road mobile machinery more difficult, as it remains unclear to what extent and to which standards a highly automated off-road mobile machine should comply to conform to the forthcoming MR.

What was contributed

This research contributes by establishing a foundation for understanding safe highly automated off-road mobile machinery by examining the challenges of conforming to standards and achieving compliance. The contribution, presented in [4], is the identification of six key areas where highly automated off-road mobile machinery faces compliance limitations:

- Run-time failures
- Algorithmic failures
- Complex architectural design patterns
- Data-driven intended behaviours
- Integration quality
- Limitations in formal verification

The research continues by identifying lessons learned from related fields facing similar challenges.

[6] This, in effect, is adding software to the definition of machinery and no longer restricting it to be just physical components.

This contribution found [5], by abstracting lessons learned from similar domains and translating them into the context of highly automated off-road mobile machinery, providing a foundational starting point for understanding its requirements. Building on this, the dissertation makes another contribution found in [6], which examines the transition from the MD to MR. This change has several key implications:

- A directive is now superseded by a regulation
- It explicitly includes software and digital components within the definitions of machinery and safety components
- It introduces additional provisions for highly automated off-road mobile machinery classified as high-risk, requiring autonomous mobile machinery and related products to have control systems capable of performing safety functions independently, even when actions are ordered by using a remote supervisory function; and
- It expands the role of the supervisor, mandating that if the supervisory function is inactive, the automated machinery must not be able to operate, while also requiring the human-machine interface (HMI) to be adapted to the foreseeable characteristics of the operators.

"A recommendation is made for the integration of Safety Reasoning Modules (SRMs) … intended as a high-level decision-maker. Analysing risks in real-time using sensor data and AI or rule-based logic to adapt responses dynamically."

This shift in the EHSR requires machines to perform safety functions autonomously, even when overridden by a supervisor, and mandates supervisory functions in high-risk machinery for event-based intervention, while also emphasising the need to enhance HMIs and prevent machine-determined changes in work rates. This signals a future where the minimum EHSR for off-road mobile machinery prioritises operator well-being and intervention capacity, positioning them as supervisors, either remotely or within the cabin and requires highly automated off-road mobile machinery to be capable of safely reasoning on the behaviour that they are executing.

As such, in [4], a recommendation is made for the integration of Safety Reasoning Modules (SRMs). While a safety function is a predefined mechanism that triggers immediate, fixed responses to hazards – such as a light curtain breach immediately stopping a machine – an SRM is intended as a high-level decision-maker. Analysing risks in real-time using sensor data and AI or rule-based logic to adapt responses dynamically. In safety-critical systems, both the SRM and safety function serve distinct yet complementary roles: the SRM evaluates the need and coordinates safety measures, while safety functions execute them. At the time of writing, one other contribution remains under review. This work evaluated and presented the specifics with respect of the technical design requirements of such an SRM.

Additionally, this dissertation has another contribution found in [7], which proposes a risk-based assessment of supervisor-machine shared decision-making, examining how supervision affects the required level of human engagement, particularly in relation to the machine's ability to remain aware of and respond to emerging hazards during runtime.

The proposed risk-based assessment of supervisor-machine shared decision-making redefines controllability as the ability of a highly automated off-road machine to prevent harm through timely reactions and the supervisor's event-based intervention. Controllability is then categorized into five Levels of Controllability (LoC), guiding design, verification, and validation to ensure the machine accounts for the supervisor's cognitive limits. This includes Machine Awareness of the Hazard (MAH) – how well the system perceives risks – and Degree of Decision Making (DoDM) – its ability to respond appropriately. The method helps define safety requirements for highly automated off-road machines, ensuring human-in-the-loop solutions where necessary. MAH varies from full hazard awareness to complete unawareness, while DoDM assesses the machine's response capabilities in relation to human reaction times.

Conclusion (Future areas of concern)

That said, many questions remain, particularly about the risk assessment proposal's effectiveness in safety design and whether further adaptations are needed for highly automated off-road machines to address the impact of human supervision. Additionally, it will be necessary to work towards realizing the proposed SRM and assessing its relative effectiveness. Nevertheless, the research presented across multiple peer-reviewed publications and compiled into one dissertation provides a theoretical foundation for safety in highly automated off-road machinery, offering valuable insights for manufacturers, researchers, policymakers, and standards organisations. Its findings support shaping the future of safety in highly automated off-road mobile machinery.

Finally, it is important to highlight how this shift to supervisory roles affects the well-being of operators. For the time being, it appears that supervisors will remain an integral factor in the safety case for event-based intervention if and when the machine fails, despite rigorous efforts by engineers to design robust machines, they do remain responsible for event-based intervention. We should research how machine 'safety by design' practices can evolve to support the needs of humans in supervisory roles to avoid and/or mitigate the negative consequences of long-term supervision on well-being.

The publication of the dissertation and the defence is scheduled for 13th June 2025. It is open to the public and everyone interested can attend. Additionally, it is possible to follow the event via livestream; simply send an email directly to the author, Marea De Koning, at marea.dekoning@gmail.com if interested.

References

[1] S. Gospodinova, "Commission welcomes political agreement on new rules to ensure the safety of machinery and robots," 15 December 2022. [Online]. Available: https://ec.europa.eu/commission/presscorner/detail/en/ip_22_7741, accessed April 2025.

[2] E. Union, "Accidents and injuries statistics," 6 2024. [Online]. Available: https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Accidents_and_injuries_statistics, accessed April 2025.

[3] E. Union, "Accidents at work - statistics on causes and circumstances," November 2024. [Online]. Available: https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Accidents_at_work_-_statistics_on_causes_and_circumstances, accessed April 2025.

[4] A.M.R. de Koning, R. Ghabcheloo, "Machine safety conformance limitations for highly automated and autonomous heavy-duty mobile machinery," in The Future of Safe Systems: Proceedings of the 31st Safety-Critical Systems Symposium (SSS'23) 7-9th February 2023 , York, United Kingdom, 2023.

[5] A.M.R. de Koning, A. Ahonen, N. Strokina, R. Ghabcheloo, "Safety architectures for cyber-physical systems: review of state-of-the-art and outlook for heavy duty mobile machinery," in The Eighteenth Scandinavian International Conference on Fluid Power, SICFP'23, Tampere, Finland, 2023.

[6] A.M.R. de Koning, A. Ahonen. T. Machado, N. Strokina, T. Minav, R. Ghabcheloo "A comprehensive approach to safety for highly automated off-road machinery under Regulation 2023/1230," Elsevier Journal of Safety Science, vol. 175, 2024.

[7] A.M.R de Koning, W.L. brown, T. Minav, R. Ghabcheloo, "Towards Safer Supervisor-Machine Shared Decision-Making for Runtime Hazard Mitigation in Highly Automated Off-road Machinery," in Safety of Industrial Automated Systems – SIAS 2024, Tampere, Finland, 2024.

