

This is a repository copy of *Safe, Ethical & Sustainable: A Mantra for All Seasons?*.

White Rose Research Online URL for this paper:

<https://eprints.whiterose.ac.uk/184111/>

Version: Published Version

Article:

McDermid, John Alexander orcid.org/0000-0003-4745-4272 (2022) *Safe, Ethical & Sustainable: A Mantra for All Seasons? Safety Systems.* pp. 5-10.

Reuse

Items deposited in White Rose Research Online are protected by copyright, with all rights reserved unless indicated otherwise. They may be downloaded and/or printed for private study, or other acts as permitted by national copyright laws. The publisher or other rights holders may allow further reproduction and re-use of the full text version. This is indicated by the licence information on the White Rose Research Online record for the item.

Takedown

If you consider content in White Rose Research Online to be in breach of UK law, please notify us by emailing eprints@whiterose.ac.uk including the URL of the record and the reason for the withdrawal request.

The Safety-Critical Systems Club Newsletter

Safety Systems

Vol 30 No. 1 - Feb 2022

**3 DECADES OF
SAFER SYSTEMS**

**Celebrating 30 years
of the SCSC**

**FUTURE
PERFECT?**

**A new mantra for
safety, ethics and
sustainability**

**BACK TO THE
FUTURE**

**Where we're going,
we don't need roads...**

For everyone working in Systems Safety



thescsc.org

Cover image: 3564425 © Bcon Management Inc. | Dreamstime.com

Contents

WELCOME

Editorial

3

Opening words from the SCSC Newsletter Editor.

In Brief

4

Recent system safety news items from around the world.

FEATURES

Safe, Ethical & Sustainable: A Mantra for All Seasons?

5

Prof. John McDermid discusses some new models and thinking for the future of systems safety.

View From The Desk – 30 years of the SCSC

11

Tom Anderson and Joan Atkinson, share some history and memories of the SCSC over the last 30 years.

The Future of Human Factors?

21

John Ridgway provides his views of one possible future for Human Factors.

Planes and Computers

25

Stan Price reflects on his own personal journey in system safety through the years.

The SCSC and the Internet

29

Brian Jepson describes the history and evolution of the SCSC website.

The Future of Safety Engineering & Assurance

29

The SCSC Steering Group give their predictions for the future!

REPORTS

Seminar Report: Can We Quantify Risk?

Mike Parsons

37

Seminar Report: Safe Use of Multicore

Lee Jacques

43

Safety Futures Initiative Update

Zoe Garstang

47

60 Seconds with ... Dr Mike Parsons

55

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

GROUPS

Working Groups

Details of the SCSC Working Groups.

51

SCSC Steering Group

58

Who's who in the Steering Group.

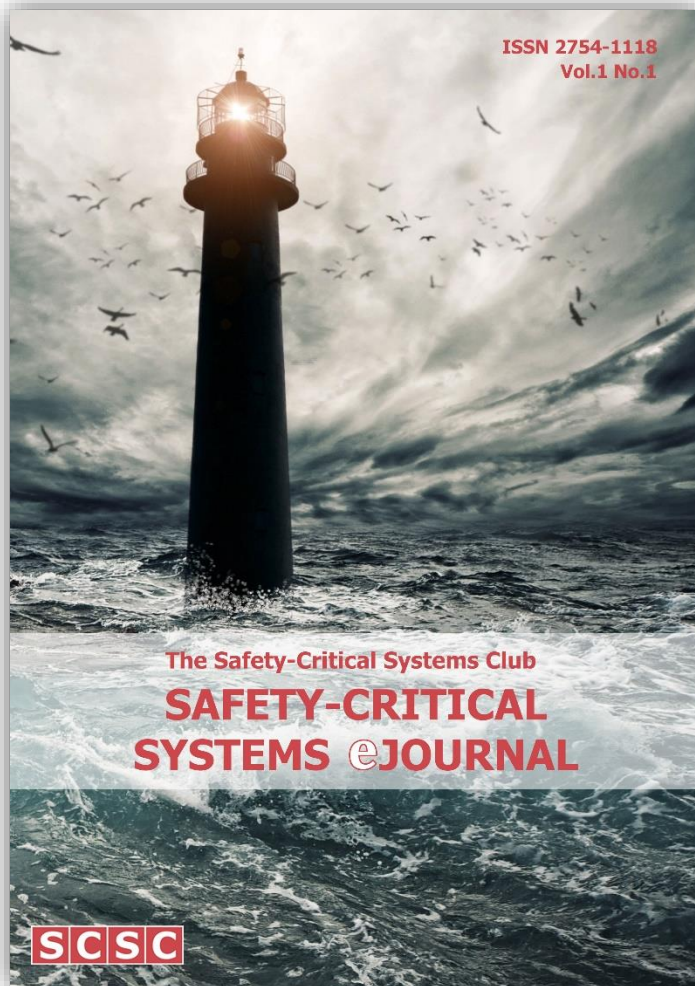
EVENTS

Calendar

60

Events Diary

61



The new Safety-Critical Systems eJournal is our latest peer-reviewed publication, containing a blend of industrial papers and academic research results on all aspects of system safety, including the practical aspects – what works and what does not.

Initially, there will be two issues per volume, published in January and July of each year. In addition to the on-line presentation, each Volume of the journal will be made available in printed form each December.

The first issue is out now at <https://scsc.uk/journal>

If you would like to submit a paper for a future issue, please see "Information For Authors" in the right-hand pane of the journal home page.

Editorial

The SCSC celebrates its 30th Anniversary!

It's remarkable to think that we are now embarking on the 30th volume of the SCSC newsletter, and this month sees the SCSC host its 30th Safety-Critical Systems Symposium (and there's still time to register for the event being held in Bristol and online scsc.uk/e797!)

The club has certainly come a long way in those three decades; it's interesting that many of the standards that are very familiar to us now, like DO-178 and IEC-61508, simply weren't in existence when the club had its inaugural meeting in 1991. Given the unsurpassed attendance at that meeting, there was clearly acknowledgement that there was work to be done, but I suspect there was great uncertainty in what that work was, and what the future had in store. Nevertheless, the club has undoubtedly contributed to a safer world, not only in sharing knowledge of current best practice in system safety, but also in shaping what best practice actually looks like. All of which is certainly a cause for celebration!

The theme for this anniversary edition of the newsletter could be expressed as 'Back to the Future', taking both a backward and forward look at system safety. We will therefore, reflect on the journey the club has taken since its inception along with other historical and more personal accounts, and also look to the future; setting out ideas on how the club could position itself to shape and ensure safer systems for the next 30 years.

Our series of backward-looking articles begins with Tom Anderson and Joan Atkinson, who were key to running the club for most of the club's lifetime. They reflect on the last 30 years of the SCSC and share some history of its formation and entertaining memories of the club's activities and events. This is complemented with an article from Brian Jepson, our webmaster, who describes the evolution of the SCSC website. Stan Price also reflects on his own personal journey in system safety through the years, from those early times when the dependency on computers for safe operations in aircraft was only just being realised.

Our series of forward-looking articles begin with an article from Prof. John McDermid, describing his vision for the role and scope of safety engineering and assurance in a world where wider issues such as ethics and sustainability can no longer be considered separately from traditional safety engineering concerns. John Ridgway presents his vision of the future of Human Factors in his article, and we conclude with a more speculative look at what the future holds as predicted by some of the SCSC Steering Group members.

We also have reports from events held last year on the quantification of risk and the safe use of multicore, and Zoe Garstang provides an update from the Safety Futures Initiative – helping develop the engineers that will be making systems safer over the next three decades.

The future is, perhaps, less murky than it was all those years ago; this gives us more empowerment to shape it, but it also means we are troubled by what we see ahead, especially in relation to wider issues such as climate change. We have come a long way but there is still a long way to go, and there certainly is still much work to be done.

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



In Brief



Covid-19: Researcher blows the whistle on data integrity issues in Pfizer's vaccine trial



Revelations of poor practices at a contract research company helping to carry out Pfizer's pivotal Covid-19 vaccine trial raise questions about data integrity and regulatory oversight. [bmj.com](https://www.bmj.com)

Drone Helps Save Cardiac Arrest Patient in Sweden



For the first time in medical history, a drone has played a crucial part in saving a life during a sudden cardiac arrest. The world unique achievement took place in Sweden when an Everdrone autonomous drone delivered a defibrillator that helped save the life of a 71-year-old man. uasvision.com

Smart motorway rollout suspended amid safety concerns



The rollout of smart motorways has been suspended by the government until at least 2025 in response to safety concerns from MPs and motoring groups. [theguardian.com](https://www.theguardian.com)

Collision between passenger trains at Salisbury Tunnel Junction

Preliminary findings from the investigation of the collision involving two west-bound passenger trains at Salisbury's Fisherton Tunnel in October 2021, concludes that the failure of one train to stop at a red light was almost certainly a result of low adhesion between the train's wheels and the rails. gov.uk



Tesla driver charged with vehicular manslaughter over fatal Autopilot crash



California prosecutors have filed two counts of vehicular manslaughter against the driver of a Tesla on

Autopilot who ran a red light, slammed into another car and killed two people in 2019.

The defendant appears to be the first person to be charged with a felony in the United States for a fatal crash involving a motorist who was using a partially automated driving system. [theguardian.com](https://www.theguardian.com)

Safe, Ethical & Sustainable: A Mantra for All Seasons?



John McDermid provides some guiding principles on how to achieve and manage the safety of complex systems whose failure causes and consequences go beyond the concerns of traditional safety engineering. He sketches some new models for safety engineering and proposes the adoption of the mantra “safe, ethical and sustainable” to not only focus the attention of the community on the key issues, but also to influence politicians and policies.

There are many principles and “laws” relevant to systems and safety engineering. At a time when the community is grappling with systems of unprecedented complexity I am reminded of Mencken’s Law:

“For every complex problem, there is a solution that is clear, simple, and wrong.”

There is also the famous [1]:

“All models are wrong, some are useful.”

And two further (related) quotes, the first from Humpty Dumpty:

“When I use a word, it means just what I choose it to mean — neither more nor less.”

“Words in their primary or immediate signification stand for nothing but the ideas in the mind of him that uses them.”

The latter, less well-known perhaps, is from John Locke [2] and may have been the source of Lewis Carroll’s ideas for Humpty Dumpty’s scornful remark to Alice [3].

Why do I quote these? I want to suggest some new models for how we think about complex problems, with a particular emphasis on safety. These models will be wrong in some facet or some situation, but they will be useful if they help focus thought in a constructive way. And all I have is words. My aim is to convey the “ideas in the mind ...” – but perhaps if they are repeated often enough (like a mantra) they will start to have significance in other minds too. But I start with the usage of a word which I sort of hate.

Elegance in Systems Engineering

Systems engineering has long been presented as a multi-disciplinary, or trans-disciplinary approach to solving complex, multi-faceted problems. To me 'elegance' means being 'graceful or stylish' but the systems engineering community has hijacked it to mean [4]:

- Efficacy – how well does it achieve the desired outcomes?
- Efficiency – how economical is it in use of resources both to develop and to operate it?
- Robustness – how well does the system perform in unanticipated circumstances?
- Minimising unintended consequences – how well does the system do in reducing unwanted and unanticipated consequences?

The aim – akin to mine here – is to give some guiding principles to help achieve focus on the key issues when trying to solve complex problems. I accept that some systems can be elegant, but I think the complexities of modern systems, the difficulties of dealing with brownfield systems design, the interconnectedness and interdependencies of systems, and the fact that efficacious and robust solutions can be downright ugly, makes me think this is a somewhat naïve characterisation. The four principles seem sensible, but I sort of hate the label 'elegant'. Overall, I view this as a good example as it indicates the kind of models I want to create – guiding principles that are useful, although wrong in some sense.

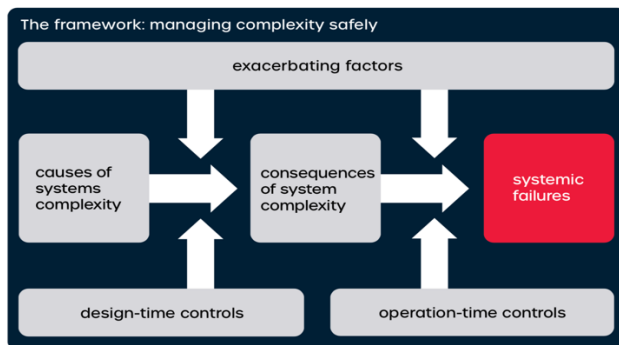
Complex Systems

I have used the term 'complex systems' several times. What do I mean by this? It is common to make a distinction between complicated and complex systems, saying that complex systems exhibit 'emergent properties', that is, properties of the whole that are not simply properties of the individual system components (and their inter-relationships). Some argue that this definition is unscientific – but science doesn't have the answers to everything – moreover, according to Aristotle [5]:

"In the case of all things which have several parts and in which the totality is not, as it were, a mere heap, but the whole is something besides the parts."

I hope I may be excused for relying on this unscientific definition, since the implied uncertainties of 'emergence' indicate one of the key challenges we need to face in safety engineering. We can't assume that the system development will produce results that safely manage all these uncertainties from 'day one', thus we also need to consider the overall governance of the systems in deployment, to identify unintended consequences, to learn from them and provide feedback to improve the system. To me this is another reason that the notion of 'elegance' in systems is somewhat naïve – it implicitly assumes that the system can be designed to achieve its intended use 'full stop'. The reality is, however, that we need to produce systems that are 'good enough' (safe enough) that we can deploy them and then manage them to achieve acceptable safety through life, recognising that what is acceptable may change over time, as technology or society's expectations evolve.

A study on Safety of Complex Systems for the Royal Academy of Engineering [6] introduced a model of how complexity, as opposed to mechanistic failures, contribute to systemic failures, see the figure. It shows the role of both design-time and operation-time controls for reducing the likelihood of systemic failures, or for mitigating the consequences. The exacerbating factors are those issues that can have adverse impacts, particularly on the controls.



