The Safety-Critical Systems Club Newsletter

Safety Systems

Vol 29 No. 2 - May 2021



TRAIN OF THOUGHT

Where next for complex software-based systems?

DANGEROUS MINDS

AI security challenges to aviation safety

THE MADDING CROWD

Architecting safety-critical wireless systems

For everyone working in Systems Safety

SCSC

thescsc.org



SCSC Publication Number: SCSC-163

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

Except where explicitly stated that licensed use of this work is otherwise restricted, this work is licensed under the Creative Commons Attribution 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by/4.0/ or send a letter to Creative Commons, PO Box 1866, Mountain View, CA 94042, USA. You are free to share the material in any form and adapt the material for any purpose providing you attribute the material to the Safety-Critical Systems Club (SCSC) newsletter, reference the source material, include the licence details above, and indicate if any changes were made. See the license for full details.

Cover image: ID 63073528 © Ian Redding | 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

Where next for complex software-based systems? 5
Emma Taylor discusses the Cambrian railway incident and overcoming the challenges of implementing the accident report's recommendations.

Cyber Security Aspects of Autonomy in Aircraft 15
Mick Warren discusses his thoughts on how autonomy will impact the cyber security aspects of safety within aviation.

Architecting Wireless for Safety Critical M2M Comms 21
Michael Green discusses the challenges around safety-related wireless communications and looks ahead at some possible solutions.

Introducing the Safety-Critical Systems eJournal 27
John Spriggs provides the background and details of the new SCSC eJournal.

SSS'21 Event Report 29
Highlights from the 29th Safety-Critical Systems Symposium – the first time the event has been held totally online.

Safety Culture Developments 35
Rick Vinter reports on the Safety Culture Development Seminar.

The SCSC is its Own Boss! 39
Mike Parsons provides the background and details of important changes to the SCSC's legal basis.

60 Seconds with … John Spriggs 47
John answers some quick-fire questions on system safety and life!

GROUPS

Working Groups 43
Details of the current SCSC Working Groups.

SCSC Steering Group 50
Contact details for members of the SCSC Steering group.

EVENTS

Calendar 52

Events Diary 53

SCSC

FOR EVERYONE WORKING IN SYSTEM SAFETY

www.scsc.uk/sss

SSS'22

Details of this and other events at: www.scsc.uk



Safety-Critical Systems Club Annual Symposium

www.scsc.uk

THE SAFETY-CRITICAL SYSTEMS CLUB

30th Safety-Critical Systems Symposium

8-10th February 2022, in-person in Bristol and blended online

The Safety-Critical Systems Symposium in 2022 (SSS'22) will be held in Bristol and blended online as a live-streamed event. This event comprises three days of live presented papers, including keynote presentations and submitted papers. There will also be an evening session on the Wednesday with additional talks.

This is our 30th Symposium and will feature talks looking back at the past 30 years, and also special anniversary events.

This event will be run in-person in Bristol at the Bristol Royal Marriott hotel and also through the SCSC website and the Whova application.

The Symposium is for all of those in the field of systems safety, including engineers, managers, consultants, students, researchers and regulators. It offers wide-ranging coverage of current safety topics, focussed on industrial experience.

It includes recent developments in the field and progress reports from the SCSC Working Groups. It covers all safety-related sectors including aerospace, defence, health, highways, marine, nuclear and rail.

The symposium features are:

- Six keynote presentations and submitted papers;
- Updates from the SCSC Working Groups;
- Audience participation and submitted questions.

And for in-person delegates in Bristol:

- A 30th anniversary banquet with after-dinner speaker;
- Proceedings book hardcopy;
- Anniversary book with specially selected articles from the SCSC Newsletter and additional introductory text;
- Special commemorative beer (or other non-alcoholic beverage) designed and commissioned for the symposium;
- Social events on the Wednesday in Bristol.

The symposium is a regular event and fosters a community spirit in the field: it is a great place to network, learn about the latest practice in safety and develop new business contacts.

To **book your place** please see: www.scsc.uk/sss

For **further information, exhibition** and **booking queries** please contact: Alex King, Dept of Computer Science, University of York, Deramore Lane, York, YO10 5GH. Email: alex.king@scsc.uk

For **technical aspects** and queries on **talks, speakers, abstracts, papers** or **posters,** please contact: mike.parsons@scsc.uk

Editorial

This month marks the 30th anniversary of the Safety-Critical Systems Club and it is a testament to all those involved in running the club over the years and, of course, its members, that it continues to thrive, even under the adverse circumstances that Covid-19 brought into play. Covid-19 has nevertheless meant that the club has had to evolve in certain areas. In particular, after several years in happy partnership with the Universities of Newcastle and York, the club has now parted ways and become a Community Interest Company (CIC). As a CIC, the club is now its own legal entity with financial autonomy and the ability to set its own direction for the benefit of all club members. Mike Parsons explains the background and the impact on membership in detail on page 39.

Covid-19 has also meant that, for the first time in its history, its annual SCSC Symposium was run entirely online. See page 29 for my report on the event's highlights. The club is now already preparing for next year's event – SSS'22 – to be held in Bristol, UK. This will be a blended event with a mixture of physical and online attendance anticipated. As this is the 30th anniversary Symposium, there will be special events and activities to mark the occasion, so not one to be missed! See the opposite page for further details, and see the back page for the call for abstracts if you would like to submit content for the event.

The SCSC Working Groups have however continued to thrive with the Service Assurance Working Group publishing an update to their Service Assurance Guidance (scsc.uk/scsc-156A) and the Assurance Cases Working Group publishing a new version of the Goal Structuring Notation Community Standard (scsc.uk/scsc-141C). The Safety Futures Initiative is also launching with two 'Get to Know You' events on 1st July 2021 (scsc.uk/e828).

Another exciting change for the club has been the launch of an eJournal to complement the Newsletter. The eJournal is intended as a platform to publish longer and formally peer-reviewed papers, with two issues planned per year. As with the newsletter, the eJournal will be free to download for SCSC members. John Spriggs, our new eJournal editor, provides more details on page 27. 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, so please get in touch with John or myself if you are interested in having your work published.

We also want the club's work to be accessible to the wider community, so there are plans to make annual print volumes of the newsletter and eJournal available to purchase by non-members. We are also introducing a one-month access pass to all SCSC content for non-members. This is being established to allow SCSC material to be available to those who require access to it, but for whom it is not practicable to become full SCSC members.

In this edition of the newsletter, we lead with an article from Emma Taylor who asks "where next for complex software-based systems?" We then have an article from Mick Warren on the challenges with cyber security of autonomy on aircraft, and Michael Green discusses data safety risks with machine-to-machine wireless communications. Rick Vinter also reports on the recent Safety Culture Developments Seminar.

Our 60 second interview is with John Spriggs.

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



In Brief



Software flaw led to 'serious incident' on TUI flight

	EST	MAX	ACTUAL
DOW	042650	------	.....
PLD	015918	------	.....
ZFW	058568	061688	.....
TOF	007927	020895	.....
TOW	066495	078999	.....
TF	005281	------	.....
LDW	061214	065317	.....
REM	002646	------	.....

A "simple flaw" caused by a language difference led to a "serious incident" for a flight from Birmingham last year. All female passengers whose title was "Miss" were classified as children – not adults – on the TUI flight after a software upgrade. *bbc.co.uk*



Covid: Man offered vaccine after error lists him as 6.2cm tall

A man in his 30s with no underlying health conditions was offered a Covid vaccine after an NHS error mistakenly listed him as just 6.2cm in height. Liam Thorp was told he qualified for the jab because his measurements gave him a body mass index of 28,000. *bbc.co.uk*

Goodwood Will 'Carefully Consider' Future Flying Car Demonstrations After Airspeeder Crash



The aviation club based at Goodwood Motor Circuit has said that any future drone or flying car displays will be carefully considered in line with new official recommendations, following a crash that only narrowly avoided houses near Chichester. Investigators said there was a "high risk of fatalities" when the Alauda Airspeeder Mk II prototype became unresponsive, rose nearly 8,000ft and then plummeted to the ground after running out of battery during the test over Goodwood Aerodrome, West Sussex, on July 4, 2019. *driving.co.uk*

'Self-driving' cars to be allowed on UK roads this year



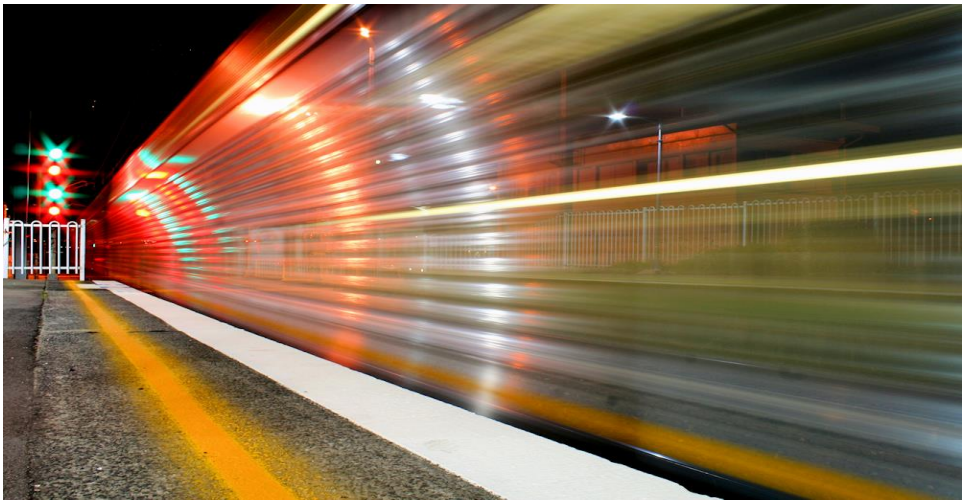
The Department for Transport said automated lane-keeping systems (ALKS) would be the first type of hands-free driving legalised. The technology controls the position and speed of a car in a single lane and it will be limited to 37mph (60km/h). But insurers have warned the government's definition of ALKS as "self-driving" is misleading. *news.co.uk*



Mercedes recall more than one million popular road cars after safety tool glitch

Mercedez Benz has issued a recall for more than one million cars over a problem with the vehicle's emergency call system which could be a safety risk. Mercedes Benz said the problem could mean emergency services are not given the "correct current position" of the vehicle. The eCall system is designed to automatically alert emergency services when the car crashes and relays location information directly to them. *express.co.uk*

Where next for "complex software-based systems"?



Dr Emma Taylor discusses the Cambrian railway incident and the roadmap for overcoming the challenges of implementing some of the Rail Accident Investigation Branch (RAIB) report's recommendations. Emma reflects on where and how the next insight-generating Cambrian-type analysis might come from, and considers whether the context provided by "cybersecurity" might add a complementary framework to create more clarity.

As an experienced safety engineer, used to imagining and asking, "what if (this happens)?" – in a rigorous and structured fashion of course – it can sometimes feel as if I inhabit a different world to many of my differently disciplined colleagues. For them, designing to requirements, standards and environmental and operational constraints to meet client and legislative requirements provides a focussed target. In contrast, safety can seem a bit open ended, for them we never seem to be in a position where we can stop worrying.