Marea de Koning, Functional Safety Expert HULD oy, Finland

Now no longer a newcomer to the field of safety, Marea de Koning, has finished her PhD research in safety for highly automated off-road mobile machinery at Tampere University. Currently, she works as a functional safety expert at HULD oy, consulting on various safety and security related projects. Her background comes from a bachelor's degree in embedded software development and a master's degree in industrial engineering received from the Netherlands and Germany respectively. Her aim is to contribute to the advancement of autonomous technologies, by ensuring that these systems can be deployed safely and she remains open to see what the future holds.

Entropy, Disorder, The Human Race, Religious Beliefs

Malcolm Jones explores whether the second law of thermodynamics – the tendency for systems to trend toward disorder – applies to human societies, such as organisational groups, states and even at a global level. History shows that humanity has been subject to periods of extreme disorder but what mitigating factors are at play to prevent an eventual "thermal death". Could religious beliefs and teachings play a part?

Introduction

The question is posed. Does the second law of thermodynamics influence humanity and does it have linkage to religious beliefs and teachings? Firstly, it seems strange to apply a physics law to a human aspect. Humanity is not a closed system in the physics sense, rather, it is influenced by its environment and is able to change the laws which govern it. This is unlike a closed physical system which cannot do either. In turn, a closed system will trend towards a state of maximum disorder. However, humanity does itself exhibit some characteristics similar in nature to that of a closed system, with a tendency to disorder unless acted upon by mitigating actions. In addition, these human negative attributes and mitigating actions are also well known in religious beliefs and teachings.

The Second Law of Thermodynamics

Everyone with a background in science will understand what the term entropy signifies when coupled with the second law of thermodynamics. It is a measure of the level of disorder and uncertainty, and lack of ordered information and, for a closed system, it inevitably moves in the direction of increasing disorder and uncertainty. A closed system is one which has no external interactions which can lead to a change in the internal laws that govern it. In such a system with some fixed laws, the thermodynamic process will continue until the system reaches its maximum disordered state – sometimes called the path to thermal death – unless mitigated by internal action!

Take the case of a simple china teacup. Its 'life' starts in the form of a set of naturally available disordered core materials. These are then taken through an **externally** applied set of energetic and information-based processes of mixing, shaping, and firing, resulting in the final ordered form of a cup.

This only occurs as the result of the application of externally derived, knowledge-based energetic processes. Of course, natural processes will lead inevitably to disorder of the ordered cup form. For example, it will quickly break into pieces by mishandling or even with the passage of time it will slowly disintegrate into a base set of materials of disordered form.

Any process to re-constitute the cup into its original ordered form will again require knowledgeable energetic action from an external source. The message here is that the progression to disorder is natural, easy to enact, can occur quickly, but the re-ordering process is more difficult and is slower to achieve.

"The message here is that the progression to disorder is natural, easy to enact, can occur quickly, but the re-ordering process is more difficult and is slower to achieve"

Humanity has inbuilt characteristics, both at the individual and group level, which can lead naturally to disorder, and if not checked can even lead to catastrophic disordered states. If humanity was a closed system, then its future would be somewhat doom-laden. Reversing the trend by internal action, based on information gained from knowledge of, and interaction with the external environment, requires the application of a great deal of information, effort, resilience, and energy.

In any non-closed system like humanity, these disordering and re-ordering processes give rise to a competing status. The human race's trajectory through time is governed by the balance between the natural 'entropy's' disordering laws inherent in the human character, and the wisdom, determinism, and energy needed to reverse the flow. Unfortunately, because disorder is characterised by being somewhat easy and can occur quickly, whereas re-order is characterised by the opposite, history shows a somewhat checkered characteristic through time.

The Natural Laws for Disorder

These are the human equivalent of the fixed natural laws in a closed system and are associated with some of the inbuilt nature of the human character. These are the disruptive negative characteristics of jealousy, hatred, revenge, spite, self-advantage, self-importance, antagonism, paranoia, etc, and even unhealthy competition. All potentially leading to conflict with others and creating disorder. This of course not only applies at the individual level but also at the group level. Each group can have its own 'group level-based characteristics' which in turn do not necessarily align with those of other groups, with resulting disorder between groups. This extends up to the state and even global level, where history shows, that this can lead to catastrophic disordered conditions, such as world wars.

A current global example is illustrated by the disorder arising from the conflict between the forces of democracy and those of a more autocratic and dictatorial alignment. If not suitably mitigated this could well lead to catastrophic global disorder and consequence. As our weapon-based technologies evolve ever further in the direction of mass destruction, this disorder could eventually lead to ever greater harmful consequence.

Another example leading to disorder on the global competitive and self-interest scale, is represented by the continuous trend of population increase coupled with an increased appetite for a better life, both challenging the earth's ability to provide the necessary resources.

It is hard to see these forces for disorder getting less strong. Also, it is generally accepted that global warming results from these appetites with increasing conflict between those who are the largest perpetrators and those who are the biggest victims.

History shows that humanity has been subject to instances of rapidly increased disorder followed by long term painful and energy intensive/wisdom-based recoveries. The second law of thermodynamic still very much in evidence. This is illustrated in Figure 1, which is not intended to show whether the long-term trend of disorder is increasing or decreasing with time, but there is increasing concern that the consequences might well do so, due to the ever more destructive nature of weapons of mass destruction (nuclear, biological, chemical, and cybernetic). Perhaps by example the peaks and the troughs in the figure might represent the last two world wars and the third trough and peak, by extension, might symbolise the current state of the world we seem to be heading into.

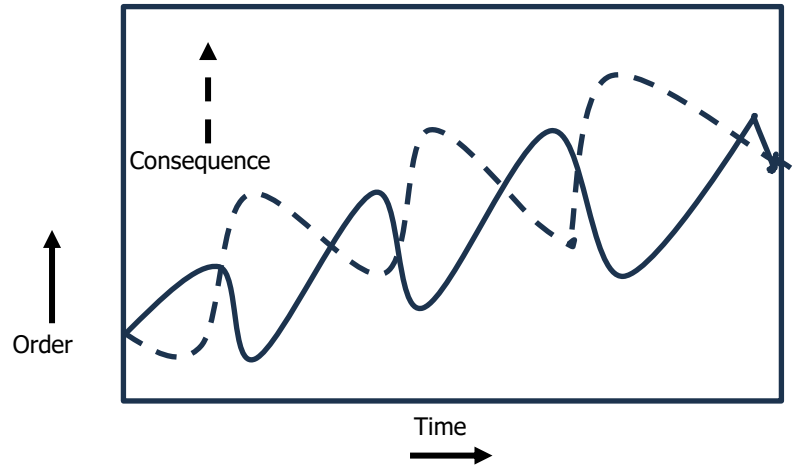


Figure 1. Progression of order and consequence over history.

Changing the Internal Laws and Religious Beliefs and Teachings

As noted previously the human-race needs not be governed entirely by fixed laws (of human negative character) and the inevitable entropy trend to disorder and uncertainty. Humans can change these behaviours for the better given sufficient intent, energy, determination, wisdom and knowledge of how to do so. However, the second law of thermodynamics still holds in that, disproportionate effort, supported by information gained from the 'outside,' is required to mitigate the disorder trend.