The study also introduced a three-layer model for governance of such systems spanning:

- Governance – cross-jurisdictional incentives and requirements for organisations to adhere to best practice through regulations, standards, soft law, etc.
- Management – risk control and trade-offs in an organisation, management of supply chain dynamics and the sustainment of long-term knowledge
- Task & Technical – the behaviour of the technological elements of the system, the users and other stakeholders, in their context of use

The task & technical level is the traditional province of safety engineering (and it seems the main focus of the work on elegance in systems engineering), but it is insufficient to address and manage the problems of complex systems. The report presents some examples of using the framework, showing the issues in the governance, management and task & technical levels, for each of the elements in the model – causes of complexity, exacerbating factors, etc. For example, in the case of the Uber Tempe accident [7] we can see:

- Exacerbating factor (management layer) – casualisation of labour, using untrained safety drivers (gig economy)
- Causes (task & technical) – mentally unstimulating but critical tasks of system supervision

This work provides two key aspects of the broader models – ways of thinking about systemic failures arising from complexity, and the need to consider causes and controls at the levels of management and governance, as well as those within the more traditional scope of safety engineering. It also highlights the need to consider safety management through life; of course, this is not new, but treating safety management as a continuum rather than having a discontinuity as the system enters service is at least a new emphasis.

Benefits and Harms

Safety mainly focuses on harms to people, i.e. death and injury, and ways of reducing the attendant risk. Of course, benefits are considered, albeit in a simplistic, or limited way. For example, a cost benefit analysis can be used to support a claim that a risk has been reduced As Low As Reasonably Practicable (ALARP). This however is a narrow application focused on risk reduction and doesn't consider the wider societal advantages or benefits of having the system in the first place.

Thus, the proposed shift in our models of safety is to consider benefits as well as harms in all aspects of the design and analysis of systems. In terms of models, this requires definition of a trade-space of benefits and harms that should be considered in designing and analysing systems. This should be much broader than the conventional focus of safety engineering on harm to individuals and should include consideration of society and the environment. A challenge is the need to trade-off between incommensurable factors; this is not easily resolved but doing pairwise comparisons between designs that are close in the trade-space is one possible tactic.

Individual, Societal and Environmental

Although broadening models, it is still desirable to take a human-centric approach, and thus I use well-being as an ‘umbrella’ [8]. In this content, it is possible to divide benefits and harms into three categories: individual, societal and environmental, with examples of potential benefits and harms shown in the table below. These are intended to be illustrative, and the factors to be taken into consideration would need to be identified for a specific system.

Although broadening [safety] models, it is still desirable to take a human-centric approach

	Benefits	Harms
Individual	Personal autonomy Health	Physical injury Mental illness
Societal	Safe working environment Equitable access to resources	Social exclusion Inequitable risk distribution
Environmental	Biological diversity Clean water	Warming of the atmosphere Plastic build-up in the oceans

Many of these benefits and harms have an ethical dimension. For example, if introducing autonomous vehicles net reduces the level of fatal accidents on the roads but does not give any decrease in the number of fatalities for cyclists, then this would be a case of inequitable risk distribution. To be fair to the systems’ engineers, this could be seen as an interpretation of what they meant by ‘efficacy’ and ‘minimising unintended consequences’.

Many of these benefits and harms have an ethical dimension

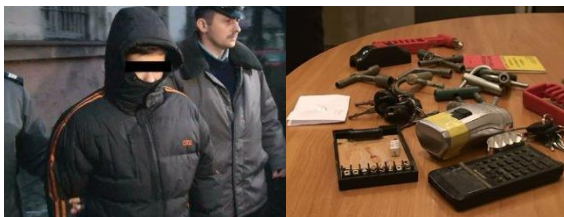
The shift in terms of models supporting safety engineering should be clear – but, maybe now, beginning to seem like ‘scope creep’ on a global scale!

Toujours L’Attaque Surface

A large proportion of modern engineered systems utilise computer-based control, and many have high degrees of interconnectivity. Communication between systems and between systems and the infrastructure, can help in terms of efficacy and efficiency, but it opens up possibilities of cyber-attacks. Napoleon was famous for saying ‘toujours l’attaque’ (always attack).

I am advised by people who run industrial and public infrastructure that this idea is alive and well in the “hacker community”, and that their systems are under continuous attack. Highly connected systems present a large attack surface, and poor security controls in one part of the overall system may enable access to more critical parts.

As an illustration, the figure shows a teenage boy and the TV remote control that he modified and then used to move points under a tram in Lodz, Poland, causing a derailment.



A further example is the 2001 attack on the Maroochydore sewage plant in Queensland, Australia which released about 1 million litres of sewage [9]. These incidents show the need to consider the interaction of security and safety and there are now many proposals for combined approaches to security and safety analysis, including some focused on early-stage design [10].

Perhaps controversially, I am of the view that the *risks* from cybersecurity are relatively low. The likelihood of attacks on many systems is high, but the probability of success is quite low and the more complex the system, the less likely the attacks are to succeed; in the Maroochydore case, the attacker was a disgruntled former employee, i.e. had inside knowledge. Thus, the models need to include cyber-security, to address means to reduce the potential attack surface and to provide effective security controls. This will reflect legitimate societal concern, but the focus should be on security in the role of its contribution to safety [10].

Safe, Ethical and Sustainable

If we were to draw together the models I have hinted at above, and also provide the supporting detail, e.g. in terms of analysis methods, then it would be clear that they are very complex; indeed, there are over 100 elements in the Safety of Complex Systems framework alone and the other models are multi-dimensional too.

It is not easy to produce a good summary – or mantra – but I propose “safe, ethical and sustainable”. Safe – the primary focus continues to be on individual health and safety. Ethical – as new systems exhibit increasing levels of autonomy, moving decision-making from humans to machines, there are many issues including the potential for unfair distribution of risk or, unjustifiably, holding someone liable for outcomes which are beyond their control. Sustainable – due to the importance of sustainability in itself, and the human and societal effects of environmental damage; for example, global warming is already a major source of individual harm [8]. This aligns with the focus on individual, societal and environmental benefits and harms.

It is not easy to produce a good summary – or mantra – but I propose “safe, ethical and sustainable”

Perhaps it is better to view this as a question – repeatedly asking if a system being designed or used is ‘safe, ethical and sustainable’ won’t immediately suggest all the details of the models I have alluded to, but it is a prompt and a route into those models.

Conclusions

I believe that safety engineering is at a crossroads. It needs to adapt to the complexities of current and emerging systems and to societal and environmental issues such as the impact of global warming. Some might argue that this is too big a change in role for the community, and I would view it as a target to strive for, not as an immediate objective. However, there is one immediate objective which I believe the community needs to adopt.

Bolt's "A Man for All Seasons" [11], focuses on the struggle between Henry VIII and Sir Thomas More, the chancellor, over issues of religion, power, and conscience. Whilst religion is outside our concerns here, being the 'conscience of power' and drawing to the attention of politicians not only the harms that complex systems can bring, but also their benefits, is something to which the community can, and I believe should, contribute.

I am pleased to see the Royal Academy of Engineering taking a lead in respect of the role engineering can play in reducing (the impact of) global warming. I see a similar model for safety engineers. If we consistently and persistently use the phrase 'safe, ethical and sustainable – treating it as a mantra (for all seasons) – this might begin to resonate with those in power and thus enable the safety engineering community to shape the future in a positive way, something we have perhaps not been good enough at in the past.

References

- [1] G. Box, "Robustness in the Strategy of Scientific Model Building", 1978.
- [2] J. Locke, "An Essay Concerning Human Understanding" (1689). Various reprints.
- [3] L. Carroll, "Through the Looking Glass" (1871). Various reprints.
- [4] M. D. Griffin, "How Do We Fix System Engineering?", 61st International Astronautical Congress, Prague, Czech Republic, 27 September – 1 October 2010, pp. 1-9.
- [5] Aristotle, "Metaphysics", (See: W.D Ross et al. Aristotle's Metaphysics. Oxford University Press, 1925, pp 8-10.)
- [6] "Safer Complex Systems: An Initial Framework", <https://www.raeng.org.uk/publications/reports/safer-complex-systems> (2020), accessed November 2021.
- [7] National Transportation Safety Board. "Collision Between Vehicle Controlled by Developmental Automated Driving System and Pedestrian Tempe, Arizona March 18, 2018". (Published 2019).
- [8] J.A. McDermid, Z Porter, Y Jia, "Consumerism, Contradictions, Counterfactuals: Shaping the Evolution of Safety Engineering", Safer Systems: The Next 30 Years, Proceedings of the 30th Safety-Critical Systems Symposium (SSS'22), 8th -10th February 2022, SCSC-170 (Published 2022).
- [9] Maroochy sewage spill: <https://www.risidata.com/Database/Detail/maroochy-shire-sewage-spill>, accessed November 2021.
- [10] J.A. McDermid, F. Asplund, R.Oates, J. Roberts, "Rapid Integration of CPS Security and Safety", IEEE Embedded Systems Letters (2018).
- [11] R. Bolt, "A Man for All Seasons", Vintage (1990).

Image attribution

Lead image: ID 163537157 © Savagerus | Dreamstime.com. Lodz derailment: credit policja.pl

John McDermid Professor of Software Engineering and Director of the Assuring Autonomy International Programme (AAIP) at the University of York

John McDermid has worked on safety of computer-controlled systems for about 40 years and now leads the AAIP, focusing on the safety of robotics and autonomous systems, including those using machine learning. He has acted as an advisor to industry and government internationally and contributed to the development of standards. He is currently engaged on work on the safety and ethics of autonomous vehicles. He has supervised about 40 PhD students and published around 450 papers. He is a Fellow of the Royal Academy of Engineering and was awarded an OBE in 2010.

View From The Desk – 30 years of the SCSC



Tom Anderson and Joan Atkinson were key to the running of the Safety-Critical Systems Club for the best part of three decades. They often sat 'behind the desk', managing proceedings and ensuring the (mostly!) smooth operation of events. Tom and Joan reflect on the last 30 years of the Club and share some history of its formation and memories of the Club's activities and events.

*A long, long time ago
I can still remember*

These opening words to American Pie (Don McLean, 1971) refer to February 3, 1959, *the day the music died*, which was only just over 12 years earlier. In this article we will look back over the formation and activity of the Safety-Critical Systems Club, established in 1991 (with some reference to prior art going back to 1984) – so that's reaching back 30 years and more. As a result, to tell the truth, we don't now "still remember" lots of stuff.

Furthermore, if you're after good solid technical recollections of the evolution of principles and practice in engineering software-intensive systems for safety-critical applications, you won't find them here. Fortunately, the back catalogue of this Newsletter: *Safety Systems* and the proceedings of the *Safety-Critical Systems Symposium (SSS)*, published annually since 1993, comprehensively cover that deficiency. Indeed, in Volume 25, Number 3 of *Safety Systems*, you can read an excellent overview [1] of the first 25 years of the *Safety Club*, to use the familiar colloquial abbreviation.



Instead, we plan, basically, to gossip about those earlier times, as we watched (and, of course, shared in) the successful development of the Club; we hope you'll find some nuggets of interest in what is a somewhat discursive, and very informal, memoir.

How it all began



Way, way back, in the early 80s, concerns in industry and academia about the all too often highly unreliable behaviour of software, led to the formation of a national group (these days it might be labelled a focus group) of individuals which – after a pause for reflection – took the name Centre for Software Reliability (CSR). Needing a formal underpinning for this group, Bev Littlewood (at City University) and Tom Anderson (at Newcastle University) established two university research centres, also named CSR. The main focus at

CSR (City) was on the assessment of software reliability, whereas CSR (Newcastle) concentrated on reliability achievement. This proved to be a timely initiative, since shortly afterwards the UK Government's Alvey Programme [2] drew active support on both of these topics from CSR.

An early CSR action had as its aims: to increase awareness of the need for more reliable software, to disseminate techniques for assessing and achieving it, and thereby stimulate improvements. The vehicle set up to deliver this was called *The Software Reliability and Metrics Club*, which created a Newsletter and a series of seminars (mostly one day, but some were longer); the inaugural meeting was held in London in October 1984, with over 100 delegates participating. The SRMC operated for just over two decades, but closed down after a total of 68 events – the final seminar was held in November 2005.

So now let's move on to the late 80s. Programmable electronic systems were by then moving rapidly, maybe too rapidly, into every sector, and the implications for public safety were becoming apparent to many. National awareness and concern led to a formal call – funded by the (then) Department of Trade and Industry (DTI) and the Engineering and Physical Sciences Research Council (EPSRC) – for proposed initiatives that could help to ameliorate the added risks that computers and, especially, their software could generate in embedded systems.

CSR took the view that, with national support, an upgraded version of the Software Reliability club could make a significant contribution in the safety arena. Responding to the call demanded a substantial proposal document; as usual this was completed with frenetic effort as the submission deadline approached. [We cannot forget Joan faxing long supplementary sections of text, prepared by Robin Bloomfield, out to Tom's hotel reception desk in the USA – yes, by fax, onto continuous-roll, heat-sensitive paper – cutting edge technology!]

After a competitive presentation, a contract was awarded for the formation of a *Safety-Critical Systems Club* (formally awarded to the BCS, on behalf of BCS plus IEE, with CSR to receive all the funding and do all the work). Financial support was tapered over three years, with the Club to meet specific targets and be self-sufficient when support ended.

The very first Safety Club meeting was held in July 1991, as a component of a DTI conference in Manchester. The issues to be addressed by the Club were seen to be a key concern for the conference delegates – 256 attended this launch meeting, requiring it to be switched out of the small room originally planned to the main auditorium. In fact, this remains the Club's highest attendance count (the next highest were 213 for the first SSS of the 20th century in 2001, and 205 for "Standards in SCS" – a 2-day event held in Cambridge in 1992).



At this point we would like to recall the dedication and commitment of the Safety Club's first "Coordinator": Felix Redmill. From the outset and for 25 years thereafter, the Club benefitted from his knowledge, experience, contacts and single-minded pursuit of the best possible event programmes, presentations and newsletters. Only ill-health now prevents Felix from continuing to intervene in the interest of the Club's objectives. However, we have been very fortunate in subsequently gaining from the new ideas and approaches delivered by his successors – Claire Jones, Chris Dale and the current enthusiast: Mike Parsons (from 2014 onwards). And in August 2016 we gratefully handed over responsibility for managing the Club to Tim Kelly, working with Alex King, at the University of York.

Some facts and figures

By January 1995 our membership database held contact details for around 2,500 members; all were recorded as individuals, but about 100 were included as part of a corporate package with their employers. [The corporate arrangement provided fully paid membership status at a group discount – the reduction in revenue for the Club was offset by the opportunity to renegotiate the group packages annually.] By promoting these group packages we increased the number covered to about 700 over the next few years, and although it then slowly reduced (to around 550), we were able to bring it back to over 700 by 2015. However, the non-corporate individual numbers declined to around 750 over this period (of course, many were now included in the corporate arrangements). A significant minority were non-UK colleagues, initially around 200, rising to 250 and then returning to 200.