Whatever sector we work in, working in safety means that we rightly 'lean in' to the challenge of exploring and communicating the many combinations of potential paths to system malfunction (both potential and realised). Pointing to previous incidents and near misses remains an effective way of raising awareness and action, and as trends emerge through reporting and analysis, the evidence for a sustained and focussed campaign of action is strengthened. In some sectors such as rail, the requirement to report, understand and share through common systems is codified in legislation. For an overview of complex software-based systems and failures, many of the Safety Critical Systems Club events and publications contain useful guidance and analysis e.g. [1, 2].

This sharing of expertise is a complementary driver for change which sits alongside industry and system-wide changes following major accidents. The latter, perhaps unfortunately, remains an established route for effecting a change in the management of risk. High profile multi-fatality accidents, recently noted for complex software-based systems, such as the Boeing 737 MAX, increase both attention and action. Despite this, identification and understanding of the causal factors, and implementation and supervision of measures to manage the risk remain complex in nature – particularly when anticipating what has not yet happened.

Fortunately, a structured framework for analysis provided by standards and guidance is a recognised route for action, working through identification and implementation of risk mitigation measures ('controls') and spanning across the recognised triad of technology, people and processes. While there are challenges associated with the application of such standards, this is a recognised approach for safety-critical systems, and often also part of a required regulatory and commercial baseline. Third party and independent assessments also play an integral part in the verification and validation over a project lifecycle.

But what changes when you are operating outside the tight constraints of such a framework, or when the framework is not fully implemented? What happens when you are looking at trying to prevent types of failures that are not yet realised or recognised? Is it then still suitable to maintain a focus on learning from lessons identified? What about systems with different SIL levels that are connected? What limitations might occur? And how can the individuals and organisations adapt to the changes being caused through complex software-based systems?

This article provides a brief and personal commentary framed by these questions as seen through the perspective of being part of an industry team addressing recommendations published by Rail Accident Investigation Branch (RAIB) for an incident on a digital signalling system known as ERTMS (The European Railway Traffic Management System).

The full report is available publicly and includes an overview of the ERTMS signalling system, the incident and investigation, and subsequent recommendations placed on industry [3]. A briefing on the UK rail regulator's approach (Office of Rail and Road, ORR) to tracking the recommendations is available [4] and the ORR's publicly available report to RAIB on industry progress at the end of 2020 has been published [5]. A glossary of terms used may be of use for readers who are not familiar with the rail sector, particularly when specific terms are used by RAIB noting specific actions [6]. Industry continues to progress, with timelines set for formal resolution of the recommendations. But some of the questions raised by implementation of the actions themselves have been difficult to answer, and it is the path that's been taken and hurdles identified that are explored in this article.

Loss of safety critical signalling data on the Cambrian Coast line

The ERTMS system is based on the principle that a train driver receives signalling information (including line speed and temporary speed restrictions) from a digital display in the driver's cab. Digital information is transmitted two-way using train communication systems, and wayside computer-based systems are used to manage and update the information used on board by the driver. This necessitates software, databases stored on servers and manual entry of information by technical staff. This may occur when changes to the speed profile are required, such as a temporary speed restriction to reflect operational needs e.g. change in track condition or other temporary condition requiring a slower speed.

Over the past few years, ERTMS has been trialled on an operational line (the Cambrian Coast line) as part of the development towards broader deployment on the GB mainline rail network. On the 20th October 2017, a train driver noticed that a temporary speed restriction that they were expecting to see on their in-cab display was no longer there. It was only when they 'called it in' to the signallers asking what had happened that it was identified that the temporary speed restriction element of the ERTMS system had not functioned as expected. (Note that the temporary speed restriction in question was in place to prevent trains passing a level crossing too quickly so the consequences of a potential collision could have been quite severe). RAIB launched an investigation to work out what had happened and why.

To understand the context, it is key to map out the equipment, software and operational steps involved in providing the driver with signalling information (provided as part of a 'movement authority'). An operational train line is divided into segments and passage of a train in and out of that segment is controlled via signals (there should be normally no more than one train per segment). Speed information and ensuring trains travelling at a set speed is an important part of controlling the flow from one segment to another, and operational reasons may mean that the speed per segment may need to be changed (a temporary speed restriction). This is inputted by the signaller (at the terminal for the GEST System, or 'poste de GEstion des Signalisations Temporaires') and the information is then encoded into the broader packet of information sent to the train. The Radio Block Centre (RBC) sends movement authorities to trains and the (GEST) system. An overview of the systems involved is given in the figure below, taken from the RAIB report. Further information on the design, including the SIL rating of the different systems is reported [3].

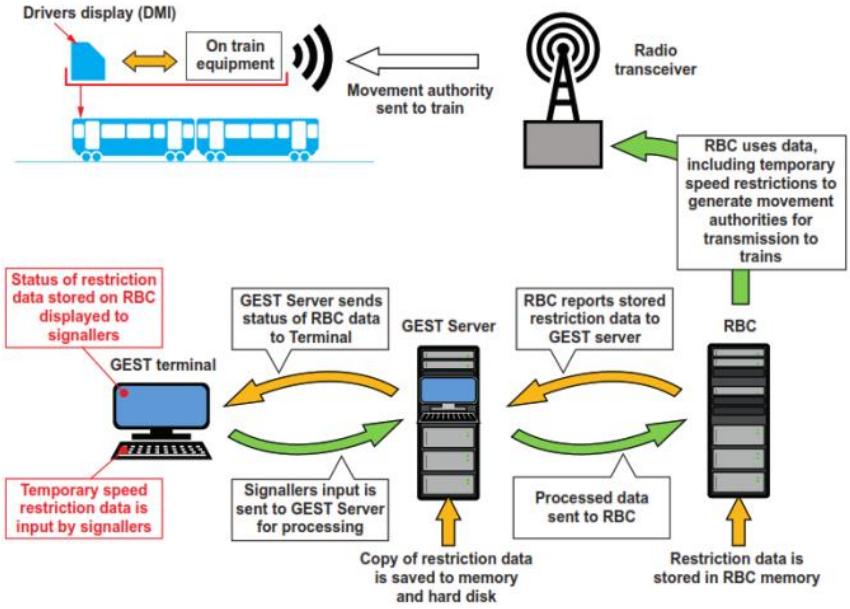


Fig 1 An overview of the Cambrian ERTMS incident [3]

Analysing a complex software-based system incident can be a complex task. The RAIB report was published on 19th December 2019, more than two years after the initial incident [3]. Comparing the date of the incident and the date of the report's publication (more than two years) hints at both the thoroughness of the investigation and the potential challenges associated with turning back time to understand where and how the root causes occur.

The process of incident investigation involved reconstructing the software development lifecycle, tracing back to when and where designs for this installation deviated from other applications of the ERTMS system, and also understanding why some local operational issues hadn't been identified and highlighted earlier. The causal factors pointed to a broad range of often foreseen problems, including problems with definition of safety-related requirements, hazard analysis process, validation of safety requirements, and design limitations around error handling/reporting, integrity checking and management of product upgrades. In the next section I'll discuss what the investigation found in the context of how industry responded to the RAIB recommendations.

An approach to implementation of some RAIB recommendations

Some RAIB recommendations (typically called 'Recs') were placed specifically on individual organisations such as the developer of the ERTMS system and Network Rail (Rec 2, Rec 4 and Rec 5) but two included the phrase "Network Rail, in consultation with RSSB and the wider industry…" (Rec 1 and Rec 3). The text of the recommendations in full are available [3]. Network Rail operated the line where the ERTMS system was installed, and RSSB is the Rail Safety and Standards Board which has a cross-industry role in a number of key areas, including railway safety.

Working in co-ordination, and with a mandate to engage the wider industry, meant that the technical challenges potentially became overshadowed by the wider engagement and communications challenge. The question of how to hit both marks became the subject of some discussion, and iterative planning by myself and others.

Network Rail, in consultation with RSSB and the wider railway industry, should review and, where necessary, improve the capture and dissemination of safety learning available through the reporting and systematic investigation of complex software-based system failures.

This need for engagement with the 'wider industry' not only reflects the prevalence of complex software-based systems across the network, but also the challenge involved in the capture and dissemination of the learning so as to create the foundation for action. It is not just information distribution for information's sake, but a necessary requirement as a route to creating greater understanding and proactive engagement with software-based systems development and operation. A separate challenge was making sure that even if content was broadcast widely, would it be received and understood; i.e. was the package 'sticky' enough to gain people's attention? Where 'sticky' means not forgotten, laying the foundation for longer-term change. A separate programme of work continues on the other 'wider industry' recommendation addressing procurement of software from a client-based perspective [4].

It was a reasonable assumption that not all incidents that could happen would have happened yet, so learning from experience ('improve capture and dissemination of safety learning') would not give a complete picture. Also, could it be assumed that there was incomplete reporting and analysis of incidents and near misses that had already happened? My view is that physical failures of railway infrastructure are usually easier to spot than those within

the digital context, unless they provoke a visible and sustained block on operations such as the National Grid power supply issue, which led to a number of trains shutting down and requiring technician restart [7]. Separate to these limitations was my opinion (shared by others) that as most people didn't have a technical basis in software-based systems, it meant that some might feel uncomfortable reading overly technical details. Reflecting, it seemed as if a formula was needed to help cut through to reach a wide audience and so 'disseminate' the safety learning.

Network Rail developed a public domain website to support their response to the RAIB Cambrian 'Rec 3' including a case study format which covered only four slides [8]:

- Description of the incident (a few bullets)
- Immediate cause (one bullet, and a picture, [fig 1])
- A summary of causal factors [fig 2]
- Mapping to the V-cycle (verification and validation) [fig 3]

The causal factors (i.e. what happened and why) were extracted from the RAIB report and then condensed down, with common themes highlighted in green, using only the RAIB form of words. Looking at this one slide allowed a non-expert to gain an overview [fig 2].

Causal Factors

- Temporary speed restriction data was not uploaded to the RBC after a software rollover because the GEST sub-system had entered a fault condition, probably due to a corrupted database.
- No indication that the system had failed was provided to signallers.
- The memory used for storing temporary speed restrictions in the RBC was volatile, allowing temporary speed restriction data to be lost during a rollover.
- The required level of safety integrity for validation of temporary speed restriction data uploaded to the RBC following a rollover was not achieved by the design.
- GEST server software was unable to detect and manage the corruption of its database.
- The vulnerability of the system to a single point of failure had neither been detected nor corrected during the design, approval and testing phases of the Cambrian ERTMS project.
- The safety-related software requirements for the GEST software were insufficiently defined.
- The hazard analysis process did not identify, and so did not mitigate against, the GEST software thread failure mode.
- The validation process did not ensure that the safety requirement for the correct display of temporary speed restrictions was met.
- GEST was accepted into service without the production of a generic product safety case (or equivalent); had such a process been followed rigorously, it would probably have exposed the shortcomings in the software design.