So, what were/are these disproportionate efforts aimed at mitigating the natural disorder trends? The earliest historical approach took the form of supernatural beings or Gods. The human-race was periodically subject to disasters, such as epidemics, earthquakes, volcanoes, floods etc. There was no scientific capability of understanding how and why these disasters arose, and of how to provide mitigation.

This 'unknowing' was attributed to the acts of supernatural beings, or gods, raining down punishments on humanity because of humanity's apparent misdemeanours.

It was felt necessary to appease such deities, through worship, paying homage and generally doing the 'right thing.' However, this often-included human sacrifice to satisfy the assumed revenge 'appetites' of the deities.

This approach eventually led to the concept of a more modern religious belief in a more benevolent God (or Gods), but who still required homage and doing the 'right thing' to ensure the relationship remained benevolent.

This required a need to follow a set of edicts in order to maintain the benevolent relationship. For example, Moses 'came down from the mountain' having received God's ethical directives – the 'Ten Commandments.' Some examples of which being: "honour you father and mother,

shall not murder, shall not commit adultery, shall not steal, shall not bear false witness against your neighbour, shall not covet." Compliance with these edicts either through belief or fear would act as a counter to the negative human characteristics, help to prevent disorder and lead to a better life and after-life.

Following on from this is the equivalent secular model of establishing human based laws, still with a strong relationship to the original religious directives. The laws were agreed at group level, and then applied to the individual, with measures of agreed punishment for non-compliance. This approach has now been extended up to state and even global government levels. With the correct choice of laws, their enactment and punishments, managed in what is seen as in a democratic manner, this represents the best form of human stability and order that humanity has achieved to date. Like the second law of thermodynamics this mitigating approach to disorder has required enormous, continuous, resilient effort and knowledge to be effective in combatting disorder. History has shown it not to be a continuous success.

"With the correct choice of laws, their enactment and punishments, managed in what is seen as in a democratic manner, this represents the best form of human stability and order that humanity has achieved to date"

Summary

Although humanity is not a closed and isolated system, it nevertheless does show some of the major characteristics associated with a closed system with a tendency for moving in the direction of disorder, unless mitigated by internal rule changes for the better. Human's negative characteristics act somewhat like the entropy rules in its second law. However, unlike the fixed laws in a closed system, humanity can challenge and mitigate the trend to disorder.

Just as in a closed system, processes leading to disorder can happen more easily and quickly, than the man-made attempts to increase order. The latter requires a great deal of determination, resilience, energy, honesty, knowledge, and continuity.

So, humanity is not independent of the second law of thermodynamics. History suggests that the future will see a continuous series of eras of disorder and re-order. Certainly, the world currently appears to be in a serious state of increasing disorder.

Perhaps the status is best described by the perennial battle between 'good and evil.'

Malcolm Jones, AWE, PhD, DSc, MBE

Malcolm has more than 50 years practising as a scientist at AWE and has been awarded a number of national and international awards in recognition of his work. Much of this work relates to system safety and, in particular, to its application to nuclear programmes, where he has been the author of a number of safety standards. His current role is broadly of an advisory nature, having previously been the scientific adviser to AWE's chief Scientist, the Head of Warhead Engineering and the Head of Warhead Technical assurance.

Image attribution:
clock; ID 294210155 | A © Anthony Baggett | Dreamstime.com
cup: AI generated Midjourney
battlefield: ID 359001792 © Oleh Bilovus | Dreamstime.com
crowded earth: AI generated Midjourney
Aztec sacrifice: public domain


SCSC
For Everyone Working in System Safety
Safety-Critical Systems Club (SCSC)
Complying with the EU AI ACT:
What is needed for Products and Systems?
Thursday 9 October, 2025
DoubleTree by Hilton Hotel, Brussels, Belgium
This one day event will cover the EU AI ACT itself and discuss the implications for organisations and engineers working with AI technology. It will have a particular emphasis on AI systems incorporated as part of solutions with safety implications.
The seminar will be useful for all those involved in production of AI systems: system engineers, safety engineers, product and programme managers, and also those involved in deployment and introduction of such systems.
Jan De Bruyne
Professor IT law at KU Leuven and
Head of the Centre for IT & IP Law
Isabella Ferrari
Professor at Università degli Studi di Modena e Reggio Emilia
Jelle Hoedemaekers
Agoria
Thor Myklebust and Dorthea Mathilde Kristin Vatn
SINTEF Digital
Karin Rudolph
AI Ethics and Governance consultant and
Founder Collective Intelligence
Mathias Verbeke
Faculty of Engineering Technology, KU Leuven
https://scsc.uk

SSS'25 Event Report

The Safety-Critical Systems Club's annual Symposium returned in February 2025 for another fully in-person event hosted at The Milner Hotel, York. Paul Hampton, the SCSC Newsletter Editor, provides highlights from the three-day event.

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

Looking Beyond the Horizon

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

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

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

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

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

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

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

AI Safety and Security

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

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

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

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

Armchair Chat

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

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

Technical Entertainment

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

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

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

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

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

Exhibition and Drinks

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

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

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

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

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

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

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

Armchair Chat

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

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

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

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

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

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

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

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

Workshops

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

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

Stream A

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

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

Stream B

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

'5 minute pitch' presentations

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

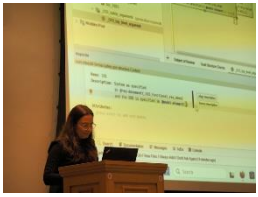
There were presentations from:

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

The winning presentation was from Prenika Anand.