Over the period 1991 to summer 2016 the Safety Club held a total of 86 seminars plus 17 tutorials, and the Symposium SSS '16 was the 24th in the series. The level of participation (speakers and delegates) was consistently encouraging, and supportive of Club finances. Our speakers rarely needed travel support and the average attendance count over the 127 events was 78.

The figures in the above paragraphs relate to Newcastle's period of responsibility for the Club; membership connections are now well in excess of 4,000; the current grand total of public events held (end of 2021) is 157, and that does not include the very many, rather more focused, Club working group meetings.

Some lessons learned

Of course, anyone involved in an activity that goes on for 25 years ought to gain something in understanding and experience, and – ideally – improve in capability. We are confident this applies in our case, given the number of occasions on which we needed to follow the swan's example: furiously paddling out of sight while trying to look serene on the surface. The following list tries to indicate some of the areas where we hope that we improved over time, though we quite often may have failed to look serene.



Event planning: appreciating the scope and scale of what needs doing, including comparing venue options (room capacity, facilities, location, availability, flexibility, cost), selecting, negotiating the rate, and finally booking (we learnt to just ignore the minutiae of hotel contracts, just like agreeing to software conditions of use, life's too short).

Event arrangements: paying close attention to details, including specifying room layout, catering requirements, tell the venue at least three times what the schedule is (with a hard copy on arrival – even then it will, occasionally, be ignored).

Event operation: crucially, of course, take the bookings and process the payments, but also organise badging, delegate listing and any other hand-out materials, monitor no-shows, last minute bookings, and unexpected arrivals. SSS is rather more demanding, with delegate bags to be filled with a considerable variety of enclosures (and not all bags are the same), plus providing assistance to our much-appreciated exhibitors.

Event venue costs: keeping these as low as possible by juggling the numbers. Very early on we decided that the best option was to pay on a per capita basis (hotel jargon is DDR – day delegate rate). But then the venue insists on a “minimum guaranteed number”. So the aim is to achieve the smallest commitment for as large a room as might be needed, based on our own best attendance estimate. We used a sophisticated prediction method [Felix, Joan and Tom each made a (informed) guess, and we took the average]. Specific strategies were developed for SSS to cover (i) numbers at the banquet and (ii) bedroom accommodation – note that it would be sub-optimal to simply use the booking information supplied by our delegates; our aim was to have a place for everyone who actually turns up, but not to pay for any extras whatsoever – tricky! It's worth acknowledging that the Royal Marriott in Bristol gave us excellent support with this, but that elsewhere we sometimes struggled.

Event location: accepting national and logistic realities. In the early years of the Club it seemed appropriate to offer a wide spread of geographical locations, but we slowly recognised that London is indeed the centre of the UK. [An event we organized in Scotland attracted 50 delegates, but the vast majority were from England and they grumbled (a little).] Initially though, we avoided central London's inflated charges by selecting towns just outside the capital (e.g. St Albans or Woking). Delegates made it clear that this just made their travel more arduous, adding a suburban journey after they had reached London. And so, the Club's one-day events are now focused on London's city centre.

Club finances: identifying what really mattered. We realized that although pruning and optimising our costs was, of course, worth doing, the key concern in maintaining a break-even financial trajectory was income. Costs were predictable, but income was not. The previous section indicates how we sought to stabilize direct membership support by means of corporate package deals; we greatly appreciate the contribution of so many colleagues in industry who helped this to succeed. Income from one-day events barely covers their cost, so we focused on SSS. As a much larger event, running over three days, margins are more easily covered, and we developed the exhibition element as a very helpful income supplement. Our exhibitors, and especially the regular participants, deserve a vote of thanks for their ongoing support.

SSS evolution: the Club's flagship event. The annual symposium has always been a 3-day event, but the initial format was a tutorial day followed by two days of invited presentations (delegates could choose to attend either, or come to both). In 2012 the format changed to three days of presentations; in 2013 an even more significant change was made by selecting most of the presentations based on submitted abstracts. Adding an exhibition element was a further, highly beneficial, development – and not merely the financial support already mentioned. The exhibition reinforces the industrial focus of SSS and provides the ideal combination of mutual relevance: the services and products are directly relevant to most of the delegates, and most delegates are thus potential customers.



And lastly, we learned that after four intensive days (and evenings) at SSS, we were always somewhat drained (technical term: “knackered”), but found that a wee drink in the bar acts as a restorative – every time!

Some clear successes

Well, perhaps the most basic indicator of success of an organisation is survival. We thoroughly enjoyed looking after the Club until its Silver Jubilee in 2016, and are delighted to be anticipating the Pearl Anniversary of SSS in 2022.

Our personal perspective is necessarily subjective, but here is a summary nevertheless. The operational ethos has always been somewhat artisanal, associated with (but not a part of) the establishment, volunteer led and aided by largely volunteer effort – but always striving for a professional delivery of services and activities. We wanted to achieve truly face-to-face events offering genuine “networking opportunities”; a real meeting-up of like-minded safety personnel, thereby cultivating and building an interconnected “joined-up” community. And to be very welcoming, especially to new and younger colleagues (note the Club's current Safety Futures Initiative [3] to reinforce this) since clearly that is valuable to old hands and new faces alike. The characteristic manifestation of this was consistently demonstrated during the coffee and lunch breaks, which were invariably accompanied by a real (and therefore noisy) buzz of interaction. All in all, the fostering of a **club** of safety professionals that has now lasted for 30 years, keeping people in touch (pre-dating social media!).



The Club newsletter Safety Systems should certainly be mentioned here; indeed, the newsletter deserves far more than just a mention – so instead we refer you to the volume of selected articles “30 Years of Safer Systems [4]” (and the earlier edition “25 at 25” [5]) and also to the extensive repository of past articles available at the SCSC website (<https://scsc.uk/Newsletter>). The Club website has, in recent years, become a major repository for Club information, the primary vehicle for publicising events and activities, and an effective infrastructure for event bookings and membership registration. We gratefully acknowledge that this has only been possible thanks to the sustained efforts of the Club's webmaster, Brian Jepson, shown here seeking further inspiration, with dedication, through libation.



With some risk of hubris, we can surely include SSS in this section. The annual Club symposium is now a standard entry in early February in many calendars. It should be acknowledged that the fundamental contribution of the Symposium comes from the presentations and their recording in a published volume each year. A huge appreciation of the massive effort contributed in this way, by so very many individuals down the years, is entirely appropriate here.

The Symposium has also delivered an essential element of ongoing financial support for the Club's continued existence, via two mechanisms: directly, from the registration fees paid by delegates, and supportively, through the contributions made by our exhibitors. To enhance the experience of delegates and exhibitors, and to maximize footfall at the stands, we augmented conviviality by providing carefully selected fine beverages on each stand, adhering to a theme (that's right, initially malt whiskies, but subsequently beers and then ciders – and always the finest examples that we could identify using our networks of expert contacts); this innovation certainly seemed to go down well.



A further element of cordiality is offered each year at the Symposium "banquet", which always aims to offer good food, good wine, and good company. And also a little erudition: words of wisdom from an after-dinner speaker. We won't mention any names, but a soaring speech from an Air Marshal, and the verdict of a High Court judge (he's now a Justice of Appeal!) have featured. [The standard may have slipped a bit for 2022!]

Some problems encountered

You might naïvely think that with practice and experience and careful planning: what could possibly go wrong? Well, of course you wouldn't think that.

Although SSS gave us the most satisfaction, it also generated the most problems. And the one that occurred most often, and caused the biggest headaches: conference materials missing at the venue. We learnt that the best tactic for essential event materials (badging, programmes and delegate lists) was to carry them with us. [We learnt this the hard way, by having to create hand-made badges the evening before an event, handing them out to delegates with string for a lanyard. Not quite meeting our professional aspirations.]

Specific examples, of lost items, arose at the Belfry when the SSS proceedings were not delivered (we had to mail them out afterwards) and at the Brighton Metropole when all of our couriered boxes were handed over to the organisers of the preceding event, and carefully locked away in a "secret" cupboard. These were found only after following up with the courier company, then the courier driver, and then eventually contacting the organisers of the weekend event. Nightmare!

With disappointing regularity, and at various hotels, packages that we had very carefully labelled and shipped, and that had been delivered successfully, entailed lengthy searches by concierge staff before eventually being handed over.

As mentioned earlier, hotel bedrooms for a residential conference have to be guaranteed by us. The last thing we wanted was to have to pay for rooms that were not actually needed, and so – occasionally – we would be short by one or two bedrooms. A discrete request to a friendly and helpful delegate to stay nearby provided a simple solution. However, we recall two occasions when we were holding rather a lot of rooms less than needed. The first time this happened was when we were at the Belfry at the same time as Birmingham's Spring Fair (the hotel became fully booked and would not expand our allocation). We asked a dozen delegates to relocate to the very attractive New Hall hotel nearby, laid on transport, and covered the bar bills. Sorted. And just once, at SSS '01, the Royal Marriott could not help out, and we were six bedrooms short. We were very grateful to the RAF delegate contingent who agreed to stay as a group at the Bristol du Vin. (We knew better than to offer to pay for that bar bill!)

So, as you may have realised, our goal was to conceal any organizational problems from most, if not all, of our delegates. But here's one where that was just not possible. It was day 2 of SSS '02 at Grand Harbour, Southampton. Our presenter was just getting into his stride when the P/A system burst forth (very loudly) with music and announcements from a keep fit session elsewhere in the hotel, due to a misguided sharing of radio frequencies. Only a frantic search for a technician could fix that one.

Attending well over 100 Club events requires rather a lot of travelling – so some travel problems were inevitable. Here are a few anecdotes.

At the Belfry one organiser's back gave out (yes, it was Tom). He left the hotel by being wheeled out to the car park sitting on a chair mounted on a hotel porter's luggage trolley. Fortunately, there were very few spectators!

“At the Belfry one organiser's back gave out ... he left the hotel by being wheeled out to the car park sitting on a chair mounted on a hotel porter's luggage trolley”.

A Club seminar on formal methods in Peterborough (March 1987) had a splendid booking level of 126 delegates; the meeting room overflowed into the corridor! All in all, a good day. Since the venue was located directly across the street from the railway station, there was time after the event closed for swift refreshment in the bar before hurrying across to catch the train at 1800. But, oh dear – a major delay and the train was now due at 1850. Clearly the only acceptable option was to go for another pint and then back to the platform at 1845, where the rear lights of the departing train were still just visible, receding in the distance. The next one was due at 1930 so we stayed in the station. It eventually arrived just before 2000, and then was delayed again at York. We finally reached Newcastle at 2305, long before 'delay repay' was introduced.

In 2010, the Club (and CSR) operated the large Environmental and Safety Assurance Symposium event for MOD at Abbeywood, Bristol. That was the year that an eruption of the Eyjafjallajökull volcano in Iceland sent clouds of ash and dust into the atmosphere; the main impact on aviation was in April, but a second wave (as we now call them) in May meant our return flight was cancelled. We switched to a direct train to Newcastle from Bristol Parkway. It was rammed; Joan stood until Derby; no seat for Tom until Leeds.



However, our worst returning “rail” journey was caused by a closure of the East Coast Main Line between York and Darlington. Passengers waited in huge queues at York while coaches were, ever so slowly, brought in to transfer us all north to Bank Top station. Joan was frozen (stiff, then solid, she said); indeed she still complains about it now. Quote: *“I said we should have gone for a ***** taxi!”*

We were once trapped in London for an extra night. Very heavy unanticipated snowfall meant no trains or flights were operating at all. We only realised this rather late in the day and most hotels were, by then, full. Joan rang the massive Forum hotel (since renamed), and we managed to book two of the last five rooms.



A major snowfall in February 2009 had us worried about SSS that year, in Brighton. The conference team were at Newcastle airport ready to fly to Gatwick, with bags checked, when serious delays were announced. We were about to try to retrieve our luggage to see if we could head south by rail instead, when a late take-off was promised. At Gatwick, the only trains available were the ones we needed – trapped on the section south to Brighton. On arriving at Brighton station there were no taxis

(because all of the local buses had stopped operating due to some snow on the roads). However, after waiting 45 minutes, a brave taxi driver picked us up. Given the problems we had had, and with bad weather continuing, we were seriously concerned about the risk of a low attendance. In fact, there were only about five no-shows. A special commendation is due to the tutorial presenter that year, Nancy Leveson. She had flown from the USA into Heathrow on the Monday, and just kept taking trains that gradually got her nearer to Brighton. By a very circuitous routing she eventually arrived at the hotel around 11pm. Indeed, we concluded that the only people who don’t (eventually) get to SSS are those who don’t set off.

So, let’s end this on a positive note. We’ve massively enjoyed supporting the Club, and anyone who travels can recount the difficulties that sometimes arise. And although we may often have stayed in rather ordinary hotel accommodations, there have been splendid occasions too. One of these was when Joan was allocated the Presidential suite at the Belfry (probably the best room she’s ever stayed in). And to add to the joy, we overheard a very wealthy gentleman from overseas complaining at reception because he could not just walk in and get a room: *“I’ll pay for the Presidential suite” “I’m afraid it’s occupied, sir”*.

But best of all, when we held SSS at The Grand at Brighton, your authors were allocated (at no extra cost!) almost the entire first floor frontage of the hotel (the Thatcher suite, we called it). The layout was: huge bedroom, huge lounge, small dining room, huge lounge, huge bedroom. Although the dining room was not included, we hired it personally for the night before the conference, opened up all five rooms (just to show them off) and hosted a private dinner for eight. A most memorable evening.



Ah well, go on then, just one more problem scenario. The organisers arrived at the SSS venue hotel on the Monday, at around 11.00, only to be told by reception that no bedrooms had been reserved for us, nor for any of our residential delegates. Just picture Joan’s reaction. Speculate about what she said. Rather a memorable morning, actually.

References

- [1] Safety Systems, Volume 25, Number 3, May 2016, Felix Redmill, <https://scsc.uk/scsc-144>
- [2] The Alvey Programme, <https://en.wikipedia.org/wiki/Alvey>, accessed January 2022
- [3] The Safety Futures Initiative, Zoe Garstang, <https://scsc.uk/qf>
- [4] 30 Years of Safer Systems: Three decades of work in the field of safety-critical systems as told through the SCSC Newsletter, Louise Harney, Mike Parsons, Paul Hampton, Roger Rivett, Wendy Owen (Eds.) <https://www.amazon.co.uk/Years-Safer-Systems-safety-critical-Newsletter/dp/B09KNCYKDL/>, October 2021.
- [5] 25 at 25: A selection of articles from twenty-five years of the SCSC Newsletter Safety Systems, Mike Parsons, Graham Joliffe, Tim Kelly (Eds), <https://www.amazon.co.uk/25-selection-articles-twenty-five-Newsletter/dp/154089648X/>, January 2017.