Fig 2 Summarised causal factors for the Cambrian ERTMS incident [8]

To create further clarity, the causal factors were then mapped to the V-cycle as shown in fig 3. This approach usefully mirrors the guidance provided by RAIB in 2019 [9].

"Demonstrating digital system safety can be difficult, but that doesn't mean that we shouldn't try to master the problem. Existing industry guidance helps us by breaking the problem down into distinct steps: specification; definition of requirements; design, checking and testing; and validation against the originally specified requirements."

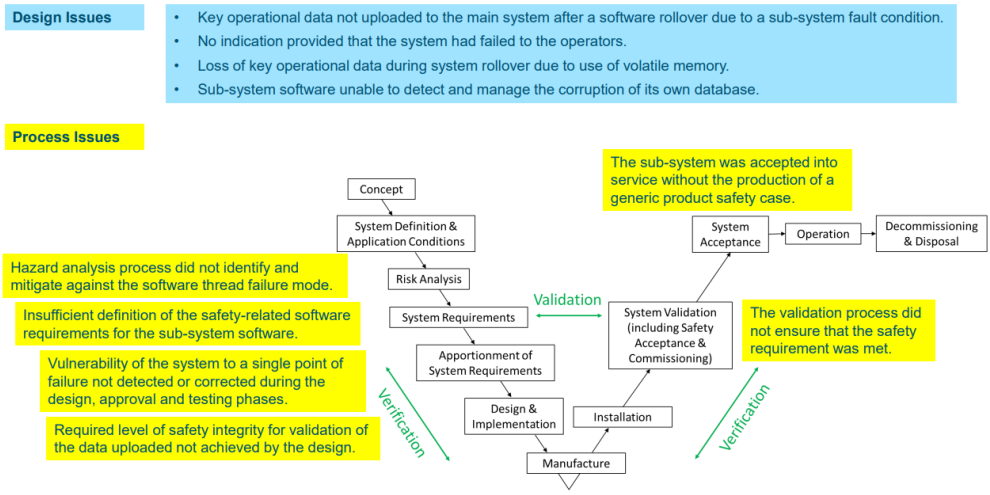


Fig 3 Mapping of Cambrian ERTMS causal factors to the V-cycle [8]

Working with the support of industry stakeholders, this formula was then used to develop 'reasonably foreseeable scenarios', further taking the causal factors and dividing them into people, technology and processes, mapping them into the categories typically used within the energy and other sectors.

The approach got people's attention, whether for real world incidents that had happened, or reasonably foreseeable ones. I – and I suspect others – started to ask ourselves: "how would we know this had happened?" thus meeting the monitoring and reporting element of the Rec, and also framing the incident within our own operational and technical experience. (Note that, although the 'reasonably foreseeable scenarios' themselves are not widely distributed, the approach is presented in podcasts and webinars, referenced later in this paper).

This need for people to be aware and able to report what they see, even if based on incomplete information capture, is part of the activity needed to address safety learning ('improve the capture' in the language of the Rec). RAIB also noted the importance of considering all reasonably foreseeable circumstances (circumstances can be taken as another term for scenarios) when developing a software system [9]:

"It is fundamental that the process of digital design is robust enough to ensure that software-based systems operate correctly in all reasonably foreseeable circumstances. In this case, the people operating the railway did not know that there was anything amiss. Digital railways need to detect when they have failed and report this to those who need to know: in this case, the signallers".

A parallel programme of work was also facilitated by RSSB to gather similar case studies across rail and other sectors [10], and to analyse and frame them within the V-cycle, delivering the case study message within a podcast format. A digital safety webinar was used to increase understanding of the importance of considering reasonably foreseeable scenarios and also the value of taking a cybersecurity perspective on train operations [11]. The concept of a 'digital train' played a key part in raising awareness and understanding of how complex software-based systems are an integral part of a transport system's operations. All

three webinar speakers met the wider engagement and communications challenge embedded in Rec 3. All of the material was made publicly available on RSSB's website [fig 4] as part of steps towards 'developing digital competency' and linked to from the Network Rail public facing page [8]. I think we got better as we went along. My favourite podcasts are the Cambrian and other case studies in a suite of four podcast episodes. The 'introduction to digital safety' one includes my Kazakhstan and space adventures too, which apparently made the software topic a bit more interesting.



Fig 4 A public resource designed to support development of digital competency [11]

At the time of writing, the RAIB Cambrian recommendation's 'wider industry' programme of work continues, including using the causal factor analysis from Rec 3 to act in effect as inspiration for "design requirements" for development of a strengthened lifecycle approach to procurement of complex software-based systems to meet Rec 1.

And, at an industry-wide level, awareness of this issue, along with an increasing call to action, continues to grow, with RAIB's Chief Inspector stating, "demonstrating digital system safety can be difficult but it doesn't mean we shouldn't try and master the problem" [12].

What else can be done – and is there another challenge to meet?

My perspective is that it's clear that the rail industry is stepping up in responding to this important incident, and that further progress will be made, noting it is 'reactive progress' as it is reacting to an incident. Improvements in the implementation of the V-cycle, combined with increased awareness at technical and procurement level as to how things could go wrong, can clearly improve the overall management of complex software-based systems. Greater awareness and use of existing safety frameworks, maturity models, standards and guidance all provide a 'thinking and doing' roadmap.

But is it enough as it is?

Perhaps more provocatively, this parallel question can also be asked:

"Could a proactive cybersecurity perspective have helped modify the pathway to this incident?"

Or, put differently, if a cybersecurity risk assessment had been carried out, could it have identified (design and operational) vulnerabilities which, if addressed, would have truncated or interrupted the steps between design vulnerabilities and realisation of the potentially unsafe situation with the temporary speed restrictions?

I also think that this question cuts to the heart of the challenge involved in complex software-based systems, well as being nothing less than an enormous can of (potentially tasty) worms, which is only just starting to be opened. As outlined in the recent seminar IET Code of Practice on Cyber Security and Safety [13, 14], considering both safety and cybersecurity is not a simple problem space and there is no one size fits all.

The speakers at the launch outlined various challenges, including the clear view expressed that you could do a safety risk assessment or a cybersecurity risk assessment, not a combined one (at least not at this time). The very few people who have the skill set to do both have to choose which hat to wear. Despite this, they stressed that steps must be taken to move things forward, as "increasing connectivity is driving complexity", not only at the technical level, but the organisational structures and cultures around the systems themselves. It's perhaps stating the obvious, but the skills and mindsets that people have need to be broadened in order for the industry to have a better chance in managing these domains and changes.

For me, my personal view is yes to a cybersecurity risk assessment, and I'll be bold in saying that I think that a high-level screening from a cybersecurity perspective should be carried out for all complex software-based systems. At a minimum, it could identify additional design and operational requirements. It certainly gets people to put their thinking caps on; I saw how the three cybersecurity speakers in the 'digital asset integrity' webinar 'cut through' to the heart of creating a real world 'here today' mindset for complex software-based systems.

We could – and I think should? – move to the position of a systems led cybersecurity review being a default starting point. And then, depending on the findings, it is then an "Opt-out" decision point for more detailed follow on cybersecurity reviews, rather than having to make the case for an "Opt-in" cybersecurity risk assessment at the start. I also think that a 'basics' approach around case studies is where we need to start, having seen the power of the format used in both public domain and restricted access discussion formats.

Finally - a call to action for SCSC members?

In my mind there is no doubt as to the size of the task ahead in implementing the scope of the Cambrian RAIB recommendations that engage the wider industry on complex software-based systems. A bit like painting the Forth Bridge, I suspect the principles behind it will never be closed off, as changes in digital systems, both scope and reach of deployment, will be ongoing, and it is hard to predict the future fully.

My personal vision, having had the benefit of working across multiple sectors across many years, is that we – as individuals and as a SCSC community – should continue to seek, wherever possible, the opportunity to frame and exchange case studies and lessons learned. We know that it is not only 'what we say' but 'how we say it' that can increase the effectiveness of the message and how it lands, sticks and creates action. I found that in working on the RSSB podcasts that analysis of causal factors of complex software-based system incidents across multiple sectors certainly found common themes, and the use of podcasts was able to reach audiences that might not normally read a long accident report, or shorter brief. I'd encourage others to give it a try. You don't need to be a media star, frame it as a conversation! For some more handy tips, there is much practical experience in the SCSC community; I also presented some ideas, blending politics and everything else, at this year's Safety-Critical Systems Symposium [15].

As for other sectors, to work on staying ahead of the complex software-based systems curve, the rail sector can and does continue to learn. Sharing case studies, particularly in the template provided, does seem to provide a way to increase collective thinking and awareness. In terms of seeking inspiration, there's no harm in looking at what I call a 'snag list' taken from the IET Code of Practice on Cyber Security and Safety [13] (fig 5).

Section 2 Challenges at the intersection of safety and security

2.1	Reasonably practicable risk reduction is not easily defined for cyber security
2.2	Perceived conflict of objectives and expectations
2.3	Lack of common language
2.4	Different engineering perspectives
2.5	Quantitative vs qualitative assessment of likelihood
2.6	Porous system boundary
2.7	Dynamic nature of cyber security; static nature of safety analysis
2.8	Tensions over maintenance of cyber security
2.9	Different risk paradigms
2.10	Different risk control philosophy

Fig 5 Ten challenges to consider when preparing a 'reasonably foreseeable scenario' for a complex software-based system? [13]

And to wrap up...What is my call to action? I hope I've made a strong case for sharing case studies, using the template and formula presented here, and also the parallel importance of considering how the engagement and communications can be delivered in order to achieve impact. I've also extended a suggestion for next steps in the development of case studies by incorporating safety and cybersecurity. I would now like to open a discussion on how the SCSC community could help build on this work so please get in touch with myself (emma.taylor@scsc.uk) and Stephen Bull (stephen.bull@scsc.uk) to share your thoughts.

References

[1] Annex B of Service Assurance Guidance Version 2 [SCSC-156A], The SCSC Service Assurance Working Group scsc.uk/scsc-156A Feb 2021

[2] Annex H of Data Safety Guidance Version 3.3 [SCSC-127F], The SCSC Data Safety Initiative Working Group scsc.uk/scsc-127F Feb 2021

[3] Report 17/2019: Loss of safety critical signalling data on the Cambrian Coast line: www.gov.uk/raib-reports/report-17-2019-loss-of-safety-critical-signalling-data-on-the-cambrian-coast-line. Accessed 1st May 2021.

[4] Handling RAIB recommendations: www.orr.gov.uk/monitoring-regulation/rail/promoting-health-safety/investigation-enforcement-powers/handling-raib-recommendations. Accessed 1st May 2021.

[5] RAIB Report: Loss of safety critical signalling data on the Cambrian Coast line on 20 October 2017: www.orr.gov.uk/sites/default/files/2020-12/raib-cambrian-coast-line-2020-12-18.pdf. Downloaded 1st May 2021.

[6] Annex B: Glossary of terms used in RAIB reports: www.orr.gov.uk/sites/default/files/om/glossary-of-terms-used-in-raib-reports.pdf. Accessed 1st May 2021.