Stream C

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



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

Social Events

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

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

Poster Session

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

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

Banquet

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

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

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

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

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

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

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

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

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

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

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

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

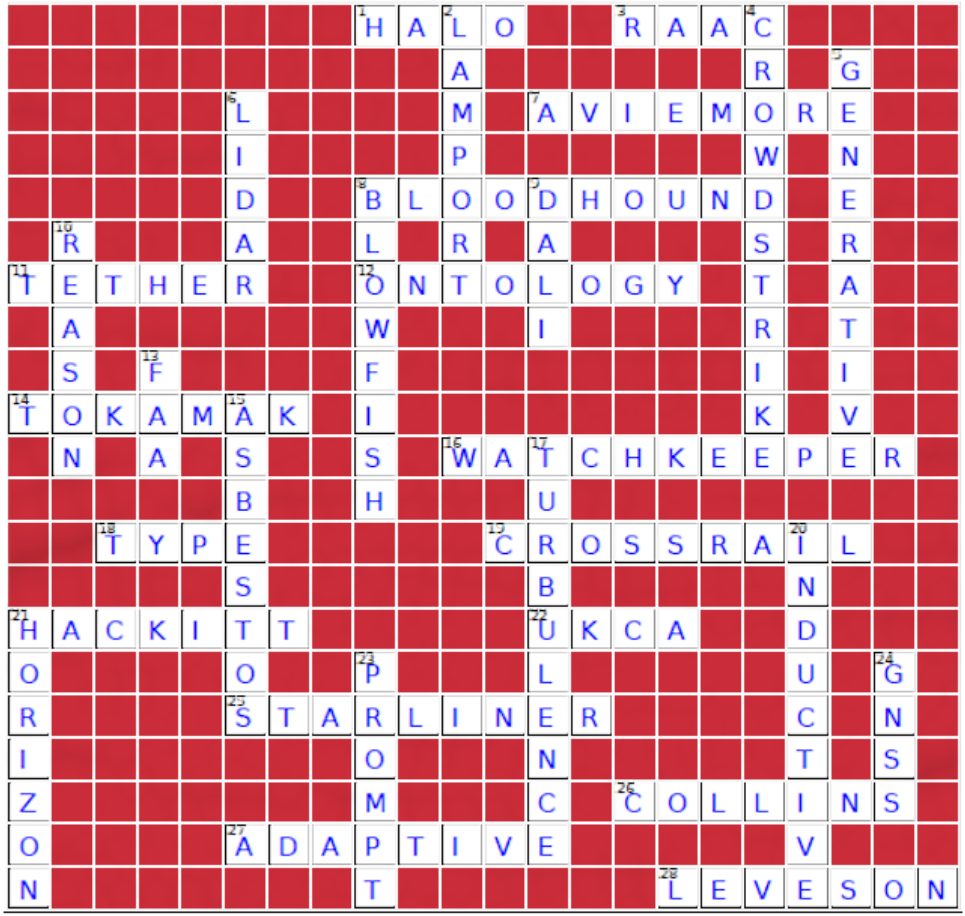
- Goal Structuring Notation (GSN)
- The 6-step method for applying the GSN notation to create arguments
- Ways of capturing challenges to arguments through, for example, dialectic arguments
- Techniques for developing confidence arguments
- Link operational arguments in design Safety Cases
- Ways to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

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

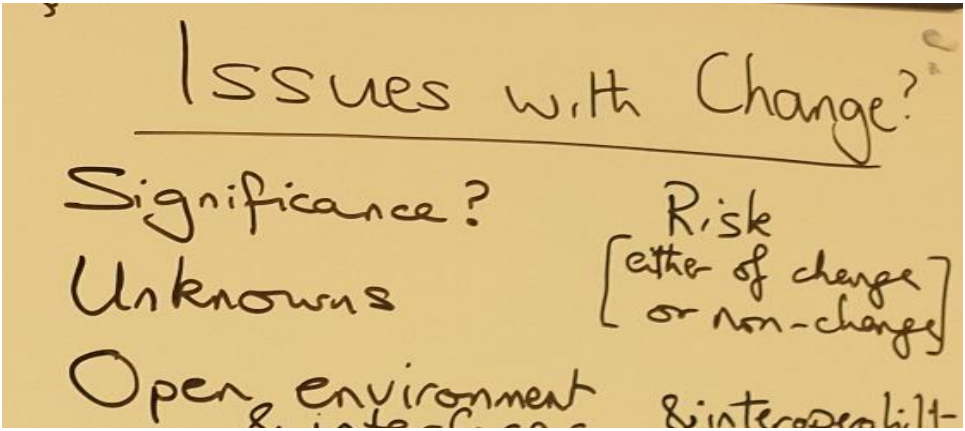
Crossword Competition

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

The answers to the crossword are given below.



Management of Change in an Ever-Changing World



This year, the Safety-Critical Systems Symposium (SSS'25) held a number of parallel workshops covering a wide range of topics. Wendy Owen reports on a workshop that she led, supported by Stephen Bull, focused on managing change in a world of rapidly changing technology, increasing cyber threats, and adapting systems for climate change and the development / update / modification of safety cases on such projects.

Introduction

How do you manage change in a world of rapidly changing technology and ever-changing priorities? Change is of particular concern where there are – or could be – safety, security, and/or environmental implications.

Consider the roles of Management of Change (MoC) and Change Management (CM) in the context of systems being designed, built, and operated today:

- MoC is the high-level approach i.e. policy, strategy or framework
- CM refers to the detailed process of managing changes

It is not that significant technological changes have not happened in previous decades, they have. However, the nature, functionality and complexity of today's systems place a particular onus on traceability, auditability, and assurance, to ensure that these systems are safe and fit for purpose both for today's operating environments and those of the future. MoC and CM are important for security (cybersecurity), safety, and environmental reasons, as – done well – they capture the raison d'être of the change(s). This can then feed into the safety, security, and environmental cases.

In a world of rapidly changing technology, increasing cyber threats, and adapting systems for climate change, it is becoming increasingly important to manage change at all levels. MoC enables intelligent business decisions at every stage of the project, system and safety lifecycles. Within the MoC process, consideration is given to the delivery of outcomes or overall goals rather than specific outputs. Acknowledgement and integration of CM within companies, engineering teams and projects is increasingly important for high-quality outputs and outcomes. Both MoC and CM can better support longer-term business goals and Key Performance Indicators (KPIs) in an ever-changing world. In today's world, it is thus also important to manage change to enable outcomes, not only outputs.

However, in such a changing world and with an increasing number of KPIs linked to external factors, such as societal or environmental changes, assessments and documentation can also quickly become out-of-date. It is thus essential to link the safety case version to the system version, or any arguments in the safety case can quickly become redundant and the safety case invalidated (the same applies to security and environmental cases). Ideally, the links should be between elements in the system specification (both requirements and design) and elements of the safety case. Linking (traceability) at this level of detail means it is much easier to identify relevant elements of the safety case that need to be re-examined in the light of changes to the system.

Legacy systems being upgraded with modern technology, or adapted for reasons of climate change, are a particular example where many changes could be implemented and require significant assessment and documentation updates.

At the time of writing, developments in digital twins, cybersecurity, autonomous systems, and artificial intelligence are all 'in the picture'. Technical publications, as well as the news more generally, are now full of such stories. How safe will all these new systems be without full lifecycle traceability of their origins and builds, and a sufficient safety justification? How will they be accepted for use [by technical authorities, approval bodies, regulators and end users]?

Focus of the Workshop

The focus of the MoC workshop at SSS'25 was on how managing change relates to systems assurance and development / update / modification of safety cases. The discussion thus pertained to the design of systems and related processes, rather than organisational changes.

Attendee representation at the workshop included those who are currently working within, or who had previously worked in, sectors such as Healthcare, Energy (Nuclear, O&G), Transport (Rail, Aerospace, Maritime, Autonomous Vehicles), Defence, Retail (payment systems, Business Information Systems (BIS)), Process, Mining and Construction.

Ten had registered to attend the MOC workshop, but over twenty attended on the day. All had previously experienced, or were currently working through or considering, notable technical and/or cultural changes.

Participants were asked: What is important to your work or projects, or your industry sector?