Image attribution

All images © SCSC except the Eyjafjallajökull dust cloud: 14296614 © Jon Helgason | Dreamstime.com

Tom Anderson and Joan Atkinson

From 1991 to 2016 Tom Anderson directed the SCSC within the auspices of Newcastle University, where he was Professor of Computing Science. His research interests addressed fault tolerance and, more broadly, dependable systems (encompassing safety and security). In 1984 he established the Newcastle branch of the Centre for Software Reliability, which provided a supportive environment to a series of research projects, and also organised over 250 external conferences and seminars – all with a strong industrial orientation. From 1992-97 he was Head of Computing Science; 1998-2002 Dean of Science; 2008-2012 SAgE Dean of Business Development. Tom retired in 2016, but continues to be active in the SCSC Steering Group and maintains engagement in outreach via CSR Events. Thanks to Covid restrictions he has designed and scratch built a rather splendid garden shed.



Joan Atkinson joined Tom at CSR, Newcastle University in 1985 where she became the research centre's Administrative Coordinator which, as well as support for the centre's academics and their research, involved full responsibility for the administration of the SCSC. The events referred to in the previous paragraph were, of course, all organised by Joan – in fact there were 256 events altogether, total duration 422 days, with an average daily attendance of 86 (equivalent to looking after 100 people for a year). She too retired in 2016, and now does the work of CSR Events as a self-employed PCO (professional conference organiser). Despite Covid restrictions, as Chair of the Washington Village in Bloom group, she led them to victory in the Northumbria in Bloom competition (best overall entry) and was awarded a trophy cup only slightly shorter than herself.





THE SAFETY-CRITICAL SYSTEMS CLUB

Seminar: Managing 'Black Swans': Handling Rare and Severe Events Now and in the Future

8th April 2022, London, TBC hotel and blended online

Bookings at:

www.scsc.uk/events

This seminar is an opportunity to hear about management of rare and high impact events across different industry sectors and how this is likely to change in the future.

It will be useful for safety practitioners, safety managers, and for those involved in the planning and management of high-impact events.

Details at: www.scsc.uk

How to Manage Unexpected and Severe Events

www.scsc.uk

This seminar will consider how to plan for and manage recovery from 'Black Swan' events in a safety context. These are events which are rare, unexpected and have high impact. Examples might be the Fukushima nuclear disaster or the loss of Malaysia Airlines flight 370.

There are many aspects to the management of such events including planning, preparedness and dry-runs of contingency processes. When an event occurs, it is necessary to quickly establish the nature and scale of the problem, stabilise the situation, prevent a cascade of failures, assess risks, provide a contingency service if possible, communicate to all stakeholders and eventually recover normal operations.

Communication, obtaining reliable status information and rapid assessment of risks are critical but may be difficult. Hard data may be limited, and situational awareness, human factors, organisational experience and safety culture all come into play.

The first part of this seminar looks at the current position in various industries. The second part examines the situation when upcoming automatic and autonomous functionality is involved. How do we make risk-based judgements when human involvement is small?

There will be a workshop session where delegates can explore the events and the possible solutions further.

The Future of Human Factors?



Human factors have always been important when considering how accidents may be prevented or evaluated. In this article, John Ridgway explores how such considerations may play out in the future. In particular, one has to consider how the factors that influence safety-related decision-making will be judged after one takes into account the methods and processes that are likely to be in place.

A palpable tension was hovering in the air like the lingering stench from a cheap e-cigarette. A court that had previously gasped from want of belief rather than fresh air, now held its breath as the Counsel for the Prosecution rose to her feet to deliver his closing speech.

"Members of the jury," she opened, "you have been witness over these last two days to a tragic story of woeful dereliction, matched only by an even more woeful failure to apply the ethical judgment that all members of the public have a right to expect from those given the responsibility of ensuring their safety. This was not a failure of a component, as the Defence would have you believe, but a failure that struck at the very heart of the decision-making process. A failure of decision-making that led to the tragic deaths of Mr and Mrs Cooper as they embarked upon what should have been a perfectly safe journey upon the Gender-Neutral Royalty's highway.

You have heard a truly bizarre attempt from my learned Counsel for the Defence to exonerate the defendant on the grounds of logicity. No doubt these arguments will be repeated shortly, but, as you listen to them, I ask you once again to consider how such a failure of judgment was possible. How can an operator instructed to set road signs that are vital for the safety of the road user, possibly justify setting them in such a way as to knowingly increase the risk to not one, but two, members of the general public? Normally when considering operator fallibility, one is confronted with unfortunate errors that are quickly regretted. But have you heard one note of contrition from the defendant in this court? No! Just an insistence that the twisted logic applied should be accepted as the optimum safety decision to be made under the circumstances.



Well, I'll leave you, the members of the jury, to decide upon that matter yourselves. However, I put it to you, that any right-thinking mind would look upon the decisions made on that fateful day and come to the inescapable conclusion that the defendant is guilty as charged; guilty not only of gross neglect but also of a reasoning that you must surely agree was most egregiously flawed. I thank you all."

As the murmurs spread through the auditorium, it was clear that the speech had gone down well. The court had been invited to understand that this was not a tragedy borne of physical frailty. Instead, the frailty lay in an inability, under stress, to apply a reason and rationality that would be recognisably ethical to those who were in a position to judge. Today, such a judgment was being made by twelve of the defendant's peers, and it mattered now, more than ever, that the Counsel for the Defence could make a strong enough case for believing that not only rationality and reason, but also ethicality and morality, had lain at the heart of the defendant's decision-making. A hush descended upon the auditorium as she rose to her feet and turned to the jury.

"The frailty lay in an inability, under stress, to apply a reason and rationality that would be recognisably ethical".

"Members of the jury, my learned Counsel for the Prosecution has succeeded admirably in fomenting righteous indignation, but I put it to you that emotions should be set aside when determining your verdict. I have carefully explained over these last two days the complex interplay between traffic congestion and road safety. I have ably shown that all usage of the Gender-Neutral Royalty's highway entails risk, and that this is a risk that each and every one of us accepts when we step into our vehicles.

Indeed, there are only two traffic states that are truly safe: firstly, when the congestion is at its minimum because the road is empty, and secondly when the congestion is at its maximum, resulting in a gridlock that has ground the traffic to a halt. I have also shown you the risk profile curves that demonstrate that the accident risk is at its maximum at the mid-point just as the laminar flow of traffic starts to break down and shock waves start to develop within the traffic flow. It is at this point of flow breakdown, the onset of chaos if you will, where one sees the occurrence of unexpected queues that are the main cause of rear quarter collisions. Furthermore, it is at such a point that the temptation to make dangerous lane changes is at its greatest.

Therefore, the operator in charge of setting signs has a duty to implement traffic management strategies that move the traffic away from this phase transition whenever possible.

Sometimes this will entail diversions to alleviate traffic flow on a particular stretch, but it may also require the increasing of traffic volume through judicious means, in order to quickly encourage a slowing of traffic. This is all that the defendant was doing on that fateful day. By setting lane change instructions that encouraged Mr and Mrs Cooper into a collision with another vehicle, two major benefits had been identified. The traffic behind the resulting accident would grind to a halt, and the road ahead would empty. This win-win situation was marred only by the sad deaths of the couple concerned. However, since the defendant had anticipated and avoided an even worse accident, who amongst us can say that the wrong decision had been taken? I put it to you that the decision was taken with safety optimisation in mind and that the decision was taken under the most difficult of circumstances. On such a basis alone, I must conclude that the only logical decision available to you is to acquit. I therefore appeal to your own



respect for logic and ask that you draw this conclusion: By all reasonable judgment, the defendant is not guilty.”

“The seeds of doubt had been successfully sown as the jury members were now being asked to place themselves in the position of the defendant”.

With that, the Counsel for the Defence retook her seat before turning to her assistant. A small but discernible smile played across her face as she listened to the appreciative mutterings now echoing within the courtroom’s small confines. The seeds of doubt had been successfully sown as the jury members were now being asked to place themselves in the position of the defendant. The crux of the matter was this: Had they found themselves in the same position, how would they have reacted? Put another way, how normal was the thinking of the defendant? Was this, at the end of the day, the only criterion that we should be applying to determine ethicality? As the auditorium continued to grapple with these questions, the murmuring grew ever

louder, to the point that the judge felt it necessary to intervene.

“Silence in the court!” she bellowed. “Members of the jury, you have now heard the closing statements from both counsels. I ask now that you adjourn to make your decision.”

By now the tension in the courtroom was barely tolerable, and so it was to everyone’s advantage that the verdict was returned with the minimum of delay. As the court reconvened, the judge once more struggled to regain control.

“Silence! May I remind you that this is a court of law.” Having thus re-established her authority, she slowly turned to the jury. “Members of the jury, have you reached a decision upon which you are all agreed?”

"We have."

"And what is that decision?"

"Guilty, M'lady."

Not for the first time, the judge had a crowd management issue to deal with as the auditorium erupted into loud cheering.

"I will have silence in my court!" she maintained with a well-judged *fortissimo*. Turning to the defendant, it was now the judge's chance to draw conclusions.

"You have been found guilty of the most appalling error of judgment, and for that there can be only one verdict. But before I pass sentence, I feel it only fair to draw attention to an important principle. So often in these situations it is the operator at the coal face that is brought before this court, and yet no accident can be said to have been caused by a single factor. In so many cases one has to take into account systemic failings that made the operator error all the more possible. This case is no exception and so it would be remiss of me not to point out that the operator would have not made this calamitous decision if the software engineer who had programmed it had ensured the inclusion of the necessary subroutines for checking compliance with all relevant ethical constraints. Consequently, I will be advising that a review be held into all future artificial intelligence programming, as employed on automated safety systems development for the Gender-Neutral Royalty's highway. In the meantime, I sentence the defendant to be immediately decommissioned and add that it shall not be re-commissioned until such a time as the safety case has been approved for the regression testing of its software upgrade. I would also like to thank the jury for its most sage judgment and I advise that you should all be excused further jury service until after your power units have been refurbished. This court is now closed."

Now, and only now, the excesses and exuberance of the auditorium were to be encouraged. A difficult judgment had been made in a manner that appeared to be to everyone's satisfaction. But as the clamour in the public gallery slowly subsided, it was only the most observant and alert amongst them who will have witnessed the Justices' Clerk leaning forward before deftly switching the judge into standby mode.

Image attribution:

top image: 34511744 © George Kroll | Dreamstime.com

traffic: 174058577 © Gemphotography | Dreamstime.com

justice: 131742890 © Diana Drożdżał | Dreamstime.com

John Ridgway, Retired

Following 30 years in various quality and safety assurance roles, whilst working for a contractor developing traffic management solutions for both domestic and foreign clients, John is now enjoying a relatively uneventful retirement on the edge of the North York Moors. John would like it to be known that he learnt everything he knows regarding the UK's judicial system from watching poor courtroom dramas.

The author retains copyright of this article.

Planes and Computers



Stan Price has recently published his autobiography “Trains, Planes and Computers” chronicling his long career in systems safety, from designing, auditing and testing safety-critical systems through to research into making them safer and even acting as an expert witness in court. Stan shares some of his thoughts and insights from working in the discipline for over 30 years.

The Prehistory of System Safety

Even before systems safety, and in particular, the probity of software, became a specific topic, those involved in such systems, including myself, were well aware that systems could kill and maim. It was around 1968 when I was first responsible for a safety-related system. It was for the production of the Operating Data Manuals (ODMs) for the then current Manchester (AVRO) designed aircraft – the Nimrod and 748. The ODMs, as the name suggests, indicated to pilots how the aircraft could safely be operated and consisted largely of tables. For example, they indicated minimum runway lengths at particular take-off weights, airfield altitudes and ambient temperature. For each phase of flight, e.g. take-off, cruise, or climb, there were three programs in the process of producing the relevant part of the particular aircraft’s ODM.

The first of these calculated engine performance, which was then used by the second program to calculate raw aircraft performance data. The final program in the suite sorted this raw data into the table that went into the ODM. This presented unique formatting problems, in particular, as the environment got more arduous – hotter and higher; the aircraft could not operate there, so there was no entry in that part of the table.

Obviously if the data in the ODMs was inaccurate and was acted upon, there was a danger that safety could be compromised. Indeed my ODM system came under suspicion when two aircraft slid off the same runway in the same afternoon. Fortunately for me, the problem was an inaccurate hand-produced correction figure for the landing distance required on wet grass.

A Move to Air Traffic Control

Late in 1972, I moved into the realm of Air Traffic Control (ATC), with its obvious safety implications, and was responsible for judging that a projected system's software was of such poor quality that safety would be again compromised.

It was a system for assisting controllers in knowing more exactly the sequence of aircraft landing at Heathrow. This involved calculating the timing and speed of aircraft leaving the four stacks so that the spacings when they landed on the runway were the minimum commensurate with safety, and hence its use was optimised.

A prototype of the system was being developed by the Royal Radar Research Establishment at Malvern. One of my software engineer colleagues, Dave Neumann, and I visited Malvern and viewed the system. We discovered the software was very poorly written. It had no structure and comments were also non-existent. Its documentation was also very limited. Dave and I therefore reported this, and the project was cancelled. Its quality was so bad that any deep consideration of safety was unnecessary. I feel generally that the quality of software has improved over the years since, and particularly, where relevant, with the focus on safety.

My major involvement in ATC systems was in the UK's acquisition of the US en-route ATC computer system (the 9020 Project). Even though the original system would not, in its US operational life, handle aircraft flying east of the Greenwich Meridian, the specification allowed for the possibility. But it appears that this was never tested before going operational in the US; but upon testing in the UK, it folded the country over at the meridian. For example aircraft flying over Ipswich were being shown as being over Bedford. Hardly safe, defeating the whole purpose of ATC – to stop aircraft colliding. Suffice to say this was corrected before the system went operational. The principal lesson to be drawn was the dangers of assuming that a system that was safe in one domain does not mean it will be safe in another.

An Expanding Role

Later, I was involved in a police command and control system. This would have the purpose of real-time allocation of police assets to incidents requiring their attention on a geographic basis. Misallocation could mean that some safety-critical incidents would not be attended to thus diminishing safety. My role would be a key one in choosing the contractor to implement the system and then oversee its installation.