[7] Report following railway power disruption on 9th August 2019: www.orr.gov.uk/media/10752/download. Accessed 1st May 2021.

[8] Improving Railway System Safety: safety.networkrail.co.uk/improving-railway-system-safety/. Accessed 1st May 2021.

[9] RAIB Annual Report 2019: assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/886627/AR2019_200521.pdf. Accessed 1st May 2021.

[10] Learning from Other Sectors, www.rssb.co.uk/safety-and-health/learning-from-experience/accident-investigation-and-learning/learning-from-other-sectors, Accessed 10th May 2021.

[11] Developing Digital Competency: http://www.rssb.co.uk/en/safety-and-health/learning-from-experience/accident-investigation-and-learning/developing-digital-competency. Accessed 1st May 2021

[12] S French, The True Needs of End Users in Safety-Critical Software-Based Systems Design, RTM, https://mag.railtechnologymagazine.com/display_article.php?id=3954332&view=697292.

[13] IET Code of Practice for Cyber Security and Safety: theiet.msgfocus.com/k/Iet/code_of_practice_for_cyber_security_and_safety. Accessed 1st May 2021.

[14] Code of Practice: Cyber Security and Safety Webinar: webinars.on24.com/theIET/CyberSafetyCode. Accessed 1st May 2021.

[15] Taylor E A (2021) Influencing for Safety and Risk: A Novel Toolkit, Systems and Covid-19, Proceedings of the 29th Safety-Critical Systems Club Symposium Virtual Conference, 9th–11th Feb 21.

Image attribution: lead image: ID681094 © Paul Neyman. Fig 1, 2 and 3 from the RAIB accident report [3], fig 4 from RSSB website [10]

Dr Emma A Taylor CEng FIMechE FSaRS

Emma is a safety engineer with 30 years of experience across space, energy and transport. This article is written in a personal capacity and references only public domain work done whilst she was at RSSB, as the RSSB lead for implementation of the Cambrian ERTMS Recs. During this project she worked closely with colleagues at RSSB and rail industry stakeholders, including Network Rail and the National Cyber Security Centre (NCSC) and would like to acknowledge the valuable contribution made by them in producing the public domain outputs. The views she expresses on the use of a cybersecurity risk assessment to assess complex software-based systems, and the blended approach to generation of future case studies, are personal, and do not form part of the industry's response to the Cambrian Recs. She is now Head of Digital Safety at a leading rail cybersecurity solutions company, RazorSecure, and is also a Past Chair of the Safety and Reliability Society, and a member of the SCSC Steering Group.

The opinions expressed here are for discussion only and should not be taken as the basis for regulatory, legal, commercial or technical advice.

The Cyber Security Aspects of Autonomy in Aircraft



Mick Warren discusses his thoughts on how autonomy will impact the cyber security aspects of safety within aviation. Including a brief background to the history of aviation safety, he discusses the challenges use of Artificial Intelligence (AI) bring. He outlines what industry is currently doing to address this, what he has done through research and application on an in-service aircraft and what the potential next steps should be.

Since the dawn of aviation accidents have occurred – from the crash of the first commercial flight in the UK in 1919 killing two to the latest, at the time of writing, of a Beechcraft B200 in Kenya. Safety is paramount as we have seen with recent problemd such as the Boeing 737 Max safety issues. This has cost 346 lives; resulted in the halting of production of the aircraft; closing of factories building the aircraft; grounding of all of the aircraft and reportedly has cost Boeing as much as $19 billion as of Jun 2020.

Historically, accidents tended to be as a result of mechanical failure. Over time, valuable lessons have been learned and the amount of mechanical failures causing accidents has reduced significantly. Accident attribution in more recent years has been the result of terrorism or crew issues. Processes and procedures have developed to mitigate such causes. Is cyber-security the next threat source for aviation accidents? We have already seen cyber-security attacks on aviation in an Airline Management Systems where 1,400 passengers were grounded and the flight plans of 10 aircraft went missing. Luckily, this was a mission impact and not a safety of flight one. However, the potential for cyber-attacks on aircraft was understood in the last century as military aircraft had already been subjected to cyber-attacks by then.

The outcomes of risks emerging from security issues are related to both mission and safety aspects. Mission issues are where the end impact of a successful cyber-security attack may cause loss of a mission; for example, an attack against the inventory management system may mean that an aircraft cannot be repaired and thus misses a scheduled flight. Alternatively, there could be a targeted attack on the inventory management system that affects flight records, potentially causing an incorrect part being fitted to an aircraft, thus resulting in a safety risk. It may also affect more than one aircraft at the same time. A potential safety risk is of particular concern in aviation – at worst case it could lead to a catastrophic accident with significant loss of life.

Cyber security threats are real and are happening within the aviation domain now

In the last 30 years aviation has moved from a traditionally isolated set of on-board and off-board systems into highly interconnected systems (such as Integrated Modular Avionics). This, when combined with more recent developments of highly integrated systems-of-systems (such as the Air Traffic Management network and Controller Pilot Data-Link Communications) and coupled with widespread internet access on-board presents significant potential security issues. Such integration provides potential significant additional threat paths – many of which are outside the control of the aviation domain – that have, hitherto, not been possible. Aviation is vulnerable to cyber security attacks. It is not necessarily that difficult to expose such issues. A security expert, Chris Roberts, tweeted that he could play with Engine Indicating and Crew Alerting System messages. This could have resulted in a significant safety impact from a cyber threat. Luckily, he didn't do it – he was making a point albeit he was arrested by the Federal Bureau of Investigation for his troubles.



Artificial Intelligence Challenges to Aviation safety

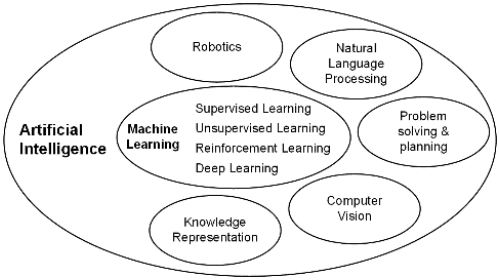
Aviation security & safety faces a new existential challenge – AI. The use of AI – and Machine Learning (ML) in particular – is on the rise, where tasks may be automated through the use of large and accurate input/output datasets. Such intelligent behaviour is already with us in day-to-day use, be it voice recognition on a smartphone, interaction with an automated call-centre, machine translation or search engines. Significant research and investments are being made in fields using ML such as autonomous cars (with $1 billion invested in a single week!), aviation, software fault prediction and electrical load forecasting. The growth is such that what may have been considered intelligent behaviour only 5 years ago is now considered hardly noteworthy.

The use of ML widens the potential cyber security threat landscape and the speed at which attacks can occur

With such growth comes the potential for malicious use – such use significantly impacts the potential threat landscape; moreover, it can significantly increase the speed at which attacks occur. In addition, current growth is such that it will invariably outstrip the ability to either provide certification (as the development of domain standards will invariably lag system development) or appropriate legislation (legislature works even slower than standards development).

What is AI? AI, helpfully, has neither an agreed general definition nor scope. It is also widely used and misused. Standard texts agree that it contains:

- Robotics
- Natural Language Processing (NLP)
- Problem solving and planning
- Computer vision
- Knowledge representation and
- Machine Learning (ML) (which has sub-sets as shown).



AI is important to the Aviation sector – it may: reduce cost (through quicker design); improve performance (through improved engine fuel burn); introduce new markets (such as local Unmanned Air Vehicle (UAV) deliveries); increase payload (by reducing the need for multiple pilots) and, eventually, provide fully automated passenger aircraft (by removing the pilot).

The use of AI may present particular challenges – requirements being one of them. DO-178C (RTCA, 2011) – Software Considerations in Airborne Systems and Equipment Certification – relies on the system safety and hazard analysis to determine system failure conditions and then applies a rigour to the software development process commensurate with their perceived effect(s). Is this feasible for AI? For a start it assumes that requirements can be traced through decomposition to design to determination and evidence. This would be a challenge for AI as not only are requirements definition, decomposition and traceability a significant challenge, there is also the potential for complex unexpected behaviour – this is often a challenge for 'normal' software. Thus, AI presents particular challenges when demonstrating its acceptable safety. Given the potential breadth of AI, a decision was made to focus on the currently most widely used sub-set of AI – that of ML.

What has the Aviation Industry done about it?

The Aviation industry is still struggling with the introduction of multicore processing into safety critical systems never mind AI. Thus far, they have concentrated on the potential safety risks associated with cyber-security threats. DO-326A / ED-202A (RTCA, 2014) – Airworthiness Security Process Specification – was issued on 6 Aug 2014. It has only recently been included within Amendment 25 of European Union Aviation Safety Agency (EASA) Certification Specifications (CS) under CS25.1319. It was previously a Special Condition for Type Certificate (TC) applicants and Supplemental Type Certificate (STC) applicants. It is incumbent on TC and STC applicants to demonstrate that security risks have been identified, assessed and mitigated appropriately. This is managed as a certification activity although the potential severity of the impact of a cyber-security threat to a failure condition comes from the system safety analysis, as enacted through the use of industry standard approaches

such as Aerospace Recommended Practise (ARP) 4754A (SAE International, 2010) and ARP4761 (SAE International, 1996). In simple terms, it has its origins in safety but is then dealt with from a certification perspective. As we move from our current paradigm into a world where ML becomes more prevalent, there is a need to ensure that the potential threats that ML may pose are recognized and appropriately mitigated.

Current aviation security standards do not consider potential impact of Machine Learning

DO-326A and supporting standards do not even mentioned ML. Arguably, if the threat resultant from ML is identified then application of DO-326A may address potential threats. It is identifying the potential threats resulting from ML and the provision of assurance on the associated risk that are the challenges.

What have I done about it?

In order to better understand where DO-326A may be adapted to explicitly consider ML and the challenges it presents, I took the following approach to help facilitate the development of an assurance case:

- Decomposed the standard and its supporting standard DO-355 – Airworthiness Security Methods and Considerations – into a Goal Structuring Notation (GSN) argument
- Rebuilt the GSN Goals and Solutions using a well-known assurance approach – that of the 4+1 Principles (R. Hawkins, I. Habli and T. Kelly, 2013). This was undertaken from three differing viewpoints: safety, cyber-security and ML. This was extended with the 4+2 Principle as developed by Dstl (R. Ashmore and E. Lennon, 2017) (which is due for inclusion in the latest issue of Def Stan 00-055). This resulted in an adapted 4+2 set of principles from a cyber security perspective
- Reviewed literature to develop 'particular challenges' that ML may introduce, convert them into GSN and adding them where appropriate in the new 4+2 structure
- Took the developed assurance case in GSN, validated it, and applied it on an actual in-service aircraft.

This approach readily allows the assurance case structure provided through application of the Principles to create a link between the potential cyber security aspects of ML, which, with the extension mentioned above, allows ML specific cyber security issues to also be fed back into the safety domain within the context of a safety-critical system. This provides a link which is presently not there.