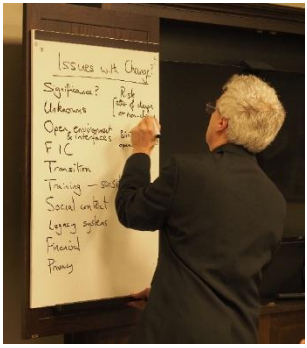
Pointers for discussions included:

- Discuss why managing changes is important, and even essential in some cases, what you need to achieve through managing changes, when you need to manage changes, who should be involved, and an outline approach
- Discuss the relationship of change management to version control and configuration management, its significance in safety-critical applications, and why it is more of a necessity in today's world of rapidly changing technology
- Organisations that adopt a continuous improvement methodology can be of concern. There is an argument that something that keeps changing is harder to assure. If anything, this tells us that it is even more important to manage change in such environments
- Changes are often related to safety, performance, reliability, or availability targets, or other KPIs; for example, tightened safety targets, or related to improved performance
- Functional change and upgrades are prevalent in industry

The following notes are a summary of the discussion, *supplemented with commentary in italics by the leader of the workshop.*

Issues With Change

It was evident that the general feeling of the group in the room – and by implication the safety engineering community – was that there are "issues" with change, with the concept of change, or of dealing with change.



This is believed to be due to the fact that safety cases, once finalised at each major stage gate of a project, tend to be "static". There is no "dynamic" approach to generating a safety case (noting that within safety cases, "dynamic hazards" may still be covered as part of the analysis). This aspect was thought as a fundamental point, almost a dilemma, behind many of the discussions. How can we deal with change if we don't have a dynamic safety case? *(it was thus very timely that one of the academic papers presented in the following session in the same room, the Young Engineer competition, covered exactly this topic!)*

Another fundamental observation was that many participants in the room did not immediately realise they were, in fact, working on changes. There is a school of thought that all developments, whether changes to an existing system or the creation of a completely new system, should be regarded and managed as changes. The argument is that even for a new system, this forces you to think about what changes will affect stakeholders and what will happen in the environment of the system. This approach can be very successfully applied to all sizes of systems.

The introduction of a change to a system or within a project introduces a change – or at the minimum a review – to the case for safety. *As we appreciate, lots of changes take place*

within projects, and also once systems are in-service, so on reflection it is no surprise that safety engineers have issues with changes, because every change that happens has to be scrutinised to a greater or lesser extent.

Other highlighted discussions have been grouped under the following headings:

The Change Itself

- Significant changes or the significance of the change. More significant changes tend to imply a significant amount of work required to update the safety case
- Risk of change. Either of the change itself or, conversely, of not doing the change
- Unknowns. Some changes can result in unknown, uncertain or unpredictable hazards. To pick these up, or at least reduce the likelihood of them, it's important to avoid group-think and have, for example, very diverse teams in HAZOPs (Hazard & Operability Studies) and design reviews. Workshops should occur before the change – SWIFT (Structured What-If Technique), HAZOPs etc. capturing the change, as well as the diversity of perspectives of the change. "Pre-mortem" rather than "post-mortem" should be the norm
- Unquantifiable changes. Not knowing the impact of greatest risk, which could be unquantifiable, is a concern (c.f. Rumsfeld Matrix)
- Innovation. It is accepted that changes due to innovation can be good; but innovation done badly can also result in potential harm. "Over-innovation" with lack of safety foresight was cited as a particular concern.
- FIC (first in class)/FOAK (first of a kind). Sometimes a change represents a "first". Something new in the operational picture, something added on for the first time, something innovative or wholly different to what was there previously. Managing FIC/FOAK is a particular challenge for safety analysts as there is often no or little comparable data, or similar systems or applications from where to draw confidence
- At the opposite end of the spectrum are changes to Legacy Systems – dealing with obsolescence, add-ons and updates to legacy systems, sometimes decades old (or in extreme cases, hundreds e.g. Victorian era railway tunnels being fitted with digital asset monitoring equipment)
- Reliance on tech. Over-reliance on technology was also noted, leading to loss of personnel or corporate knowledge

The processes around the change

- Anticipation of change. Anticipation of a forthcoming change is helpful, particularly for "intimidating" changes (for example, those regarded as significant in themselves, ones anticipated to involve a significant amount of work, or that could have a major impact in some form)
- Interoperability. Systems are becoming ever more integrated and inter-connected, and a push towards interoperability is a change in itself. Managing a shift towards interoperability can be complex, across boundaries, across operators, across countries and can put limits on what can be changed if interoperability is to be maintained
- Open environments and interfaces. Some changes result in open or larger interfaces

with other systems or environments. These can be hard to manage, or hard to control
- Operating environments. Major changes to operating environments (which often also include maintenance regimes) require significant management of change generally, and thus significant management of safety during the transition periods
- Changing environments due to climate change are already having impacts on systems design, and by implication, safety and dependability cases
- Transitions. These are situations where the change is effectively a shift, be that gradual, progressive or step-change, that requires attention and requires safety management, to enable the transition to happen safely
- Social context. Sometimes changes also have a social context e.g. accessibility
  Financial impact. Changes often have a financial impact
- Complement of stakeholders. A full complement of stakeholder should be identified as early as possible. There can be different drivers of/for change, and openness is required for safety reasons

Personal Impact

- Loss of agency. A few participants reported a loss of control or independence of their work when changes were made. It would be worth exploring why this happened or was perceived to have happened
- Training, sensitisation and awareness. Informing people that there has been a change to the system or operating environment is key to the success of the implemented system or update
- Privacy. In some circumstances, there are potential privacy, (personal) security or GDPA (general data protection act) issues alongside the system change
- Customer perspectives, including any surrounding deceptions (e.g. hyping or falsification of product claims), also need to be accounted for.

Regulation of Changes

Acceptability of the change – by an official safety approver/regulator, a business, operator, or the public etc (depending on system purpose) – becomes more difficult the more complex the change. Demonstrating the As Low As Reasonably Practicable (ALARP) principle is integral to acceptance of the change, and sometimes this (still) happens too late in the project lifecycle.

The group discussed regulation in several contexts.

- Regulatory changes on systems development
- Lagging regulations
- Regulating the unknown
- Advising the regulator

The latter three appear prevalent in the context of rapidly-shifting technologies and shifts in security threats (with safety implications).

Wrap-up

The reason many – if not arguably all – safety cases (and updates thereof), come about in the first place is due to some engineering or operational change or similar. It is certainly recognised in industry guidance that 'engineering change' is an instigator of the need for a safety case. An engineering change generally takes the form of a wider project, of course.

Safety engineers can be rather cautious about change and dealing with change. Designing for change at an early stage of project, alongside early involvement of the safety team, is preferred or essential. Safety is expensive retrospectively, but safety engineers are still often enough being called in too late in the lifecycle of a change.

Groupthink with not enough diverse thought can impact both the success of a change and its safety implications.