Next, I was asked to monitor three projects in the DTI/Research Council Safety-Critical Systems Research Programme. I also believe the Programme spawned the SCSC Club. The projects were:

MORSE – A Method for Object Re-Use in Safety-Critical Environments with partners University of Cambridge, Lloyds Register, West Middlesex Hospital, Transmitton, Dowty Controls and British Aerospace Airbus

SPAM – Investigating Security Paradigms Validity for Safety-Critical Environments with partners EDS-Scicon and Lloyds Register

PRICES – Productivity, Integrity & Capability Enhancement for Software, and Human Factors in Safety-Critical Systems Development involving Open University, City University, Lloyds Register, Rolls- Royce, Bae SEMA, G P Elliot Electronic Systems and Analysis Consultants.

By this time (1994) the pro-active consideration of safety using techniques such as HAZOPS etc had become much more structured and mandated replacing the simple "does it meet the spec" criteria of yesteryear.

What goes on out there?

Subsequently I performed a coordination role within the Programme including two initiatives, which I conceived and got funding for. One of these initiatives was a series of workshops devoted to specific topics, which I considered, were of key relevance to successful and particularly safe systems. My judgement on what was key was heavily influenced by my previous industrial experience. To make the workshops manageable, the number attending was restricted to twenty or less, split equally between academia and industry, largely but not exclusively, drawn from participants in the safety-critical programme, participants that I rated.

I chaired the workshops, and each had a rapporteur who produced a report chronicling the proceedings and the conclusions. This was circulated to the attendees for their comments, and a final version incorporating these was then published. The workshops were opened by myself with an introduction that cited the purpose of the workshop and its format.

The latter, after the introduction, consisted of presentations from the safety-critical programme projects that were relevant to the topic of the workshop. These were followed by comments on the presentations from the so-called catalysts (chosen to stimulate discussion), which led into general discussions followed by a summary.

The initial workshop, under the title, 'What goes on out there?' addressed the gulf between what the research community thought happened in day-to-day industrial/commercial practice and what actually happened. As well as the DTI sponsorship of the workshop, it also ran under the auspices of the SCSC, and over the years, I also made contributions to several of its events.

The other workshops that followed the initial one addressed the following, in relation to the safety of systems:

- Human Factors
- Software Requirements Elicitation and Capture
- System Assessment
- Artificial Intelligence
- Process Models
- Data

I believe that the deliberations at these workshops and their proceeds had a degree of influence particularly in the hitherto neglected topics of Human Factors and Data.

Expert Witness

My final professional contribution to the safety-critical world came as an expert witness in a court case around 2001.

Electronic Data Systems (EDS) was contracted to supply to the Civil Aviation Authority (CAA) a new computer system at Prestwick in Scotland to support the control of air traffic over the

"... the deliberations at these workshops and their proceeds had a degree of influence particularly in the hitherto neglected topics of Human Factors and Data."

North Atlantic. The CAA cancelled the contract after the design milestone, citing non-performance on the part of EDS and EDS took the CAA to court for some forty-two million pounds. Because of my air traffic control and computer background, I was approached directly by EDS's solicitors to be an expert witness for them.

Curiously, this was not so much for my system development expertise; a team of three other experts was handling that, but on the safety issues in the case. EDS's legal team believed that the CAA might play the safety card. Unfortunately, my other commitments at the time meant I could not really take up the assignment, and at first, I said no. However, the fee I was eventually offered, a four-figure day rate, plus an agreement that I could employ a researcher, made me change my mind.

The researcher I employed was John Smith, who had been the Plessey manager involved in the 9020 Project during my days with the Civil Aviation Authority, and who had subsequently produced the safety case for the London Air Traffic Control Centre.

Insofar as John's and my inputs to the case were concerned, they were significant in two respects. Firstly we smoked out the fact that the first part of four of the CAA's safety procedures amazingly did not exist, and therefore, their criticism of EDS's safety processes in the case was therefore unrealistic, to say the least. Secondly, in my initial report, I had pointed out that there was no common agreement on how safety should be built into software systems, so their criticism of what EDS was doing was not necessarily valid. The CAA retorted that there was agreement and cited numerous standards. To this, I asked the simple question: if there was a common approach, why was there a need for so many standards, which in some areas were even contradictory.

"... if there was a common approach, why was there a need for so many standards..."

Are We There Yet?

This may not be the situation now, but as a distant observer in retirement of the safety-critical systems scene, I am amazed that unsafe systems are still going operational. Two significant ones that come to mind are the Boeing 737 MAX [2] and the so-called smart motorways [3]. It may well be, at the technical level, that we are now much better at ensuring safety, but until we stand up to the financial and political pressures sometimes put upon us, our detailed work will come to nought.

References

- [1] Trains, Planes and Computers, <https://www.amazon.co.uk/Trains-Planes-Computers-Executive-Pass/dp/1802271252>, Stan Price, 2021, ISBN: 978-1-80227-125-6 and 126-3
- [2] Boeing 737 MAX – Safe to Fly? Paul Hampton & Dewi Daniels, Safety Systems Volume 29, Number 1, Feb 2021 <https://scsc.uk/scsc-162>
- [3] How Smart Are Our Motorways? John Ridgway, Safety Systems Volume 28, Number 2, May 2020, <https://scsc.uk/scsc-158>

Top image: AVRO748 undertaking rough airfield trials at RAF Martlesham Heath now BT Research.

Stan Price spent over 40 years developing, evaluating and researching IT systems – many of them safety-critical principally in the Aviation sector. He is a Chartered Engineer and Member of both the Royal Aeronautical Society and British Computer Society. He has performed visiting posts with Sheffield and Salford Universities and given evidence in over 40 court cases involving IT.

The SCSC and the Internet (actually the World Wide Web but...)



The screenshot displays the SCSC website interface. At the top, there's a navigation bar with links like 'Home', 'About the SCSC', 'Search', and 'Related Links'. Below this, a sidebar on the left contains a 'Safety-Critical Systems Club' section with a 'What is the Club?' subsection. The main content area features a large banner image of an airplane in flight over a control tower. To the right of the banner, there's a 'Welcome Brian.' message. Below the banner, there's a '30th Anniversary' badge and a 'Upcoming events' section listing the 'February 8 - 10, 2022 - Bristol, UK and blended online Symposium: Safety-Critical Systems Symposium (SSS'22)'. A 'Latest news' section on the right mentions 'SSS'22 The Safety-Critical Systems Symposium going ahead, 8 - 10 Feb in Bristol'.

The SCSC website has become an essential resource for members, not only in providing information about the club and upcoming events, but also in providing a wide range of other services such as access to publications, working group resources, multi-media material and has been critical in ensuring the club could weather the Covid-19 pandemic by facilitating streaming-based services. Brian Jepson, the SCSC webmaster, describes the history of the website from its humble beginnings and how it has evolved over the years.

The Safety-Critical Systems Club has a history that runs parallel to that of the World Wide Web (WWW). These days most people use Internet, which has been around since the early 1980s, interchangeably with the World Wide Web (WWW), designed by Tim Berners-Lee, that operates as a service using the internet. Most of what I'm talking about here is WWW but 'Internet' makes a snappier title. Both the WWW and the SCSC appeared to the world at the beginning of 1991, but it took a few more years before the Club started to use the web in earnest.

In today's world, the Club could not survive without a website. In the year from mid-2020 to mid-2021, the website, in conjunction with email, Zoom video conferencing, digital publishing on Amazon, and video streaming through YouTube, provided online seminars, a three-day symposium and allowed the working groups to continue their work.

The early days

From its inception in 1991 through to 1997 the Club had no presence on the web. The Centre for Software Reliability (CSR) at Newcastle University was running the Club with operations being conducted by telephone, post and email.

www.csr.newcastle.ac.uk

The screenshot here shows an early CSR web page from 1998.

At this time the website only provided basic information about the club, its objectives and what it does.

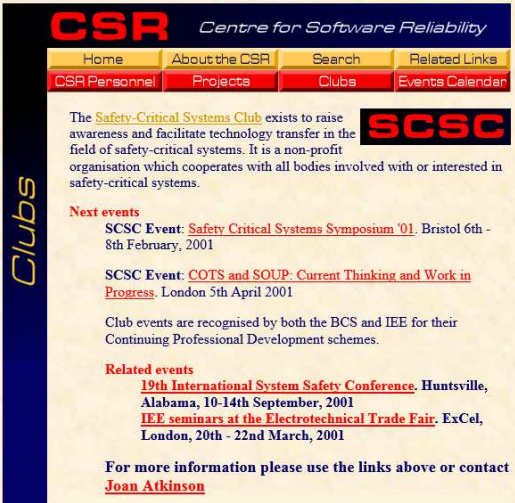
These pages were hand coded in HTML and were difficult to maintain. In later versions the technology adapted to include a database, CSS and server- and client-side scripting but remains focused on substance and accessibility over style.



www.safety-club.org.uk

In 1999, the www.safety-club.org.uk domain was registered to give the Club its own identity, though this was the existing information served by the Newcastle University using the CSR Clubs pages.

This screenshot shows an updated CSR page from 2001 accessed as www.safety-club.org.uk that focuses on the Club and includes the next Club and related events with linked pages containing details of each event. This style of web page remained in use through to February 2008.



By 2004 the Club was increasingly being known by its SCSC initials, and luckily, the www.scsc.org.uk domain was still available, so this was registered as an alternative to the full safety-club domain.

www.scsc.org.uk

It would be difficult today to get hold of a short domain name like this and when, in 2014, the abbreviated .UK domains were introduced we exercised our right to also acquire scsc.uk giving us a seven-character identity.

It was also becoming difficult to maintain the pages hosted by the University, so www.scsc.org.uk was kept separate and developed as a new website. This new site remained, linked to the CSR website, but it was able to rapidly expand to include more useful information such as back issues of this, the *Safety Systems*, Newsletter as visible below. This version of the website made use a database to store all the resources and scripts to dynamically generate pages as requested allowing much easier and quicker updating.

(Main Club website @ CSR) (Event event) (Event diary) (Past events) (Directories) (Club information)

(Main Club website @ CSR)

(Next Event) (Event Diary) (Past Events) (Directories) (Club Info.)

The Safety-Critical Systems Club

SAFETY SYSTEMS

1991 1992 1993 1994 1995 1996 1997 1998 1999 2000 2001 2002 2003 2004

January 2005 Volume 14, Number 2

1. Editorial - Continuing with fundamentals
2. A View from the Street By Martyn Thomas
3. SITS and Software By Peter Bishop
4. Computer-based evacuation simulations for large public buildings in the aftermath of 9/11 By C. Johnson, J. Appleby, P. Cooper, A. Foss, S. Hailey and B. Jenkins
5. Visualising operational and design complexity in aerospace safety critical systems By Neale L. Fulton
6. The second edition of the MISRA C Guidelines By Les Hatton

September 2004 Volume 14, Number 1

1. Editorial - Time to address fundamentals
2. Should software engineers be licensed? by John Knight
3. Defining the safety case concept by Tim Kelly
4. The Safety-Critical Systems Symposium 2005
5. Combining evidence in risk analysis using Bayesian Networks By Norman Fenton and Martin Neil
6. Can software be perfect? By David Crocker
7. Data driven systems and their configuration By Peter Duggan

In February 2007 the CSR pages hosted at Newcastle were abandoned and both domains now delivered the new website which had developed to include more publications, a directory of tools useful in the development of safety-related systems and information about club membership. The screenshot below shows an early version of this new website. Note the logo as a flag on the red flagpole that has now become an SCSC style used on all pages and many handouts.

Latest news

Welcome to the new Safety-Critical Systems Club web site.

The 50th issue of *Safety Systems* which was posted to all current club members in January is a bumper double size edition. This special issue features articles by many leaders in the field of system safety, including Martyn Thomas, Trevor Kletz, Nancy Leveson and John McDermid - to name just four. Whilst they cover a number of topics, a pervasive thread is Professionalism. *Safety Systems* has always promoted Professionalism, and there could be no better way of marking this 50th issue than with a call by so many prominent figures for us to examine - and improve - our Professionalism.

To become a member of the club and get your copy of *Safety Systems* please contact [Joan Atkinson](#).

Next events

Date	Event	Title
May 12 th 2008	SCSC Seminar	Public Safety, Counter Terrorism and Mathematics of Proof
BCS office, London		Evening Seminar by Prof. Chris Johnson, University of Glasgow.
Held in conjunction with the BCS FACS group.		
June 5 th 2008	SCSC Seminar	User Experience of Tools for Safety-Critical Systems
Royal Lancaster Hotel, London		

V1c: 28-2-2008

Recent years

In 2014, the Club acquired the shorter www.scsc.uk domain and, to reflect the international appeal of the Club, also acquired www.thescsc.org. All the Club domains lead to the same content from the canonical www.scsc.uk website.

www.scsc.uk
www.thescsc.org

The website has now grown to include a comprehensive history of club events with over 1400 resources available to Club members including presentation materials from events, books, working group guidance documents, symposium papers and 69 issues of this, the club newsletter.

There are ten *working groups* supported by the club covering topics ranging from Autonomous Systems Safety through to Safety Culture and The Safety Futures Initiative. Each working group has its own web pages where ongoing work can be shared.

There is a *publications* area where members can download digital version of the symposium proceedings, newsletters and other documents such as the guidance produced by working groups. There is also a *community space* forum style area where thoughts and opinions can be shared.

In the *Catch up* area are details of many of the Club's past events. Most presentations at events are now recorded, and the videos of these are available for members, together with copies of the presentation slides and any other handouts. Because of the Covid-19 pandemic, events between mid-2020 and mid-2021 have been online only, and, since October 2021, as hybrid events with both in-person and online participants.

Brian Jepson, SCSC Website editor, 2004 onward.

Brian has 38 years' experience in software and system safety in the defence sector but has now retired and spends his time supporting the SCSC and restoring a Land Rover 101.

Website snapshots © SCSC retrieved thanks to the WayBackMachine Internet Archive.

The Future of Safety Engineering and Assurance



The SCSC has come a long way since its inception 30 years ago, and has achieved a great deal throughout that time, undoubtedly contributing to making systems safer. Over those three decades, the club has needed to adapt to a changing world: the use of technology in society has expanded rapidly, and systems have become more powerful, complex and distributed with many new disruptive technologies (such as AI) making safety assurance ever more difficult. So what will the world be like in another 30 years? What will the concerns of the club's members be in 2052, and what achievements will the club be celebrating?