A number of 'particular challenges' were identified which would need to be considered specifically for ML as part of any assurance argument. It is worth a brief exploration into some examples of the 'particular challenges' discovered during the work. These are:

- **Aircraft specific ML threats affecting safety of flight have been appropriately considered.** Arguably, in an assurance case all potential threats need to have been considered. As the use of ML is emergent then specific attention was deemed necessary.
- **Aircraft specific ML threats which may be architecturally mitigated have been appropriately considered.** One would expect them to have been mitigated as part of any design. However, there are two potential issues here. Most designs are adaptations/evolutions of in-service equipment and the failure, from a safety viewpoint, may

have been mitigated from an unintended perspective only; questions may arise as to the frequency of intentional attacks and the ability of current architecture mitigations to address potentially significantly increased probabilities;
- **Maintenance specific ML threats have been appropriately considered**. On-aircraft systems and equipment tend to be tightly regulated; the off-aircraft systems – such as maintenance laptops – that may connect to the aircraft less so. These form part of the aircraft security environment which may readily introduce significant threats to on-aircraft systems. Discussion later on shows that this is of concern in a real-life application.

Application on in-service aircraft

At the time of development of the assurance case approach there were no known instances of systems on-board aircraft that are labelled as using ML. There is significant work underway on how systems may use ML. This includes: data analysis on Health and Usage Monitoring Systems; Category IIIc Instrument Landing Systems where the aircraft lands autonomously with pilot supervision and Air Traffic Management systems.

A system on-board a typical aircraft that may be subjected to ML-like off-board analysis is the Engine Health Monitoring (EHM) Systems. EHM uses sensors on-board the engine and its ancillaries to monitor and then record the status of engine systems and components. Its aim is to allow the early detection or indications of defects before they cause safety issues. The information is stored and downloaded – on some systems it is actually transmitted, real-time, back to the manufacturer – thus introducing potentially significant additional threat paths. Off aircraft analysis takes the significant amount of data produced and performs complex analysis on it. The analysis can help predict early onset failure of components. This is not strictly speaking ML, but the complexity of the trending and monitoring on the data has ML like tendencies. Indeed, work is ongoing in the use of ML to perform such data analysis.

The totality of the assurance case approach was applied on an in service aircraft. This included an assessment against the EHM system. The main conclusions discovered from the application were:

- The argument structure provided a robust methodology to develop an assurance case to include the 'particular challenges' that an aircraft may face from ML. It did not solve the fundamental problem of how certain evidence may be developed – that was beyond its remit;
- There are weaknesses in DO-326A and DO-355 which need to be considered when applying it. For example, it was noted that the standard focussed on the word 'adequate' for test procedures. Whilst not necessarily an issue – as it is an aim to be demonstrated – the use of ML potentially challenges this – what is 'adequate'?

Next Steps

I have taken the work above and developed templates and guides on how to implement DO-326A, DO-355A and DO-356A. These are presently being trialled on differing projects to refine further. These will then act as the basis for a number of aircraft in order to demonstrate compliance with the appropriate certification specifications – these specifications are the same as those used in civil industry. This work has resulted in an understanding that more effort needs to be undertaken to ensure that the dynamic nature of cyber-security and the static nature of safety analysis is further considered. More importantly, the potential use of ML may challenge the cyber security aspects of the air domain from a developmental, assurance, integration, testing and safety assurance time perspective – it needs to be done significantly quicker than current process facilitates as it is sensitive to real-time changes to the threat landscape.

It is possible to develop an assurance case that considers the use of ML

References

[1] RTCA, DO-178C - Software Considerations in Airborne Systems and Equipment Certification, Washington, DC, USA: RTCA, 2011.

[2] RTCA, DO-326A / ED-202A - Airworthiness Security Process Specification, Washington, DC, USA: RTCA, 2014.

[3] SAE International, ARP 4754A - Guidelines for Development of Civil Aircraft and Systems, Warrendale, PA, USA: SAE International, 2010.

[4] SAE International, ARP 4761 - Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipments, Warrendale, PA, USA: SAE International, 1996.

[5] R. Hawkins, I. Habli and T. Kelly, "The principles of software safety assurance," in 31st International System Safety Conference, Boston, MA, USA, 2013.

[6] R. Ashmore and E. Lennon, "Progress Towards the Assurance of Non-Traditional Software," in Twenty-fifth Safety-Critical Systems Symposium, Bristol, UK, 2017.

Image Attribution
lead image: Crown Copyright 2021 (https://www.defenceimagery.mod.uk/fotoweb/archives/5042-Downloadable%20Stock%20Images/Archive/RAF/2021/March/45167916.jpg)
Visualization of interlinked systems in the civil aviation domain showing several potential vectors for cyber-attacks: Gontar, Patrick and Homans, Hendrik and Rostalski, Michelle and Behrend, Julia and Dehais, Frédéric and Bengler, Klaus Are pilots prepared for a cyber-attack? A human factors approach to the experimental evaluation of pilots' behavior. (2018) Journal of Air Transport Management, vol. 69. pp. 26-37. ISSN 0969-6997

Mick Warren, Frazer-Nash Consultancy Ltd

Mick Warren is a highly experienced and qualified systems safety professional who has undertaken aircraft, submarine and ATM safety work. He also specialises in software assurance and, more recently, has returned to his 'roots' undertaking cyber security work having completed a research-based MSc in Cyber Security focused on DO-326A. He has been the lead in developing a Cyber Security for Airworthiness approach (against DO-326A) where he now leads a team applying this on several aircraft to determine the potential safety impact of cyber security threats. All opinions expressed in this article are entirely his own and do not reflect the views of his employer.

The author retains copyright of this article.

Architecting Wireless for Safety Critical Machine to Machine Communication



Michael Green argues that wireless communication in an increasingly crowded radio spectrum is inherently and increasingly hazardous for command & control operations. Machine to machine (m2m) / Internet of Things (IoT) communication between embedded devices is particularly at risk. As such 'critical' m2m messages sent over wireless should never be relied upon to be 'safely' received. All is not lost, in addition to best practice risk mitigation, new technologies are being applied to wireless that will ensure messages that get delivered can be more trusted, thus enabling safer sensing, command & control of assets at distance.

'Critical' messages over wireless ... what are they?

Referencing the work of Nancy Leveson & Dr John Thomas at MIT [1] on system safety, a 'critical message' within a system would be one that has potential to cause a significant 'loss' scenario, such as an "undesired or unplanned event that results in human injury or death, property damage, environmental pollution, mission loss, etc". To be safe, a 'critical message' must arrive from a trusted sender in time to be acted upon by the recipient.

'Critical' messages over wireless ... examples:

Definitely 'critical':

- Wireless remote control of individual aircraft, drones, vessels, vehicles, machinery and infrastructure
- Wireless control of assets in formation such as a platoon of trucks, a fleet of boats or a formation of drones such as a swarm
- Commands sent to assets operating autonomously, such as updated orders, status feedback or for firmware updates
- Sensing an alarm condition that will result in loss, such as a gas or radiation leak, intruder, fire alarm or a water level sensor
- Messages to/from medical devices where lives are dependent on those devices operating as intended

NB: for real time (millisecond) control, wired communication is typically used, but there are cases where wire is not an option. Where wireless is used, allowance should be made for latency, loss of connection, lost packets and retries.

"Unforeseen developments, unpredictable communication, changes in behaviours: The Arlington Report on the communication on 11 September 2001, the report on the hearings of the City of London after the events referred to as the 'London Bombings' in 2007, the lessons from the 2016 terrorist attacks in Brussels. Communication while working from home or quarantining, remote alerting in the coronavirus era – all these examples underscore the fact that mobile phones alone cannot be the only solution for communication in extreme situations." [2]

What it might also be (depending on the context):

- A message to a satellite commanding it to de-orbit
- A distress message from a car that has crashed or failed, perhaps in a remote region without mobile/cell coverage
- A message to an autonomous marine vessel or drone transferring control to a new operator
- Messages to and from infrastructure, such as controlling the state of traffic lights
- A heartbeat message raised by a fire sensor or a water level sensor to indicate it is working ok

What it is not (typically):

- Music radio broadcasts
- Satellite TV broadcasts
- Voice calls & texts made over the telecoms network (most of the time)
- A 'heartbeat' message from a sensor device indicating it's working normally
- A sequence of messages from one or more sensors reporting the average moisture level in a field

As you can see, a 'critical' message depends on the context, the level of loss and the tolerance of stakeholders to risk.

Understanding Rising Spectrum Congestion & Interference

The Electromagnetic Spectrum is a limited capacity resource which, as a society, we entrust national and international regulators to divide up. To achieve this, regulators divide the radio frequency and microwave spectrum into bands based on its characteristics and a learned assessment of its suitability for specific applications. With this done, they 'license' these 'bands' in whole or part to organisations for their use. As a catch all, some frequency bands are defined as 'unlicensed', which can be used by anyone within an authority's geographical jurisdiction … provided, they adhere to the 'rules' of that band; if not, enforcement is by prosecution under national & international laws based on regulators jurisdiction.

The best-known frequency band is Wi-Fi. In the UK this band spans 2.412 to 2.484 GHz. The Wi-Fi band is further split into 13 channels, each 20MHz wide in most world regions. Exceptions being 11 in the USA and 14 in Japan, hence the region question during set up.

A caveat being that the regulator, for the purpose of giving fair access, requires the radiated power (Effective Isotropic Radiated Power - EIRP) must be no more than 20dBm / 100mW.

This is important, because radio communication is akin to people in a room chatting. The regulator says, no one must raise their voice, if they do, they'll be fined.

Now consider that everyone is compliant, but many speak different languages (radio protocols) and some even try to save energy (low power protocols) by whispering. You can easily imagine that distance between people becomes critical to everyone's ability to communicate.

As the room gets busier, everyone stays compliant but some start to use novel ways to get themselves heard (encodings). There are lots of tricks used. Perhaps clicking to get attention, or emphasising certain words.

So, the regulator, has introduced the concept of a 'duty cycle' in some rooms (typically unlicensed frequency allocations like the Industrial Scientific & Medical – ISM bands). In this scenario everyone who talks for 1 second (say) must wait 99 seconds before talking again.

All works as well as it can, conversations get harder and shorter as the room noise increases. People start to repeat messages and some start to guess things they haven't heard (error correction).

While 'critical' conversations were possible when the room was empty … would people think the same as it gets busier and busier? What if a Rock Band (solar storm?) or a big crowd (9/11 situation) or a very angry person / adversary (who doesn't obey rules) arrives?

Now communication steadily or suddenly becomes impossible, including that which is critical.

Symbols

Hopefully the noisy room scenario is in mind. Now imagine the lights are turned off and everyone is given a buzzer. They now 'talk' using Morse code! The long buzz & short buzz are referred to as 'Symbols'. Sequences of symbols define letters and sets of letters, words.

With the richness of human speech removed, it's easy to realise that if everyone presses their buzzer equally loudly (amplitude) and at the same pace (frequency), chaos will ensue. To communicate, everyone needs to be either a) very close to the party they are talking with or b) listening out for differences in the buzzer sounds. Different 'symbols'.