The why of the change, keeping evidence / audit trail and succession planning, are important. When changes occur, safety case managers and regulators are keen on experience, evidence, and being able to show that enough is in place to provide adequate assurance.

With rapid changes, standards and regulations may lag, which can cause delays or problems in presenting a good case for safety.

End Notes

Post-workshop, Wendy observed that *the workshop allocation was only an hour and, with more than double the number of people in the room than who had registered, the session became rushed.*

As the co-author of the originating paper behind this workshop (shortly to be published in the SCSC's e-journal), Keith Collyer provides the following post-workshop comment:

One thing that we did not make explicit in the paper and does not seem to have come out in the discussions is the need to define criteria for the change to be considered successful.

Wendy and Stephen concur that:

- *Further work (or workshop) includes looking at success criteria, including approvals*
- *The concept of static versus dynamic safety cases should also be given more consideration for future SSS presentations/workshops*
- *We need to develop tools for helping safety engineers to respond in a timely manner to the increasing pace of change*

Stephen remarked: *I look forward to exploring this more in a later session, because there's a lot to consider!*

The workshop was led by Wendy Owen (Independent Consultant), supported by Stephen Bull (Ebeni). Post-Workshop Review was by Keith Collyer (Independent Consultant, Systems Engineer).

Seminar: New Developments in Rail Safety Systems

This seminar *New Developments in Rail Safety Systems* will feature 6 technical speakers presenting new technologies for improving safety on the railways. It is aimed at rail practitioners working in safety engineering including Safety Engineers, Safety Consultants and Safety Managers.

It will be held at the Eurostars Book Hotel, Schwanthalerstraße 44, 80336 München, Germany, located in the centre of Munich, the Bavarian capital, next to the central railway station (Hauptbahnhof).

This seminar will be conducted in English. All times are Central European Time (CET), one hour ahead of GMT.

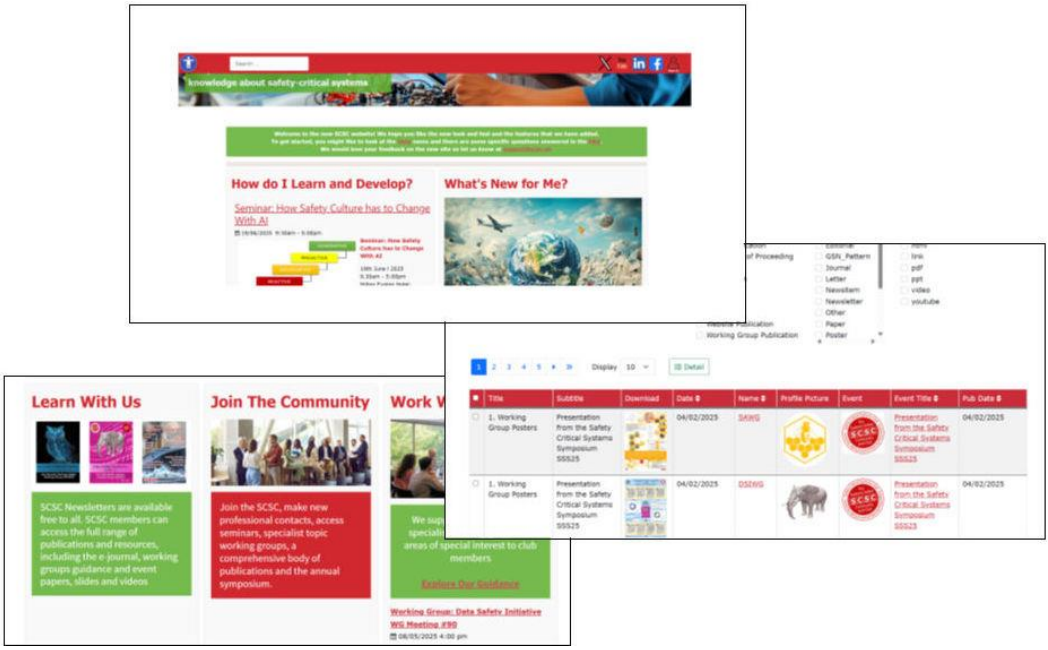
This seminar will be held in the normal SCSC format, with registration from 09:30 and talks starting at 10:00 (local time).

The cost will be €315 (€335 including 1-month's SCSC membership) with a student/retired rate of €35

Event Information

Event Date	04/12/2025 9:30 am
Event End Date	04/12/2025 5:00 pm
Individual Price	€315 (€335 including 1-month's SCSC membership) with a student/retired rate of €35
Location	Eurostars Book Hotel

New SCSC Website!



The SCSC has a new website! After over two decades of creating and running the SCSC's website, our current website master, Brian Jepson, has decided to pass on the reigns to give him more time for other pursuits. Paul Hampton describes how the club has used this transition to take advantage of many of the more contemporary website tools now available to make the management of the site simpler, and to introduce some great new user experience features.

In the Feb 2022 edition of Safety Systems, Brian Jepson described the fascinating story of how the SCSC website came about and how it has evolved over almost 25 years. The site has only existed through Brian's tireless efforts to craft, maintain and evolve the site and his extensive knowledge of the suite of languages and tools required to build and run a successful site. Its inception predates the modern frames such as Wordpress, Joomla and other commercial services such as Wix so the site was pretty much built by hand. It's hard to overstate the range of skills required to do this, not least: HTML, CSS, PHP, Javascript, XML, Regex and Linux. Clearly a very hard act to follow!

The approach has therefore been to leverage as much as we could from a modern framework and Joomla was chosen along with a number of extensions to help with functionality to support Events Booking and Membership Management. The components are mainly configuration driven with no or very little code required so they can be used with little or no training or technology skills.

With previous knowledge of setting up Joomla websites, I took the lead in designing the migration activities and Brian along with Alex King and Mike Parsons have collaborated closely on the functionality and look-and-feel of the new site. Thanks also to Stephen Bull, Chris Hobbs, Dave Banham and Phil Williams for providing early feedback on the prototype.

Old Features, New Style

The intention was to ensure we kept has much of the functionality and content of the previous site but to update the general style and presentation to give it a more contemporary feel. You can, for example, see the upcoming events and recent club news from the Home page as previously, book and pay for events and download resources. The Forums have not been left behind, and these along with most of the previous content have been migrated and more closely integrated with the website while retaining the same abilities for users to create and comment on posts.

Working Group content has also been migrated into the new website with all previous working group content being lodged and filed in a dedicated document management system. This system provides some new benefits such as document thumbnails, a document search facility and the ability to rate documents. Another functional reimagining is for the management of resources or in other words, the papers, presentation and videos provided by authors to support events such as seminars and the annual symposium. The content is largely unchanged but functionality has been added to make it easier to search and filter the thousands of resources accumulated over three decades of club operations.

New Features

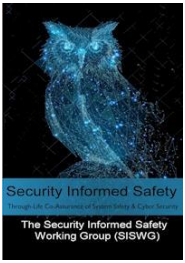
The new framework brings a number of new features more or less 'out of the box', such as a sitewide search facility and ability for authorised users to edit articles directly through the frontend application; this means that the job of maintaining the site can be distributed among many people.