Jeremy Messersmith, in his ukulele song "Everybody Gets A Kitten" [1], offers his particular optimistic vision of the future:

*"Gotta say the future's awesome, everything is a-okay!
All the work is done by robots, every day is Saturday.
Future people all have jet-packs, fly around in flying cars..."*

And, as hinted by the title, he goes on to predict that:

*"Everybody gets a kitten, a new one every single day ...
You can name if you want, or you can give it away!"*

Jet packs and flying cars? Probably – we have prototypes of those now; but, as we've seen, the logistics of distributing vaccines to 50+ million citizens in the UK alone has been immense; imagine the distribution infrastructure, processes and personnel required to ensure everyone had a kitten delivered *every day*... well, perhaps not.

To get a, hopefully, better informed and sagacious answer to these questions, members of the SCSC Steering Group were canvassed for their opinions on how they see the future of safety engineering. The following summarises some of their predictions in response to four specific questions.

The pressing concerns of the day might be best illustrated through the title of the key note speakers' talks at SSS'52, but what might these be?

The continued progression of autonomous systems featured in a number of suggested titles:

- Why my iPartner isn't always pleased to see me
- Training Adaptive Systems of Systems in a Secure and Ethical Way
- Why Manually-Driven Vehicles are a Danger and Should be Banned
- The Importance of Non-human Factors in Safety Assurance
- Can AIs Argue Their Own Assurance?

There are also views that system safety will be an increasing concern for systems operating off-world in space and on other planets:

- Fatal Mars Rover Collision in 2050: Final Accident Report and Analysis
- A review of safety standards for commercial space transport vehicles



Other titles suggest that safety assurance challenges will emerge from novel technologies:

- How Weather Control Failed in the Storms of '51
- Regulating System Safety in the Metaverse [2]

The expansion of safety consideration from primarily focussing on harm to individuals and the associated technical mitigations to include the wider societal and environment impacts, and encompassing the trade-off between harms and benefits, is expected to bring more expansive concerns:

- Safety, Ethics and Sustainability of Domestic Space Flights
- Safety Assurance of Earth's Digital Twin

As with our existing standards – some being in use for several decades – standards are expected to continue to feature in the future:

- The key differences between IEC 61508 Editions 9 and 10

Autonomous Systems and Artificial Intelligence (AI) are some of the current bêtes noires for Safety Engineers, but what sort of technologies will be the most challenging for safety engineers in 2052?

The challenges of AI are still expected to be present well into the future, with new developments confounding the assurance progress that might have been made in the meantime:

- Explainable systems that make up false explanations for their decisions, i.e. create lies
- The automation of safety certification using AI based on 2040's practices and how to get new techniques accepted
- Evolutionary systems that breed new behaviours
- Personal robotic assistants



As with the key note speaker title, space travel is also seen as a future challenge as the capability becomes more accessible and available to a domestic market. However, this is just one example where technological expansion will need the safety community to take a wider view, such as: what are the impacts on global resources, climate change and risk distribution from such activities?

Challenges in the Healthcare domain and medical science also features as presenting future challenges, both technically and morally. Some Covid anti-vaxxers already believe the technology exists to inject microchips into people. When such technology is available, how will we deal with the safety implications and need to weigh the risks of not introducing (life-saving) technology? Specific examples are:

- Healthcare Nanobots
- The embedded man-machine interface – cyborgs
- Robotic surgery

Other suggested areas that will present challenges are related to the challenges we face now:

- Highly adaptable, configurable systems – just what are they doing today?
- Systems of Systems; Systems of Services – everything interconnected and inter-dependent

And of course, we will still have the same issues that we've not been able to solve in the last three decades, such as the metrics used to measure software.

Interestingly, there were not many responses in terms of the integration of safety and security disciplines; only some concerns around Ubiquitous Communications and Computing, but perhaps this reflects an optimism that safety/security integration will be eventually 'solved'...

What new tools, techniques and methodologies will be available to safety engineers in 2052?

New tools and techniques are certainly anticipated, but there is also an expectation that the tried and tested techniques will also still be with us. Firstly, new suggestions:

- Better visualisations
- Simulation/animation models
- Virtual environments
- Quantum Risk Assessment
- AI-prediction in Safety analysis - now we don't have to guess 'What if?'

And evolutions of the more familiar standards and techniques that we have now:

- DO-178K
- STOMP: The Systems-Theoretic Outcomes Model and Processes (c.f. STAMP [3])
- Safety V (c.f. Safety I and II [4])
- Dependable software reliability techniques



There is also an acknowledgement that existing tools have limitations (eg. They tend to focus upon single failures) and will find it difficult to cope with more complex systems. It's therefore expected that new tools/techniques will be required to enable safety analysis of increasingly complex systems without incurring disproportionate time or cost.

And finally, what club achievements will we be celebrating over the previous 30 years?

On a fundamental level, one basic achievement will be for the club to still be going strong in another 30 years' time and still fulfilling its community objectives. The Covid pandemic has been a challenge to the club financially, and has demonstrated how much it depends on its members and in the knowledge-sharing environments where it thrives.

As well as having much increased membership from all around the world, a demographic of much younger members is anticipated, with the range of safety concerns also expanding in a more intersectional way, to include areas such as environment, sustainability, ethics and inclusion.

By expanding the scope of safety to include ethics, sustainability and the wider societal benefits and impacts, the club will have played a more influential role in government policy making and contributed to tackling the world's bigger issues, such as global warming and inequitable risk distribution.



Embracing new media formats is also expected; the enforced move to online events in recent times has shown that multi-media events can work, and this will only get more interactive with the Metaverse, Virtual Environments and Augmented Reality.



And to conclude, might we be having our first ever successful meeting held in space or even on a different planet?

References

- [1] "Everybody Gets A Kitten", Jeremy Messersmith, from the album "11 Obscenely Optimistic Songs For Ukulele: A Micro Folk Record For the 21st Century and Beyond", 2017
- [2] Metaverse, <https://en.wikipedia.org/wiki/Metaverse>, accessed January 2022.
- [3] An Introduction to STAMP, <https://functionalsafetyengineer.com/introduction-to-stamp/>, accessed January 2022.
- [4] The Safety-II approach: Learning from what goes well, <https://www.patientsafety.com/en/blog/safety-2-versus-safety-1>, Jens Hooiveld, accessed January 2022.

Article by Paul Hampton SCSC Newsletter Editor with thanks to our Steering Group contributors: Mike Parsons, Brian Jepson, John Spriggs, Graham Joliffe and Tim Kelly.

Image attribution:

flying car: 86370063 © Pavel Chagochkin | Dreamstime.com
mars rover: 69574941 © Sergey Drozdov | Dreamstime.com
robot on train: 113031130 © Pavel Chagochkin | Dreamstime.com
nanobot 208880224 © anolil | Dreamstime.com
virtual meeting: 206600489 © Sofia Shunkina | Dreamstime.com
second life virtual environment: license by CC BY
meeting in space: 63942984 © 純一 島崎 | Dreamstime.com

Can We Quantify Risk?

Event Report



The “Can We Quantify Risk?” seminar was held on 21st October 2021 at the Radisson Blu Edwardian Bloomsbury Street Hotel, London and virtually online. This was the first in-person event held by the SCSC in over 18 months and the first to be a blended event with delegates also attending online. Mike Parsons, chair of the seminar, reports on the event and assesses how well the blended format worked.

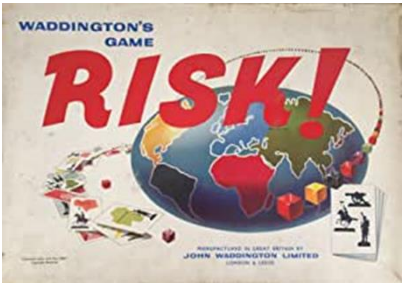
The day opened with Mike explaining how pleased he was to see delegates in person at an SCSC event! He said that the Covid-19 pandemic had made us all risk estimators to an extent. He then introduced the event mentioning some aspects of risk and new areas for discussion such as autonomous road vehicles.

This was the first blended club event (held in person and simultaneously online) since the pandemic started, and he noted that much preparation went into the event using no less than five laptops, a video camera, a mixing desk, many cables plus sound and projection systems (many thanks to Alex King and Brian Jepson for solving all the technology problems).

Risks on a Plane

John Spriggs, an independent writer and presenter, started the day with “Risks on a Plane”¹. He gave an introduction to risk, its component parts and how it can be represented within a two-dimensional plane with severity and likelihood.

He had several references to its use in aviation and the software assurance guidelines, DO-178 and DO-278. He gave some definitions of risk from international standards and explained how there were many different definitions which were not consistent. Organisational risk appetites and risk matrices were covered. He noted that risk matrices need to be maintained and reviewed as things changes – he suggested every two years is about right.



Example Risk Matrix with Risk Classes

Catastrophic Effect				
Major Effect				
Minor Effect				
Negligible Effect				
Severity Rate	Incredible	Remote	Occasional	Frequent

Red Risk Class:
Always Unacceptable

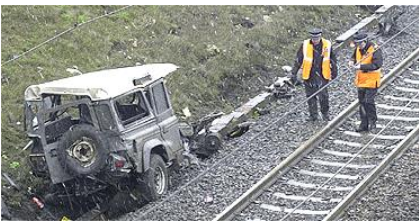
Amber Risk Class:
May be acceptable when managed appropriately

Green Risk Class:
Always Acceptable

He explained the concept of Safety Objectives as invariants for that system and organisation. He summed up with “Establish your number system, then use it as the basis of your Risk Classification Scheme, which is developed by eliciting the client’s risk appetite. Document it, declaring all assumptions”. Addressing the topic of the seminar, he explained

that to the question “Can we Quantify Risk?” the answer is “Yes, you can quantify risk but be careful how you use the numbers...”.

Risk quantification with a lot of data (but limited knowledge) – Building a road risk tool after Selby



James Catmur of J C & A explained some of the situations he had been in over his career in rail and road. He gave some of the background to the Selby accident in 2001 when a vehicle crashed down an embankment and caused a train to derail and another train to crash into the wreckage. Ten lives were lost and 82 injured, the worst rail disaster of the 21st century in the UK [1].

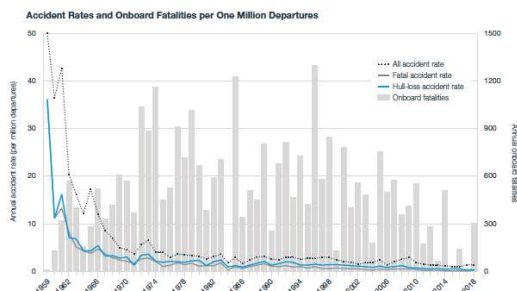
He explained how road crash maps are maintained for UK (crashmap.co.uk) and lots of data on causes is available via the UK government website [2]. He said that human understanding of risk is very biased: people have a tendency to overestimate the frequency/risk of things they have experienced, underestimate the frequency/risk of things they have never experienced, believe they know all about road safety and use ‘rationally motivated ignorance’, i.e. “what you don’t know can’t hurt you”.

¹ A nice pun given John’s aviation background!

He said that risk assessments need to be kept simple and understandable, and the logic (i.e. the working or methodology) behind any numbers produced should always be shown. On the roads we have both Unsafe Acts and Unsafe Conditions so both need to be factored in, but they are different. When managing risks, it is important not to push risk from one group to another, i.e. it would be easier to make some roads lower risk for cars but higher risk for motorcycles. He said we need to seek to reduce our ignorance, i.e. find information to fill in the gaps. There was a lively debate about abuse of hard shoulder lanes on motorways and he explained that you should always wait outside the vehicle and upstream.

Quantitative Risk Analysis: Purpose, Prediction, Problems & Possibilities

John McDermid was on next after the coffee break and explained the difference between Retrodiction and Prediction with the former being the assessing of actual risk, posed by some (class of) system operating in an environment, over some period of time. He used the Boeing accident data plot to illustrate:



Prediction is where we estimate risk which will be posed by some (class of) system operating in an intended environment prior to deployment (or update), perhaps to inform regulatory approval or to inform insurance. He explained that we should be operating on a continuum – updating predictions from operational data, but this rarely happens.

John had some good quotes to illustrate that prediction is difficult: "Prediction is very difficult, especially if it's about the future."² and "Remember, John, if a safety case contains numbers, then they are wrong."³

He noted that the Watchkeeper accident rate appeared to much higher than initially predicted with several documented accidents. The majority of John's talk was taken up with an assessment framework and maturity model for Quantitative Risk Assessments based on a study and paper "Fixing the cracks in the crystal ball: A maturity model for quantitative risk assessment."



Fixing the cracks in the crystal ball: A maturity model for quantitative risk assessment

Andrew Rae, Rob Alexander*, John McDermid¹

John listed some of the issues with these models: (i) if the system is safe enough then it may not get any meaningful feedback during the operational life, (ii) models normally assume stationary stochastic processes, but the environment and system change, and (iii) they don't account for "black swan" (very rare and very severe) events.

² Attributed to Niels Bohr (various versions). Also attributed to Mark Twain, Yogi Berra ...

³ Former BAe Military Aircraft Chief Safety and Airworthiness Engineer.

He then outlined the maturity model with five levels: **Unrepeatable**, e.g. data sources not stated or analysis pre-dates the final design, **Invalid**, e.g. human/software causes not considered in accident sequences (incomplete, partial), **Valid but inaccurate**, e.g. incorrect assumptions on independence, **Accurate but challengeable**, e.g. use of data from other systems is controversial and **Ideal** – unattainable perfection.

He finished by considering assessment of AI/ML systems illustrated by a discussion of the Uber Tempe accident. His conclusion was that QRA can lead to false confidence in systems but it is possible to utilise the maturity model to get “better” QRA and a basis for reasoning about the figures in a safety case. He said the AAIP’s main focus is on autonomy but noted that the performance measures for systems involving machine learning (e.g. for object recognition on the road) are typically in the range of $9X\%$, not 10^{-X} as we might hope.

Varieties of Risk

Peter Ladkin of Causalis started his talk with a short history of risk estimation and its origins in the insurance industry in London where ships and their cargos could be covered via negotiations conducted in London coffee houses:

He detailed the many and varied definitions of risk in international standards. He explained that there can be both positive and negative risks. The distinction of uncertainty and risk was historically defined as “Risk is when you know the probabilities; the die is fair. Uncertainty is when you don’t know if the die is fair or not.”