Some people, being ingenious, decide to change the speed at which they send their Morse code, while others listen to the buzzer starting, or ending its sound. Still others get their buzzers to get louder slowly versus immediately. These are known as modulations.

Add encryption to messages, so others can't tell what you are saying. Get clever, changing the order of buzzer beeps (bit flipping) … you get the picture!

This is the situation with wireless in the wild. It's hard to talk, harder to hear someone's messages but, somehow, it works most of the time. If messages are encrypted, they can be hard to crack, but with the right skills, determination and tools [2], it is sometimes possible!

Wireless – inherently hazardous? … why?

Despite all the ingenuity and endeavours of people working in the wireless communications field to make it so incredibly reliable and useful, there will always remain a possibility that a wireless connection will fail and/or the message being carried will not arrive in a timely manner, arrive corrupted and need to be resent.



Even in an environment where everyone is compliant with regulations, wireless communication remains vulnerable to spectrum interference or non-compliant operator [3].

We should also not ignore the risk that communications are intercepted, decrypted and/or subverted by an adversary [3].

Wireless for 'critical' sensing, command and control - the risks:

While the exploits referenced earlier, are historic, Safety Risks persist from several vectors:

The spectrum

To quote: "Unlike wired networks, wireless communication channels are unstable, scarce, and prone to interference." [4]

1. the unstable nature of wireless spectrum, puts the reliability of wireless communication largely beyond the sender's / receiver's control
2. architectural choices come into play, such as whether the wireless device is normally connected or disconnected, if the protocol is adaptive, message repeated etc.

Probability

3. will the message arrive? … it depends on the state of the spectrum
4. will it be in a consistent state, unaltered from the original? … hopefully, but not guaranteed in all cases (watch the Packet in Packet exploit [5])
5. will it be in time to be actioned as intended? … if it does get received, then maybe

Trust

6. can the sender's identity be confirmed as true and trusted?
7. is the sender trusted?
8. is there assurance that the privacy of the message is uncompromised?

In terms of things that can be improved in wireless communications, recent work on wireless blockchain indicates that improving message Trust and utility, has significant potential.

In summary, best practice for 'critical' sensing, command & control over wireless, requires

an alternative communication path [6] to be on standby, ready to step-in on failure / interference, however small. Meantime we can embrace emerging opportunities to ensure messages that are received over the radio spectrum are secure and can be fully trusted.

To some extent this requires us to go back several millennia, to the time when each message carried its own seal. A seal that could be verified as being unbroken by the recipient and who's origin could be trusted.

Architecting wireless for safety 'critical' m2m messages …

From an architectural perspective, in this digital world, there are essentially two options. Both these options are implemented at the seventh ISO stack 'application layer':

Architecture #1 – **centralised verification** - using Certificate Authority (CA) technologies

Architecturally, in today's digital world, this requires implementing a system where each message packet is encrypted AND signed BEFORE delivery. On receipt, the recipient device contacts the signing CA to confirm the message is unaltered (consistent) and its origin can be verified.

In effect, this equates to using an X.509 certificate to sign each and every radio packet, with the associated communications to create, sign and verify plus maintain stores for large numbers of public and private keys.

This architecture may work for normally connected wireless communications, but is almost certainly unfeasible at all but small scale.

Architecture #2 – **distributed verification** - using (decentralised) blockchain technologies

Blockchain is an emergent technology that has many flavours [7]. It provides four benefits at once:

- message privacy – as does encryption
- immutability – ensuring the message received is consistent with the one sent
- auditability – enabling messages to be traced back to their origin, and
- smart contracts potential (the ability to send code that is trusted to a remote device for execution, in contrast to predicting actions and saving code on the device until needed).

However, there are other implementations, some of which are engineered to use minimal resources that have been tried on wireless communication testbeds. Blockchain systems may be centrally managed or distributed, with various strategies for deciding who can update the chain and how transactions in the chain are linked. In brief, blockchain is a ledger. It differs surprisingly little from the historic vision of a trusted scribe writing on parchment with indelible ink. The differences with regard to blockchain are:

- There can now be more than one trusted scribe
- Trust is assessed by a quorum using an agreed process, such as proof of stake (PoS) or proof of work (PoW)
- Parchment has gone digital and can thus reside in more than one place at (almost) the same time

In terms of implementation, this depends on the type of blockchain being applied, many are resource hungry and unsuitable for a resource constrained environment like wireless.

Another consideration is whether the wireless network operates in a normally connected or normally disconnected manner. There are initiatives to apply blockchain to normally connected wireless networks like Wi-Fi and 5G, however the task of applying blockchain to a normally disconnected wireless network poses all of the resource challenges PLUS the need to minimise transactions over spectrum, ideally to just the one.

Conclusion

Wireless communication should never be considered to be 100% safe, despite it being ever more reliable with the development and application of new standards, such as the 5G New Radio (NR) for air interface [8].

Given that wireless communication is now amazingly useful despite operating over an inherently hazardous spectrum, there is an opportunity to evolve the utility of messages transmitted to ensure they remain trusted and secure in the dawn of the quantum computing era [9].

References

[1] John Thomas, "Introduction to STPA", Engineering Systems Lab MIT, 2020 http://psas.scripts.mit.edu/home/wp-content/uploads/2020/07/JThomas-STPA-Introduction.pdf

[2] Matt Knight of Bastille Networks, "Decoding LoRa PHY (33c3)", 2016 https://youtu.be/NoquBA7IMNc

[3] Bart Hendrickx, "Russia gears up for electronic warfare in space" The Space Review, Oct 2020, https://www.thespacereview.com/article/4056/1

[4] D. Yu, W. Li, H. Xu and L. Zhang, "Low Reliable and Low Latency Communications for Mission Critical Distributed Industrial Internet of Things," in IEEE Communications Letters, vol. 25, no. 1, pp. 313-317, Jan. 2021, doi: 10.1109/LCOMM.2020.3021367

[5] Travis Goodspeed and Sergey Bratus and Ryan Speers and Ricky Melgares, "Packet in Packets: Orson Welles' In-Band Signalling Attacks for Modern Radios", In Proceedings of the 5th USENIX conference on Offensive Technologies, 2011, https://www.usenix.org/legacy/events/woot11/tech/final_files/Goodspeed.pdf

[6] Quote from Press Release Critical Messaging Association Sept 2020 https://critmsg.org/wp-content/uploads/2020/04/202009-Press-Release-New-Home-for-CMA.pdf

[7] Liehuang Zhu, Keke Gai, Meng Li, "Blockchain Technology in Internet of Things", 2019, DOI 10.1007/978-3-030-21766-2

[8] Sacha Kavanagh, "What is 5G New Radio", March 2020, 5G.co.uk https://5g.co.uk/guides/what-is-5g-new-radio/

[9] National Cyber Security Centre, "Preparing for Quantum-Safe Cryptography", Gov.uk, Nov 2020 https://www.ncsc.gov.uk/whitepaper/preparing-for-quantum-safe-cryptography

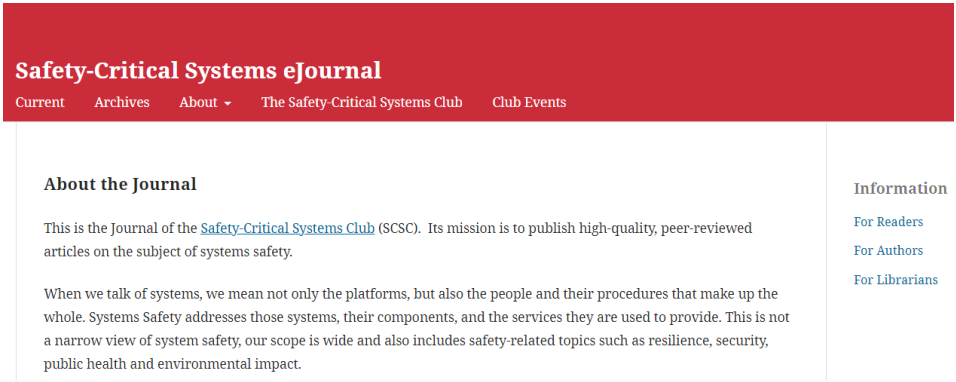
Image Attributions: Front image: licensed by eComergy from iStock; Northern Lights: CC licensed

Michael Green, Founder & Director, eComergy Wireless.Works Ltd., Weightless.Space Ltd

Michael has a degree in Mechanical Aeronautical & Production Engineering. He started programming 50 years ago with ICL, and has implemented both large and small systems including IT security for banks and multinationals. In the last decade Michael has focused on the challenges of Low Power Wide Area (LPWA) wireless networks for IoT device deployments beyond the range of mobile / cell networks, hence the interest in low frequency (sub-1GHz) on aerial and satellite platforms for critical sensing, command & control that are both highly robust and able to scale.

The author retains copyright of this article

Introducing the Safety-Critical Systems eJournal



A New Journal

When the Safety-Critical Systems Club was set up thirty years ago, its objectives were to raise awareness of safety issues and to facilitate safety technology transfer. To achieve these objectives, the club organised events, such as Seminars and an annual Symposium, and published a newsletter, *Safety Systems*, three times a year.

The Newsletter has, in addition to news, opinion, correspondence, book reviews, and the like, also carried articles discussing current and emerging practices and standards. The length of such articles is limited to about two and a half thousand words, which does not allow an in-depth treatment. It has therefore been decided to add a third string to our bow and supplement the events and newsletter with a journal containing longer papers, six thousand words, say.

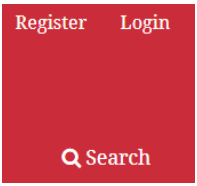
The journal will be published on-line, as the *Safety-Critical Systems eJournal*, and is to comprise two issues a year. There will also be an annual print volume of all the issues presented on A4 sized pages, which will make the provision of clear diagrams and graphs easier than it is in the smaller Symposium proceedings and *Safety Systems*.

Mission Statement
To publish high-quality, peer-reviewed articles on the subject of systems safety.

Registering for the eJournal

An eJournal is a website configured to present the content of a journal via simple navigation menus. A link to the *Safety-Critical Systems eJournal* can be found on the SCSC website. Alternatively, go straight there using: https://scsc.uk/journal/index.php/scsj. We have built our eJournal using Open Journal Systems, which was developed by the Public Knowledge Project in North America [1]. You do

not need to register to read the journal; however, there is an advantage if you do, in that it will automatically send you the Contents List by e-mail each time a new issue is published. When you go to the website, you will see the Register link to the right-hand side. Clicking on that takes you to a page asking for name, e-mail address, etc. One of the fields is Affiliation, which is intended to be your employer or university; it is quite acceptable to put None in there.