Considerable work has also been done to help support Working Groups and in particular the Working Group Leads who can now:

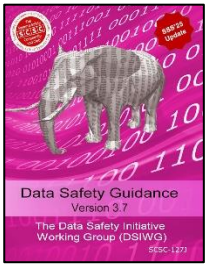
- maintain their own 'shop window' page for their group, that is, publicly available content to explain the purpose and objectives of the group and how to get more involved
- maintain a 'blog' for the group to make announcements about activities in the group
- create working group events to make users aware of future meetings and joining details
- list all the current users associated with a group

A new permissions model has been created to help support engagement with Working Groups. If users are interested in a working group, they can express this interest at registration or at any time by selecting 'Follow Working Groups'. Once a **Follower** of a group, the user can then see the Working Group Lead's blog covering latest developments and for example, details of future meetings. If more active engagement is sought then a Follower can get in touch with the Working Group Lead who can assign that user as a **Contributor**. A Contributor can then get full access to the Working Group document repository. This is useful if a user wants to review and contribute to guidance documentation while it is in development. Why not try the new site out at scsc.uk and we'd love to hear your feedback on the site at support@scsc.uk

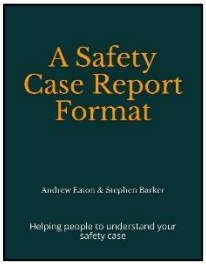
Recent Safety Publications



Through-life Co-Assurance of System Safety & Cyber Security (first issue)
scsc.uk/scsc-173



Guidance on the management of data safety risks (V3.7)
scsc.uk/scsc-127J



A Safety Case Report Format
Andrew Eaton & Stephen Baxter
www.amazon.co.uk/dp/B0DPL3C84P

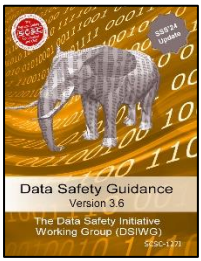
Safety-Critical Systems eJournal vol.3 no.2
Summer Issue 2024
scsc.uk/scsc-196

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

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

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

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



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

60 Seconds with ... Graham Jolliffe

Following a successful career as a Fleet Air Arm Air Engineer Officer, Graham has become recognised as one of the UK's leading Safety and High Integrity Software specialists. Graham has led a number of teams of Safety and software evaluators notably as the Technical Assurance manager for safety at QinetiQ Boscombe Down where he led a team of over 70 Safety Engineers who provided safety expertise for all military aircraft and associated systems. This led to him being awarded a Fellowship of the Royal Aeronautical Society.

He enjoyed many notable successes during his time in an engineering consultancy including acting as Thales' Safety Manager for the Chinook Mk6 Cockpit Display System and Mission Avionic System. Graham became freelance in 2013 and has continued to work on many interesting and diverse projects. These have included a safety review of QinetiQ's weapons testing facilities and providing safety advice to various aerospace companies including Boeing, Lockheed Martin, L3Harris and the Royal Navy. His most recent task was to provide a safety assessment of the Common Infrastructure for the new Dreadnought submarine for BAE Systems Combat Systems Directorate.

Graham is now semi-retired but continues to promote and explore new expedient methods of assessing System Safety and has contributed to a number of safety standards and guidance for which he has been commended. He has also taken an active role in a number of UK and International Safety organisations, including writing and presenting a number of papers for conferences and symposia.

What first attracted you to working in System Safety?

I was working with aircraft weapon systems in the mid 90's and having to determine whether the software had sufficient integrity to enable the weapons to be fired or released safely. This needed a 'systems' view to understand the interactions between software and hardware and the user. So, it was inevitable that I had to address 'system safety' rather than focus solely on the software.

So you've recently retired! How are you finding life outside of work?

I still have work to do with the SCSC as well as a long list of jobs from my wife. If ever I get near to completing them, I'm hoping to play a bit of golf and use my eMountain bike more often.

What aspect of your career are you most proud of?

I've been fortunate to have worked with a lot of very good people on interesting projects. None of us can do our jobs in splendid isolation so I am grateful for all the support and assistance I've received over the years.

Tell us one interesting unusual fact about yourself!

Difficult to choose one fact, but I was proud to represent Great Britain at shooting in South Africa in 1994.

What advice would you give to yourself age 12?

So, I already knew I wanted to join the Navy at that age and I was determined to achieve my qualifications to enable me to join when I left college. It was hard to keep focussed on achieving those qualifications when there were, as now, many tempting distractions. So I would say it's important to have a goal.

Which real-world role model do you get most inspiration from and why?

I would choose Nelson Mandela and Horatio Nelson as inspirational people simply because they inspire others through their leadership and example. What is particularly interesting is they come from completely different backgrounds. Horatio Nelson had a privileged upbringing, but was ahead of his time in recognising the needs of his men. They were well cared for judged by the standards of the day, and in turn, they performed much better than their enemy counterparts. Nelson Mandela had a much humbler background, but his self-sacrifice proved inspirational to millions especially during his incarceration. He could have been forgiven for wishing some form of redress once he had been released and elected president. Instead, he continued to lead by example by seeking reconciliation with his former adversaries.

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

I would love to be able to play a musical instrument but simply do not have the aptitude for it. I can only marvel at the ability of talented musicians.

Artificial Intelligence – a positive revolution or are we all doomed!

Probably the answer is both although there is already software purporting to be AI when it isn't. We are all aware of the benefits the internet has brought in recent decades, but now we are also seeing how it's misuse can have devastating effects on members of our society. The same is likely to be true for AI. It does offer the potential to reduce the possibility of human error, but we have already seen many examples of the adverse side. It's difficult to know how to guard against such threats. I know there is a lot of research being undertaken in this area, but it feels that our current system safety toolkit is inadequate as things stand.

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.

The working group recently published its first piece of guidance: Co-Assurance of Safety and Security and presented a poster at the SCSC.

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.

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.

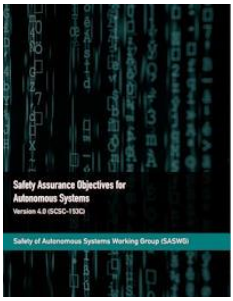
The group published guidance v4.0 in Jan 2024: scsc.uk/scsc-156D

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.



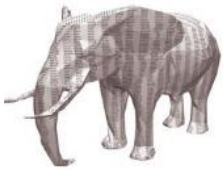
The working group was kicked-off at SSS'24 and is led by Alan Simpson. The SAIWG will conduct regular meetings, workshops, and publications to share knowledge and experience on various topics related to AI and safety systems, such as coordination of safety with other disciplines, evaluation of risk,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

For specific details on SASWG contact: **Philippa Ryan** pmrc@adelard.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 (v3.7) was published in Jan 2025: scsc.uk/scsc-127J

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 statement of the problem:

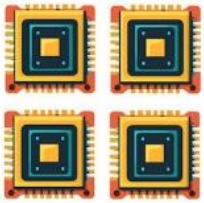
- It is acknowledged that complex systems are becoming more prevalent with more opportunities to cause harm
- There are also new complex systems arising from using combinations of existing systems and services which are then used for safety purposes
- Complex systems are not sufficiently addressed in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

The group produced the first version of Guidance on the Through-Life Assurance of Complex Systems (scsc.uk/scsc-200) in January 2025.