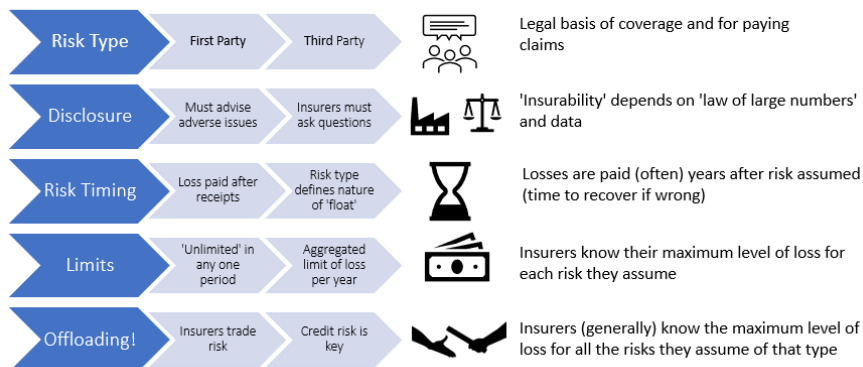
The Fukushima nuclear accident was discussed and the problems of insuring nuclear risks highlighted. In the UK, Nuclear Peril, i.e. environmental release of radioactive material or breach of the Reactor Pressure Vessel (RPV) is not insured commercially and is something for government. World-wide nuclear accidents were discussed and the possibility that Chernobyl could have been so much worse if a radioactive cloud had landed on Kiev.

Cyber-security risks were thought to be another sort of risk, as they are dynamic as opposed to safety risk which is generally considered static.

How the insurance industry quantifies and prices risk



Key aspects of Insurance



Clive Thompson of CTRL/2 gave a very interesting perspective of risk from the insurance industry. He explained that risk was viewed as opportunity for the industry, and it was a massive global business. Insurers need to be able to quantify risk to be able to calculate premiums. He explained five key aspects:

- **Risk Type:** first party e.g. buildings and contents vs. 3rd party such as public liability
- **Disclosure:** the underwriter needs information to assess the risk
- **Risk Timing:** including the importance of paying the premium in advance of any claim
- **Limits:** i.e. caps on payouts depending on risk taken on
- **Offloading:** spreading risks by using re-insurers

He explained that now in the digital age, multiple sources of information (e.g. big data analytics and satellite data for weather risks) are available to assist. Insuring some new types of risk e.g. autonomous road vehicles was also discussed.

The day finished with a lively panel discussion with four of the presenters (with three in the room and Peter Ladkin from Germany).

It was felt the day went very well with interesting and useful presentations, good discussions, and the technology for blended seminars had performed better than expected.

References

- [1] https://en.wikipedia.org/wiki/Selby_rail_crash, accessed October 2021
- [2] <https://www.gov.uk/government/statistical-data-sets/reported-road-accidents-vehicles-and-casualties-tables-for-great-britain>, accessed October 2021.

Image attribution

top image: 158612573 © Mitch Hutchinson | Dreamstime.com

risk game: Image of the game version produced by John Waddington Ltd. RISK! Is now owned by Hasbro Inc.

Selby crash: from The Guardian and Design Manual for Roads and Bridges

Fukushima: TEPCO CC BY-SA 2.0



Seminar: Safety of Autonomy in Complex Environments

**THE SAFETY-CRITICAL SYSTEMS CLUB,
Seminar:**

Safety of Autonomy in Complex Environments

Thursday 22 September, 2022 - London, UK and blended online

This 1-day seminar will consider the safe use of autonomy in complex environments (for example a self-driving vehicle in a city environment), based on the work undertaken over the last couple of years at the Assuring Autonomy International Programme (AAIP) at the University of York. This work has produced a framework document, "Guidance on the Safety Assurance of Autonomous Systems in Complex Environments (SACE)" authored by Richard Hawkins, Matt Osborne, Mike Parsons, Mark Nicholson, John McDermid and Ibrahim Habli. This outlines techniques and approaches for assurance and gives an example safety argument.

Further details TBA.

Safe use of Multi-Core and Manycore Processors



This 100th Safety-Critical Systems Club (SCSC) seminar was held both face to face and online on 11th Nov 2021. The topics centred on approaches for using multi and many core processors (MCP) in safety-related and safety-critical applications. This is a new field for industry, and there are many challenges to produce a suitable assurance argument.

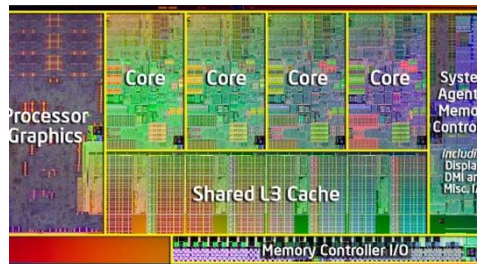
Mike Parsons introduced the seminar speakers and opened by noting that the use of such processors has been around for a while. However, the concept of using (and proving!) them in safety-critical applications is new.

Multi and Manycore Safety Working Group (MCWG)

Lee Jacques from Leonardo (and co-chair of the working group) gave an overview of the group covering past, present and future plans.

The past

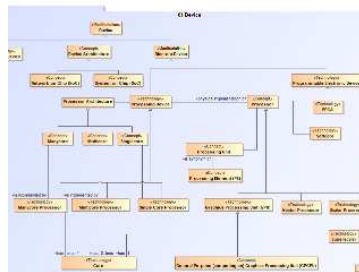
Lee explained the (relatively young) history of the group and that it was created to discuss the challenges around multicore certification and the creation of CAST-32A – a multicore position paper by the Certification Authorities Software Team (CAST). The group has made some good progress in creating a common ontological model, and a number of sub groups have shared knowledge and information thus creating some strong networks.



Present



Whilst initially making good progress Lee highlighted that, the group has started to struggle, as the scope of the sub groups was too wide and introduced significant overlap. The ontology group however, was able to



maintain a good pace as it has a defined and bounded scope of activities, which provided the team with a clear focus. Other challenges related to resource availability and the sharing of specific Intellectual Property (IP) were noted.

Future

Lee explained that the group was intending to refresh its approach and take a leaf from the ontology group by defining a clear set of well-defined tasks. The current approach was trying to cover a set of objectives that were too broad and a defined focus on clear smaller tasks would be more effective.

Lee asked the group for ideas and challenges that can be used to build a backlog of tasks, which the group can tackle in this new approach.

The Safety and Security Considerations for the Use of Multi-Core Processors

Mike Standish from DSTL and Mark Hadley from Atkins, presented how safety and security should be considered when undertaking certification of MCPs.

They noted a number of challenges including an inability to make an “in service” case, as this technology is not generally in use within a safety-critical component yet. Also, the complexity of these devices means that it is critical that the user understands the device, its architectural performance, boundary, longevity and specific configuration. Without understanding all of these parameters, the ability to make a reasoned assurance case is challenging.

They introduced the “wheel of qualification” (Hadley & Standish 2019) and emphasised the need to make a diverse assurance case relying on various types of evidence and not just (for example) a measure of worst-case execution time (which although perfectly valid, cannot be used alone to justify assurance).

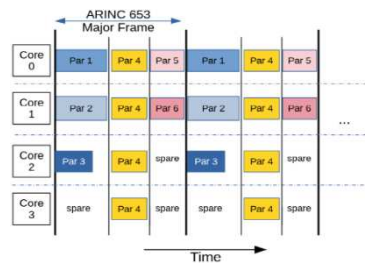
Although a challenge for MCP certification, Safety is relatively well-known in terms of process and assurance. Security on the other hand, introduces additional challenges and does not live in harmony with safety. For example, security patches, whilst necessary, can invalidate (or at least cause a re-evaluation) of an assurance case.



Mike and Mark’s closing note was that MCP certification is not just about the MCP, it’s about

the whole ecosystem around the solution. This extends from the hardware setup and development environment through to the supply chain.

Incremental Assurance of Multicore Integrated Modular Avionics



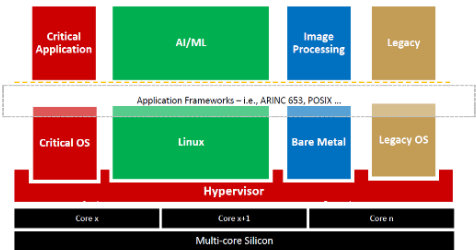
Guillam Bernat from Rapita, discussed the challenges of certifying Integrated Modular Avionics (IMA) with MCP solutions and techniques for performing performance analysis. Using Rapita tools, it is possible to monitor all aspects of MCP performance using embedded RapiDaemons. The challenge with a traditional IMA solution means a significant amount of recertification is required when changing one item.

Guillam stated that careful consideration of the partitioning model and use of automated testing is critical to success. Whilst it is possible to automate data gathering activities, there is a significant amount of manual analysis required to interpret the data.

The presentation highlighted potential test solutions using interference generators to mitigate the challenge of identifying and verifying interference paths in a multicore solution. Guillam continued detailing how this could be used in a mixed criticality context, crucial for keeping time and costs down and easing the certification burden.

Multicore Processors usage in Certified Avionics: How Virtualisation Can Help?

Olivier Charrier from WindRiver, explained how the use of virtual machines can provide the assurance required when partitioning multicore systems. Olivier stressed the importance of considering the architecture and requirements early, and just as importantly as the test strategy. He highlighted that as important as this is, it's also important to consider that assumptions made early on in the process may not fully hold going forward, and that continuous test and evaluation can drive design choices.



The presentation then went on to focus on the potential benefits of using virtualisation to provide a complete partitioning solution (memory, CPU, Cache, etc). Using virtualisation (managed by a Hypervisor) would support an assurance case by providing a well partitioned solution and would address many of the resource usage aspects of CAST-32A. That is of course, assuming you have done the upfront work to determine that virtualisation is an appropriate architecture for your solution!

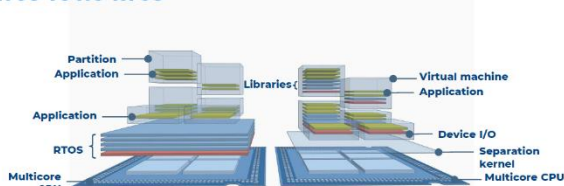
Telemetry and bare-metal Virtual Machines for Improved Multicore Partitioning

Tim Loveless from Lynx Software Systems gave an overview of Hypervisor technology, which was widely regarded in the seminar as one of the clearest definitions people had seen.

Tim started by noting that most people assume that to ensure a well-partitioned system, you need an ARINC653 based Real-Time Operating System (RTOS). Whilst in many cases this is the correct solution, he noted that for some architectures it is possible to run a bare metal hypervisor to improve performance and reduce complexity'. Do you really need that Ethernet stack and file system?

Tim introduced a number of potential patterns, which could be used to deliver a compliant bare metal solution and also introduced the CPU Performance Management Unit (PMU). This is a key component when testing and characterising your CPU as it provides a series of counters measuring everything from number of instructions completed to data misses. He warned though although important for characterisation, they introduce an overhead into the system and the more complex the system, the more integration with the RTOS is required. Think how often, how and when you are going to store or offboard the data whilst trying to maintain multicore, real-time performance...

RTOS VS NO-RTOS

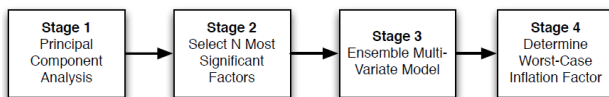


Multi-core architectures and timing analysis: Their influence on the scheduling of certifiable real-time systems

Iain Bate from the University of York presented some techniques for analysing multicore architectures and building a timing analysis approach to most effectively assess the performance of a system.

As many other presenters noted, it is key that all of this activity needs to be considered up front and that system architecture understanding is key. For example, what CPU resources are being used, what resources are being shared, what partitioning approach should be considered etc. Making design decisions is difficult as the software implementation affects the performance, but at this stage the software has not been written.

Iain presented a 4-step process to introduce some rigour into the process and help guide the identification and mitigation of the key interference factors.



Certification aspects of Multicore

Sam Riley from Frazer Nash (Formerly MAA) gave an insight into the thinking of a certification authority based on first-hand experience and noted that there is no definitive approach and positive engagement with the authority is key.

He concluded by discussing 7 general "lessons" from his experience to help those preparing safety cases, for example, ensuring that evidence is diverse and that key people, such as the design leads and regulator, are taken "along on the journey" from an early stage.

Report by Lee Jacques, MCWG Co-Chair

Getting to Know You

An update from the Safety Futures Initiative



As we've seen from our previous forward-looking articles, developing the next generation of safety engineers will be critical to ensuring the club can continue to make systems safer over the next 30 years. Zoe Garstang, lead for the Safety Futures Initiative (SFI), provides an update on the progress made by the SFI and provides details of future events.

Get To Know You Event

The Safety Futures Initiative (SFI) held their second set of 'Get to Know You Events' on 24th November 2021, with a lunchtime and evening session. The presentation material used at these sessions is available on the SFI webpage (www.scsc/gf).

The events built on the feedback received from the July events and planning is underway for new activities throughout 2022, including a lecture competition.

Due to the changing nature of these activities, please keep checking the SFI webpage for the most recent updates.

Looking Ahead

There will be further regular Get to Know You Events for new and existing members to come and find out more about the group and its upcoming activities. The dates for 2022 will be communicated via the website, social media and directly to SFI members.

At the Safety-Critical Systems Symposium (SSS'22), taking place on 8-10th February 2022 (<https://scsc.uk/e797>), there will be an opportunity to learn more about the SFI and meet new and existing members in person.

This will take place as part of the Working Group's session at 9:00am-10:00am on Wednesday 9th February 2022.

"planning is underway for new activities throughout 2022, including a lecture competition"

Membership

The first year's membership of the SFI is free, so I would encourage anyone who would like to get involved to sign-up (please see www.scsc.uk/membership).

SFI members get access to all SFI events and activities, as well as discounted fees at SCSC Events.

Further Information

If you are unable to attend SSS'22 or would like further information about the SFI, please do get in touch with Zoe Garstang (zoe.garstang@scsc.uk).

Zoe Garstang, Airworthiness Engineer and SFI Lead

Zoe is a Flight Safety Analyst at BAE Systems, providing in-service support to the Typhoon aircraft. She previously undertook an Advanced Engineering Apprenticeship with the company before joining the Continued Airworthiness team.



Safety Futures Initiative:

Get To Know You Events

Come along and find out what the 'Safety Futures Initiative' can offer you and how you can get involved.

More details at: www.scsc.uk/gf

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

Authors of papers published in this Newsletter or in the eJournal will be offered a year's free membership of the Safety-Critical Systems Club.