Contributing to the eJournal

For a successful journal, we need a lot of authors and, as this is a peer-reviewed journal, reviewers too. To volunteer your services, please Register on the website. It assumes you want to be an Author and asks if you want to be a Reviewer. It lets you specify the sort of subject matter you wish to review; this could be industry specific, e.g. railway signalling or airspace management, or cross-industry topics, such as data safety or services assurance. If you do not want to be an author, or later decide you wish to be a reviewer, edit your user profile, ticking as required the Author and/or Reviewer boxes under the Roles tab.

Are you working on something new? We want to hear about it. We also want to know if you are working on something old; how do you sustain a legacy system in a changing environment? You may think that your day-to-day job is uninteresting, but what is normal in your industry may just be what another industry is looking for.

Is your assurance based on compliance with a published standard; how do you interpret that standard, and how do you clearly demonstrate compliance?

Have you learned any lessons recently, or analysed an accident or incident? If so, please provide a summary article.

Mike Parsons, Safety-Critical Systems Club Managing Director, said on LinkedIn, "The SCSC is creating a new publication, "The Safety Critical Systems eJournal" for high-quality technical articles on any area of systems safety. This will be published twice a year via the SCSC web site, with a compilation hardcopy available on Amazon annually. The focus of the journal will be on safety practice, industrial applications and standards/guidance. The editor is John Spriggs, a long-time supporter of the club and respected author and presenter.
Please consider submitting an article on your work."

References

[1] Open Journal Systems, (2021), in Wikipedia https://en.wikipedia.org/wiki/Open_Journal_Systems, accessed 24 March 2021

John Spriggs, Independent Author and Presenter (and now Editor)

John Spriggs was a designer of avionics systems in the 1970s and '80s. In the 1990s, he became an assurer of equipment for Air Traffic Management and Airports. From 2000, he was the Safety Assurance Consultant for an innovations factory, and later provided assurance for air navigation services providers. John is now an independent author & presenter; he is author of the Goal Structuring Notation textbook.

The author retains copyright of this article.

SSS'21 Event Report



The Covid-19 pandemic has had a significant impact on the way organisations operate, and the SCSC is no exception with the annual SCSC Symposium (scsc.uk/e683) being moved to an entirely online format for the first time in its history. The event proved to be highly successful, but how did the online format deal with aspects that only a physical meeting can bring, such as networking, exhibitor stands and after-dinner speeches?

The 29th annual Safety-Critical Systems Symposium took place between the 9th and 11th February 2021. The event was entirely online, running over three afternoons and included an evening session on the second day in lieu of the traditional banquet and after-dinner speech. As with the physical meetings, the programme was split into themed sessions with a chair introducing speakers and managing proceedings. Live presentations were then followed by some pre-recorded presentations that attendees could view at any point throughout the symposium.

Thought for the Symposium



After opening the symposium, Mike Parsons, Director of the SCSC, handed over to Tim Kelly from the Church of England who gave his "Thought for the Symposium". Tim described how the pandemic has forced everyone to become experts in risk management and risk mitigation, with some becoming "armchair statisticians" formulating and revising their own predictions based on the daily figures and graphs being published.

Tim stressed that there is a huge gulf between the understanding of risk and the communication of risk. This is borne out by how the initial simple messages of staying at home and protecting the NHS were effective, but as the message was naturally revised to reflect improved data, such as variations in mask wearing and social separation distances, this introduced ambiguity and required too much interpretation.

The impact of the initial simple messages was being lost with increasing violations and people taking matters into their own hands. Also, behind these messages is an overt display of decision making from a utilitarian/ethical perspective balancing the risk of mortality against quality of life. It has also been a challenge to keep hold of the fact that, behind the numbers, there are real people with families and friends and there is humanity behind the discipline of system safety.

Tim concluded by saying we need to be careful not to become abstract mathematicians and analysts divorced from the reality and that the job ultimately concerns saving lives; we need to ask the difficult questions about what is important and it is more important than ever to make the work of system safety count.

The Pivotal Pandemic

Harold Thimbleby's Keynote presentation identified the long-standing gap in perception and skills between the use of technology – seen as exciting and enabling, and the unsung endeavours of the underlying disciplines, such as software engineering, required to make the technology work.

The Covid-19 pandemic that has driven the development of many technological solutions has been a stark illustration of this gap. Many failings in the delivery of technologies such as Track and Trace, has highlighted a lack of maturity – what Harold calls "digital immaturity" – in the underlying engineering disciplines required to manage safety-related data and build safe systems. Harold also said that even authoritative bodies have issues and gave an example of NHS Digital's guidance on NHS numbers and the problems with the sample code they promoted for wider use. Harold said that some cases were so egregious he could quote Wolfgang Pauli in saying "it's not even wrong!"

One of his recommendations to tackle the issues of digital immaturity is for every University to set up a Software Engineering Board with professional software engineers to help those working in the pandemic to do better software engineering. He concluded by appealing for other ideas from the community on how we can get the message out to the world and to ultimately improve the quality and safety of technology.



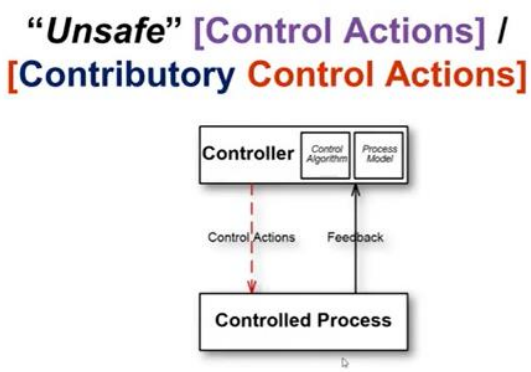
Learning from the UK pandemic response using STAMP

In the next of the first day's Keynote presentations, Simon Whiteley discussed his thoughts on what can be learned from the UK response to the coronavirus using STAMP and how this learning could shape future responses and policies.

Simon briefly introduced the concepts around STAMP (Systems Theoretic Accident Model and Processes) that, at its core, uses a closed loop feedback control model. In this model, a

Controller is empowered to send control actions to the controlled process in accordance with a Control Algorithm and feedback received from the process. This basic model can be combined in a hierarchy to model more complex systems.

With this model, potentially unsafe control actions can be considered and goes beyond just failures/faults but can also consider "dangerous successes".



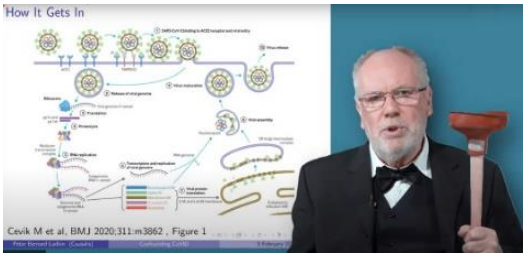
Simon showed how this model can be applied in the context of the Covid-19 pandemic. For example, processes under control could be Population Behaviour and Virus Transmission with lockdowns being typical control actions. Feedback would represent the daily statistics of infections and deaths used to inform further actions. Simon went on to show diagrams that modelled the detailed interactions between stakeholders such as the government, police, media, medical, the general public and patients.

Simon noted how the governmental messaging such as staying at home could be considered unsafe control actions depending on the context of the individual (eg. someone that needs to seek medical care for a non-covid illness). Also, social media channels such as Twitter have a role to play in the model as they are effectively control actions that can influence the public's mental models. This results in interesting dynamics and considerations that require optimisation in light of model changes, such as virus variants and success or failures of control actions (c.f. Track and Trace).

Simon concluded by saying that a STAMP based approach provides a great opportunity to model and learn from the control structures for both current and future situations. For example, a STAMP based model could be used in advance of a future pandemic to ensure it is appropriately resourced.

Confounding Covid

In a pre-recorded Keynote presentation, Peter Ladkin provided background on the science of infectious diseases such as bacteria and viruses and the distinction between these: bacteria being cell-based and viruses being RNA or DNA genetic material enclosed in a lipid envelope. He described how the Coronavirus replicates within cells, demonstrating the process using a football, a knife and a kitchen plunger!



He noted that we already knew about the risks of viruses such as SARS in 2002, MERS in 2012 and Swine Flu (H1N1) in 2009, and quoted a Gresham College lecture given by Chris

Whitty, the Chief Medical Officer, in 2018 on epidemics and how they spread. Viruses have different transmission routes such as airborne, food, touch etc. but airborne transmission is particularly problematic as it is indiscriminate and difficult to disrupt; inhibiting the route of transmission is seen as key.

Peter referred to research showing that aerosols from a sneeze can reach 6 to 8 m and that many activities, such as just talking, can also spread the virus. He noted some of the common engineering solutions to preventing transmission such as barriers (masks), social distancing and air conditioning. Peter listed other engineering mitigations compiled as part of the Covid Working Group that included "situational awareness" – such as satellite imaging of human activity and social media, supporting remote working, modelling and general improvements in the supporting IT.

Infodemiology was noted as an emergent concept related to the spreading of accurate information and dampening the spread of inaccurate information including countering myths and conspiracy theories. Peter however thought there were at least two sides to this and he suggests further public debate is needed.



He also noted some of the surprising benefits that arose from lockdowns, such as reduced traffic making roads safer.

He concluded his presentation with a rendition of Cuil Aodha on his flute!

Assurance 2.0: A Manifesto

The second day's first Keynote talk was given by Robin Bloomfield. Robin said there is a need for change to assurance approaches as trustworthy systems are expensive, slow to produce and still have failures. There are also new emerging challenges with new technology that need to be addressed.

Robin suggested we need a new approach and introduced "Assurance 2.0" to make assurance an enabler for innovation, not a brake. The approach is to keep the structure of traditional assurance cases but strengthen the focus on evidence and reasoning. It also advocates bringing the assurance thinking earlier in the life-cycle and having greater support with known best practice - eg. "pre-validated" blocks or templates.

Robin presented the key points of the manifesto:

- making explicit inference rules and separating inductive and deductive reasoning. The more that can be moved to deductive the better leverage there is in terms of analysis and tool support
- explicit use of doubts and defeaters to establish counterclaims to arguments – a form of hazard analysis for an argument to explicitly deal with the source of doubt
- focus on evidence integration, addressing both the relevance and provenance of evidence
- confirmation theory to evaluate strength of evidence and argument: a method of evaluating the strength of a claim by calculating a confirmation ratio
- an explicit approach to reducing bias by using counter-cases and confirmation theory

Robin also said that this is not just a theory but is being actively used in real scenarios (both safety and security) and supporting tools and guidance are being developed. For example:

- an interim report on safety case templates for autonomous systems has been published where the principles of Assurance 2.0 have been adopted, such as providing a methodology for defeater identification, and how CAE notation can be augmented to represent defeaters.
- There is an interactive online course that has integrated the elements of Assurance 2.0 and four pilot courses have already been run successfully.

Robin concluded by saying that the methodology and supporting tools will continue to be evaluated and developed.

Evening Session (After-Dinner)

The traditional 2nd day evening banquet and after-dinner speech was replaced by a more informal online event hosted by Tom Anderson, with live presentations from Emma Taylor and Patrick Hudson. Emma discussed her personal thoughts and experiences in using words more effectively to help improve how we communicate and influence stakeholders in the safety domain. Patrick then discussed the history and evolution of safety culture and his work in developing tools and techniques to improve best practice.