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. https://scsc.uk/r189:1

The upcoming seminar on 19th June 2025 in London will focus on how Safety Culture practices need to change to accommodate Artificial Intelligence. See page 18 and scsc.uk/e1156 for further details.

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.

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 **Khadijah Khatun** khadijah.khatun@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

We have great pleasure in announcing the formation of a new working group aiming to cover Safety Management and also Safety Management Systems so will have the acronym (SMSWG). 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 will be led by Si Hays so get in touch with him if you want to find out more about the group.

Lead **Si Hayes** 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, the SCSC Newsletter and access to presentations and other resources from events.

Individual Membership

To become an individual member of the SCSC please register on the SCSC website using the Home submenu option of "Register" (click on the triangle icon next to the Home menu option). Complete and save your account registration and then verify your email address. Once registered and logged in, select the Membership menu option to explore the various membership packages.

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

Corporate Membership

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

Renewing Membership

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

Membership Fees

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

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

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

We also offer free membership for three months for all those who give presentations at Seminars and Symposia.

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


Jane Fenn
jane.fenn@scsc.uk


Paul Hampton
paul.hampton@scsc.uk


Louise Harney
louise.harney@scsc.uk


James Inge
james.inge@scsc.uk


Brian Jepson
brian.jepson@scsc.uk


Khadijah Khatun
khadijah.khatun@scsc.uk


Alex King
alex.king@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


Roger Rivett
roger.rivett@scsc.uk


John Spriggs
john.spriggs@scsc.uk


Sean White
sean.white@scsc.uk

Honorary Members


Tom Anderson


Robin Bloomfield


Dai Davis


Graham Jolliffe


Tim Kelly


Felix Redmill


Phil Williams

Club Positions

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

Managing Director

Mike Parsons 2019-

Tim Kelly 2016-2019
Tom Anderson 1991-2016

Steering Group Chair

Dewi Daniels 2024-

Roger Rivett 2019-2024
Graham Jolliffe 2014-2019
Brian Jepson 2007-2014
Bob Malcolm 1991-2007

Programme & Events Coordinator

Mike Parsons 2014-

Chris Dale 2008-2014
Felix Redmill 1991-2008

Manager

Alex King 2019-

Honorary Solicitor

Dai Davis 2022-

Newsletter Editor

Paul Hampton 2019-

Katrina Attwood 2016-2019
Felix Redmill 1991-2016

University of York Coordinator

Mark Nicholson 2019-

Website Editor

Paul Hampton 2025-

Brian Jepson 2004-2025

eJournal Editor

John Spriggs 2021-

Administrator

Alex King 2016-

Joan Atkinson 1991-2016

Diversity, Equity and Inclusion (DE&I) Lead

Louise Harney 2024-

Wendy Owen 2023-2024

Safety Futures Initiative Leads

Khadijah Khatun 2024-

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

Calendar

May '25

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

June '25

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

July '25

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

August '25

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

September '25

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

October '25

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

November '25

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

December '25

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

January '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	

February '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	

March '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

April '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			

Events Diary

16 May 2025
Working Group Meeting

Working Group: Data Safety Initiative WG Meeting #90

Zoom from 4pm to 5.30pm

scsc.uk/e5018

2 June 2025
Working Group Meeting

SISWG Regular Teams Call

Teams from 1pm to 2pm

scsc.uk/e5036

12 June 2025
Working Group Meeting

Working Group: Safer Complex Systems WG meeting #19

scsc.uk/e5019

10-13 June 2025
Conference
Paris, France

AEiC 2025: 29th Ada-Europe Int. Conf. on Reliable Software Technologies

scsc.uk/e1114

16 June 2025
Working Group Meeting

SISWG Regular Teams Call

Teams from 1pm to 2pm

scsc.uk/e5037

15-19 June 2025
Conference
Stavanger, Norway

ESREL SRA-E 2025: 35th European Safety and Reliability Conf.

esrel2025.com

19 June 2025
SCSC Seminar
London, UK

How Safety Culture has to Change With AI

scsc.uk/e1156

23-26 June 2025
Conference
Naples, Italy

DSN 2025: 55th IEEE/IFIP Int. Conf. on Dependable Systems and Networks

dsn2025.github.io/

30 June 2025
Working Group Meeting

SISWG Regular Teams Call

Teams from 1pm to 2pm

scsc.uk/e5038

14 July 2025
Working Group Meeting

SISWG Regular Teams Call

Teams from 1pm to 2pm

scsc.uk/e5039

28 July 2025
Working Group Meeting

SISWG Regular Teams Call

Teams from 1pm to 2pm

scsc.uk/e5040

4-6 Aug 2025
Conference
Chania, Crete, Greece

IEEE Int. Conf. on Cyber Security and Resilience

www.ieee-csr.org

9-12 Sept 2025
Conference
Stockholm, Sweden

SafeComp 2025: 44th Int. Conf. on Computer Safety, Reliability and Security

safecomp2025.se

9 October 2025
SCSC Seminar
Brussels, Belgium

Complying with the EU AI ACT: What is needed for Products and Systems?

scsc.uk/e5003

4 December 2025
SCSC Seminar
Munich, Germany

New Developments in Rail Safety Systems

scsc.uk/e5004

10-12 February 2026
SCSC Symposium
York, UK

Safety-Critical Systems Symposium 2026

scsc.uk/e10

thescsc.org/membership

Invitation to submit an abstract for a presentation

34th Safety-Critical Systems Symposium

February 10-12th 2026, York, UK

Suggested topics are:

www.scsc.uk/sss

Accident Analysis
Agile Methods
AI
Autonomy
Airworthiness
Analyses
Assurance Cases
Architectures
Autonomous Vehicles
Certification
Complex Systems
Data Safety
Devops
EMC/EMI
Environmental Safety
Human Factors
Machine Learning
Methods and Tools
Model-Based Techniques
Multicore / Manycore
Ontologies / Formalisms
Regulation
Resilience
Robotics
Security / Cyber
Safety Culture
Safety Management
Safety Practice
Services Safety
Software
Standards and Guidance
Through-Life Safety
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 2025**
Authors notified if their abstract has been accepted	**by 31st July 2025**
Authors submit their paper for inclusion in the proceedings book	**by 30th Sept 2025**
Review comments fed back to authors	**by 30th Oct 2025**
Final versions of papers submitted	**by 31st Nov 2025**

If you would like to give a tutorial, run a workshop or present a poster at SSS'26, please contact mike.parsons@scsc.uk for further information