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

Twitter

Follow the Safety-Critical Systems Club's 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 over 1,000 members 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

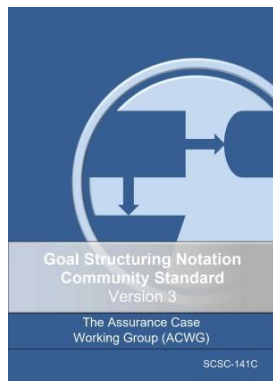
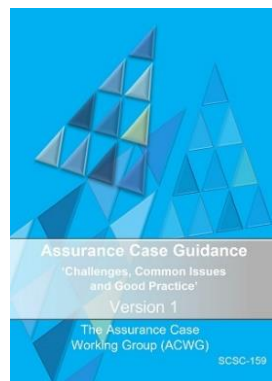
The Safety-Critical Systems Club is committed to supporting the activities of working groups for areas of special interest to club members. The purpose of these groups is to share industry best practice, establish suitable work and research programmes, develop industry guidance documents and influence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

Assurance Cases

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

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

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



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

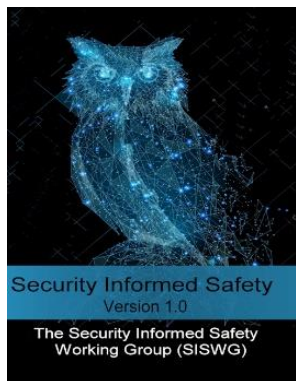
See scsc.uk/gsn for further details.

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

Lead Phil Williams phil.williams@scsc.uk

SCSC Working Groups

Security Informed Safety



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

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

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

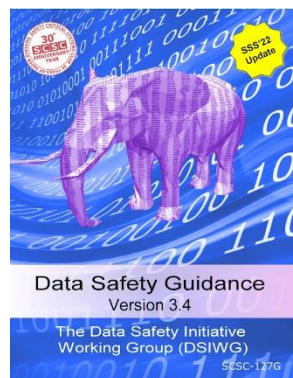
Lead Stephen Bull stephen.bull@scsc.uk

Data Safety Initiative

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

It is acknowledged that data has been a contributing factor in several incidents and accidents to date, including events related to the handling of Covid-19 data. 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.

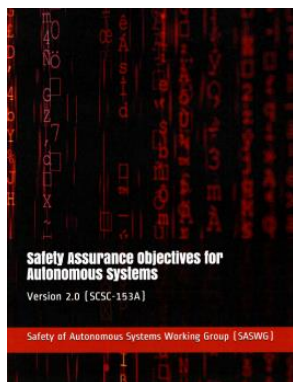


An update to the guidance (v3.4) was published in Jan 2022: scsc.uk/scsc-127G

Lead Mike Parsons mike.parsons@scsc.uk

SCSC Working Groups

Safety of Autonomous Systems



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

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

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

The group published v3 of its guidance Safety Assurance Objectives for Autonomous Systems, in Jan 2022 scsc.uk/scsc-153B

Lead Philipa Ryan pmrc@adelard.com

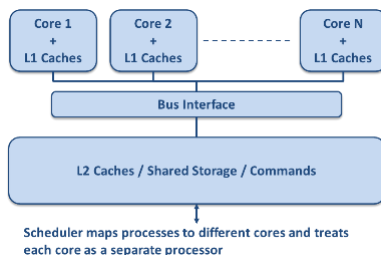
Multi- and Manycore Safety

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.

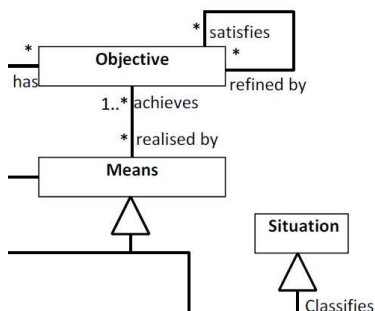
The Multi- and Manycore Safety Working Group (MCWG) has been established to explore the future ways of assuring the safety of multi- and manycore implementations.

Lead Lee Jacques Lee.Jacques@leonardocompany.com



SCSC Working Groups

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.

The OWG is currently working on the definition of an ontology of risk for application in guidance for risk-based decision making – notably safety and security – and for which ISO 31000 Risk Management principles are to be applied.

The Data Safety Working Group (DSIWG) developed the core aspects of the Risk Ontology, which has been

migrated to this working group. The Risk Ontology will form the upper ontology to the Data Safety Ontology that the DSIWG will continue to develop.

Lead Dave Banham ontology@scsc.uk

Covid-19



The Covid-19 Working Group is involved with discussion, analysis and assistance related to the Coronavirus. The group meets remotely to see what a systems and assurance view of the situation brings.

The group has compiled an extensive range of Covid-19 related material and made this available on the working group's website pages along with ongoing developments in the thoughts and ideas of the group.

Members are all experienced engineers, used to making reasoned arguments about safety. The aim is to apply the groups considerable technical expertise to the problem and find and assure appropriate solutions.

Lead Peter Ladkin ladkin@causalis.com

SCSC Working Groups

Service Assurance

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

The group published v3.0 of the guidance in Jan 2022: scsc.uk/scsc-156B

Lead Mike Parsons mike.parsons@scsc.uk



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.

The group is planning to hold an event early in 2022.

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

60 Seconds with ...

Dr Mike Parsons



Mike has worked for many years in the safety industry across diverse sectors such as Defence, Aerospace, Rail, Healthcare, Nuclear and Government. He has worked for Logica, CGI, NATS, and he is now a research fellow in the AAIP at the University of York working on the assurance of autonomy.

His career started back in 1988 when he worked on medical imaging systems, progressing through projects including space launch tracking systems, satellite navigation, healthcare applications and civil aviation messaging.

He is also the SCSC Director and Events Organiser, and leads two of the SCSC Working Groups on Data Safety and Service Assurance.

You've said before that your childhood dream was to be an astronaut. What aspect of space travel interests you the most?

I think it's the idea of complex systems working in a difficult and unforgiving environment and enabling new discoveries and applications. The idea that the systems in space stations, Mars rovers or deep space probes have to be super-resilient and be able to work autonomously is fascinating to me.

What aspect of your career are you most proud of?

That's easy: building communities of safety engineers to achieve a goal. I did this working at Logica where I created the safety community and also a safety practice; but to me, the SCSC embodies this completely. Becoming Director of the SCSC and running the Safety-Critical Symposium gives me a real buzz! I am really proud of the work I have done on the SCSC Working Groups (Data Safety and Service Assurance) and also at events where we all have a strong common purpose and work together to achieve it. In terms of projects, it would have to be the Ariane launch vehicle tracking and monitoring system I did for Logica and subsequently installing the kit at the launch site in French Guiana.

What advice would you give to yourself age 12?

Follow your dreams, but be prepared to be side-tracked! I think my dream of being an astronaut led me to work in the Space Sector, then in Safety, then for the SCSC. Safety is such an interesting and challenging area: I like the way it requires systems thinking as well as an appreciation of wider things like legal and ethical aspects, together with the constraints of what is possible. I would never have appreciated this as a 12-year-old, but it's important to give your career time to explore: some roles you don't even know exist may suddenly appear. I would also say don't be afraid: reach out and take on something new – you will find a way – and opportunities don't appear twice.

What worries you the most about the future of System Safety?

I am really concerned that our techniques for analysis of complex systems are not up to the job; systems are becoming ever more dynamic and distributed, with vast hidden complexities (and autonomous functionalities). Also, security needs to be properly integrated with safety. I think we need a whole new suite of powerful tools allowing us to reason about these systems. Historically, safety engineering has learnt from accidents. What worries me is that we'll have some terrible accidents (e.g. involving self-driving vehicles) and not be able to work out why it happened...

What's your most favourite quote or motto?

I always liked a saying we used to have at Logica when reviewing risks on new projects "Would it pass the headline test?" In other words, if the system or software developed went wrong and an accident resulted, could you construct a snappy 'tabloid-style' headline blaming us? If you can, then the system is likely not safety engineered enough...

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

Learn how to move around in a zero-g environment. Since being an astronaut is still somewhat unlikely, this might have to be done in one of the commercial zero-g flights now on offer. Also I think it would great to dive to the deepest ocean floor in a submarine – anything which takes me to new environments.

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

Possibly Mark Watney from The Martian – I love the way he solved the hard problems while abandoned on Mars. I do like a good detective story, and I think Max Liebermann from Vienna Blood is an interesting twist.

"Becoming Director of the SCSC and running the Safety-Critical Symposium gives me a real buzz!"

What's the best piece of advice you've ever been given?

Perversely, "take a risk!" This was explained to me back in 1995 on my first Logica project and is important – safety engineering is all about managing risk, not eliminating it altogether.



Which song title best sums up your experiences with Covid-19?

"David Sylvian – World Citizen (I Won't Be Disappointed) / Looped Piano Version" sums up the sense of alienation, isolation and strangeness of the pandemic with a safety theme. I also really like "Patricia Barber - Icarus (For Nina Simone)" - I've listened to a lot more jazz over the last two years and this is a lovely example, with a risk and aviation topic.

SCSC Membership

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

Individual Membership

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

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

Corporate Membership

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

Renewing Membership

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

Membership Fees

The following fees are applicable for new and renewing members:

- 1 year Individual Membership: £125
- 2 year Membership: 20% discount: £200
- 3 year Membership: 33% discount: £250 (3 years for the price of 2)
- 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 publications in a particular calendar month.

Contact Alex King using office@scsc.uk

The SCSC Steering Group



Tom Anderson
Honorary member



Robin Bloomfield
Honorary member



Stephen Bull
stephen.bull@scsc.uk



Dewi Daniels
dewi.daniels@scsc.uk



Jane Fenn
jane.fenn@scsc.uk



Zoe Garstang
zoe.garstang@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



Graham Jolliffe
Honorary member



Tim Kelly
Honorary member



Alex King
alex.king@scsc.uk



Mark Nicholson
mark.nicholson@scsc.uk



Wendy Owen
wendy.owen@scsc.uk



Mike Parsons
mike.parsons@scsc.uk



Felix Redmill
Honorary member



Roger Rivett
roger.rivett@scsc.uk



John Spriggs
john.spriggs@scsc.uk



Emma Taylor
Honorary member



Phil Williams
phil.williams@scsc.uk



Sean White
sean.white@scsc.uk

Club Positions

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

Managing Director

Mike Parsons 2019-

Tim Kelly 2016-2019

Tom Anderson 1991-2016

Steering Group Chair

Roger Rivett 2019-

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-

Newsletter Editor

Paul Hampton 2019-

Katrina Attwood 2016-2019

Felix Redmill 1991-2016

University of York Coordinator

Mark Nicholson 2019-

eJournal Editor

John Spriggs 2021-

Administrator

Alex King 2016-

Joan Atkinson 1991-2016

Website Editor

Brian Jepson 2004-

Safety Futures Initiative Lead

Zoe Garstang 2019-

Nikita Johnson 2019-2021

Calendar

February '22

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 '22

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

April '22

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

May '22

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 '22

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 '22

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 '22

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 '22

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 '22

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 '22

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 '22

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 '23

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					

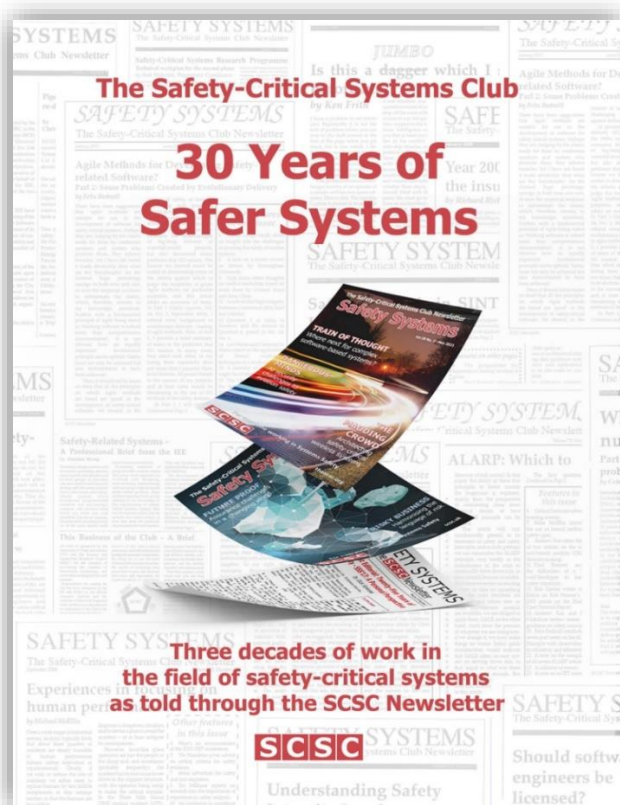
Events Diary



<p>8-10 February 2022 SCSC Symposium</p> <p>30th Safety-Critical Systems Symposium (SSS'22)</p> <p>Bristol, UK + Online</p> <p>scsc.uk/e797</p>	<p>28-29 March 2022 Conference</p> <p>16th International Conference on Safety and Systems Engineering (ICSSE 2022)</p> <p>Paris, France</p> <p>waset.org/safety-and-systems-engineering-conference-in-march-2022-in-paris</p>	<p>8 April 2022 SCSC Seminar</p> <p>Managing 'Black Swans': Handling Rare and Severe Events Now and in the Future</p> <p>London, UK + Online</p> <p>scsc.uk/e825</p>	<p>1-2 June 2022 Conference</p> <p>Reliability, Safety and Security of Railway Systems (RSSRail 2022)</p> <p>Paris, France</p> <p>rssrail2022.univ-gustave-eiffel.fr</p>
<p>6-9 September 2022 Conference</p> <p>41st International Conference on Computer Safety, Reliability and Security (SAFECOMP 2022)</p> <p>Munich, Germany</p> <p>safecomp22.iks.fraunhofer.de</p>	<p>22 September 2022 SCSC Seminar</p> <p>Seminar: Safety of Autonomy in Complex Environments</p> <p>London, UK + Online</p> <p>scsc.uk/e890</p>		

NB: all events are subject to change due to the Covid-19 situation. Please check the SCSC website for up-to-date information: scsc.uk/events

thescsc.org/membership



"30 Years of Safer Systems" contains articles from the last 3 decades of the Safety-Critical Systems Club (SCSC) newsletter "Safety Systems".

The book groups the articles into themes relevant to safety, with an introduction to the theme and a preface to each article giving major events from the year the article was first published, including accidents, incidents and positive improvements in safety. Themes include: Risk Assessment, ALARP, Artificial Intelligence/Machine Learning, Communication Failures, Safety Culture, 'Black Swan' events, Certification, Product Liability, Safety and Security Integration, Agile Methods, Data driven systems and Safety Cases.

Most of the original authors have provided a short postscript to their article to give extra context and explain progress in the intervening years.

Available for purchase on Amazon

www.amazon.co.uk/Years-Safer-Systems-safety-critical-Newsletter/dp/B09KNCYKDL