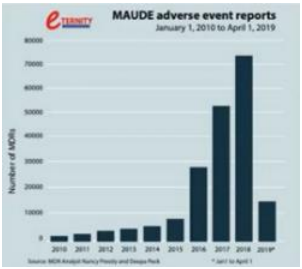
PETER – A Pan-European Training, Research and Education network

The final day's Keynote presentation was given by Prof. Davy Pissoort. Davy provided examples of electromagnetic interference (EMI) and how this is a well-known problem, for example, why we are asked to turn off mobile phones in hospitals and applying flight mode to devices on aircraft.

Davy said that EMI will have increasing importance as there is growing use of electronics through the proliferation of sensors (eg. IOT devices) used for safety-related decision making, and the increasing social dependence on interconnected electronic systems that are inherently "EM-noisy". This also extends to interference on communication lines leading to data errors, and Davy illustrated how this would be particularly problematic for:

- autonomous vehicles that require robust, low-latency wireless data communications
- smart manufacturing where "cobots" are working in close proximity to people
- robotic surgeons, personal carers, assistants in healthcare

Davy noted this is not just theoretical; there is evidence of an increasing number of safety-critical failures as a result of EMI in domains such as medical devices.



Davy went on to explain that there are problems with the current regulation on EMI, especially around safety-related equipment. For example, the EMC Directive and supporting standards cover EMI but exclude safety of equipment. Manufacturers usually come back to showing compliance using an EMI testing chamber, which has limitations and not all combination can be tested – especially simultaneous EMI effects.

Davy introduced the PETER programme to train young engineers so they can develop a different approach to managing EMI risk – to go from a standards-driven rules-based approach to a risk-based approach. The programme will bring together an international interdisciplinary team combining intensive training and doctoral research. The focus will be on system planning, implementation and validation in the context of a number of case studies, such as medical devices and smart grids.

Davy concluded by describing the ultimate goals of achieving EM Resilience that are, in summary:

- good EMC and functional safety engineering practice used throughout the design
- equipment passes all immunity tests throughout its lifecycle
- actual EMI errors are detected and handled in a safe manner.

Virtual Networking and Exhibitions

For the wholly online event, the usual symposium physical networking and exhibitor stands were facilitated through the use of the event's Whova platform and app. The app allowed users to find and get in touch with other attendees, open up topics for discussion across the community, share feedback on the presentations and explore other areas such as job openings.



Exhibitors were able to build their own event profile where they could share files and video presentations, offer promotions, chat with attendees and schedule live showcases through Zoom.

With some of the events being pre-recorded, it was acknowledged that the usual Q&A sessions could not be held in all cases. It was therefore decided to have a follow-up online session on 24th Feb 2021 where attendees with questions on papers and presentations (either online or pre-recorded), which were not answered during SSS'21 itself, could be discussed.

Success!

Overall, despite the difficult circumstances, this year's symposium was hugely successful. Over the three days, the average rating based on the events survey feedback of the technical content was 4.2/5.

A number of novel solutions were required to overcome the challenges of hosting a purely online event, but these proved highly successful with the Zoom experience receiving an average score of 4.5/5 and the Whova experience receiving an average score of 4.4/5.

Congratulations to all those involved in setting up the event and making it such a success!

Report by Paul Hampton, SCSC Newsletter Editor

Safety Culture Developments Seminar Report

"*The safety culture of an organisation is the product of individual and group values, attitudes, perceptions, competencies, and patterns of behaviour that determine the commitment to, and the style and proficiency of, an organisation's safety management system (within the overall business management system)*".

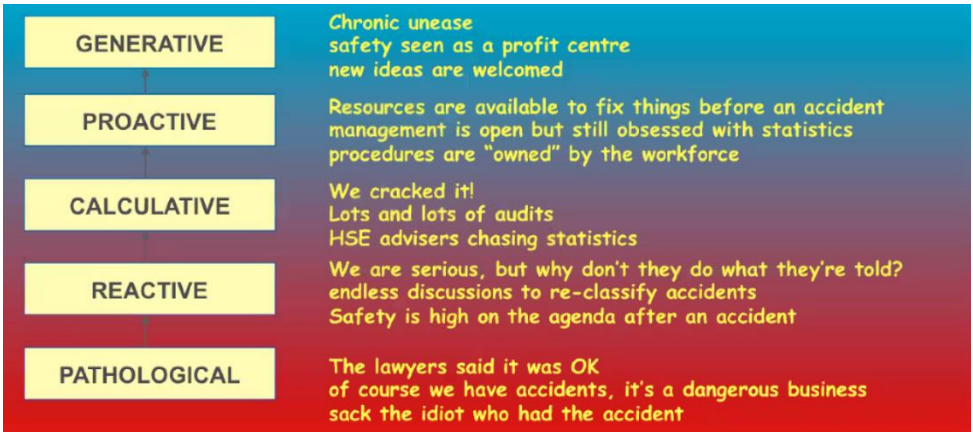
Adapted from ACSNI Human Factors Study Group: Third report - Organising for Safety (HSE Books, 1993).

The SCSC held an online seminar on Safety Culture Developments (scsc.uk/e793) on 13th April 2021. The seminar reviewed approaches to measuring and improving safety culture in organisations, and summarised results from the SCSC Safety Culture Working Group's Online Survey.

This seminar was led by the SCSC's Mike Parsons and Paul Leach (Rail Safety and Standards Board). Four individual presentations were given by industry experts, followed by a panel session. Approximately 50 delegates and speakers attended from a range of industries.

Moving Up the Culture Ladder: A Case Study

Patrick Hudson (Delft University of Technology) and Tim Hudson (Hudson Global Consulting) summarised the findings from a review of a major aviation Maintenance Repair and Overhaul programme using the safety culture ladder model.



Surveys and workshops were used to measure an airline's safety management system in terms of twelve cultural dimensions in April 2016. Process Performance Indicators and improvement actions with completion dates were defined based on desired behaviours for each dimension, resulting in nine divisional projects.

Project progress was monitored on a monthly basis. By November 2017, significant improvements were reported in the survey scoring. Tangible benefits were realised by the organisation in terms of: increased staff involvement in SHEQ activities, clearer staff roles and responsibilities, two-way communications, enhanced training materials, improved Safety Notice Boards, simplified Standard Operating Procedures. The findings from the review emphasized that senior management's understanding and commitment to the ladder process was critical to achieving sustained cultural improvements.

Pilot – Human Performance

Rob Saunders (Shell) discussed a safety culture initiative used during investigation of several major incidents. The incidents occurred at one of its Dutch plants between 2014 and 2016 and led to fatalities, serious injuries, plant shutdown and staff dismissals.

In 2017 a "deep dive" assisted reflective learning activity was undertaken with the plant's leadership team and operators, which raised cultural concerns around: variability in task performance, error-traps, tasks without independent verification, competence, confidence, clarity of roles and responsibilities, assurance not scaled with risk criticality, work mindset, and differing perceptions of consequences.



A Human Factors "Pilot" workshop focussed on three tasks with a high chance of human mistake. A Safety Critical Task Analysis (SCTA) systematically reviewed aspects of the tasks in terms of: Steps, Errors, Consequences, Existing Safeguards, Performance Influencing Factors and Actions.

The SCTA helped to identify required improvement actions – e.g. changes in the language, attitude and ways of working, design of separations, training, visual aids to situational awareness, operator verification, and engagement with plant maintenance.

The tasks were changed in recognition that "*People make mistakes – this is not a license for poor workmanship, but setting people up to succeed*". Following implementation of these actions, the unit's safety KPIs improved significantly in 2018 and 2019 and there have been signs of a cultural shift in terms of behaviours, language and perceptions.

Safety Culture: Stimulating Change

Sarah Whittaker (Defence Equipment & Support) discussed how DE&S measures and tracks safety culture within its organisation, and summarised some improvement initiatives.

The vision of DE&S is to deliver equipment and services to the Armed Forces that are safe to operate, and to ensure its people are safe at work ("Delivery focused; Safety driven"). Its safety culture must demonstrably support this vision. DE&S undertakes an annual safety culture assessment of its organisation spanning both Occupational Health & Safety and Acquisition Safety. These assessments use the safety culture ladder model and a toolkit of methods including a questionnaire and culture level indicators.

The DE&S Acquisition Safety Project was launched in 2018 aimed at improving safety culture. To raise staff awareness a video using live actors was produced to dramatize several safety incidents, and an e-learning course was developed. This initiative helped to identify a taxonomy of safety assignments and clarified DE&S safety roles and responsibilities.



The initiative helped to realise improvements in the equipment design and support processes, and to identify information to help Operating Duty Holders to use equipment safely. DE&S plans further improvements to its Acquisition Safety and Environmental Management System supporting safety assurance and safety culture. An environmental culture ladder has also been developed in line with DE&S climate change and sustainability objectives.

SCSC Safety Culture Working Group: 2020-21 Survey Results

Michael Wright (Greenstreet Berman) summarised the results and conclusions from the SCWG's recent survey on safety culture that received 122 full responses from a range of sectors.

Benefits and disbenefits of measuring safety culture

Benefits	Disbenefits
Enables targeting of areas for improving safety culture	Cost, time and effort required to carry out reliable measurement
Improves the organisations understanding of their safety culture	Results are often subjective and it can be hard to understand the context of answers and therefore what they mean for understanding and enhancing culture
Promotes safety behaviours within the organisation – helps staff understand behaviours to demonstrate	Can create false sense of achievement e.g. certain overall score achieved means no improvement required
Provides opportunity to measure effectiveness of improvements implemented and benchmarking safety culture against other organisations	Results can be used to criticise management and staff
Contributes to continuous improvement in performance and business success	Staff may not see the benefit because they may not see improvements after measurement and so do not engage or do not see safety culture as an important area
Fosters and facilitates safety leadership – helps leaders focus on safety culture	

The survey results were summarised as:

- Reasons for assessing or not assessing safety culture
- Benefits and disbenefits of measuring safety culture (see table above)
- Assessment methods and models, their advantages and disadvantages
- How the results of safety culture assessments are evaluated and used
- Whether the results present a valid profile of the organisation
- Safety culture KPIs and objectives
- Approaches taken, key challenges and enablers to improving safety culture
- What worked well and not so well in engaging individuals
- Who leads, and who would be approached with ideas, to improve safety culture
- Levels of management commitment
- Future help from the SCSC in terms of assessing or improving safety culture

The SCWG's survey can be found here: https://www.surveymonkey.co.uk/r/SCWGsurvey

Panel Session

A wrap-up session led by Paul Leach gave delegates an opportunity to put further questions to the speakers. The panel was asked for its views on:

- The main threats to improving safety culture. The panel's responses included: lack of senior management commitment, contradictory communications, lack of authenticity, psychological safety, complacency, distraction from safety objectives.
- How to help staff understand their contribution to safety culture. The panel's responses included: education, using exemplary staff as role models, involvement in risk assessments.

Report by Rick Vinter, Principal Safety Consultant, CGI IT UK

The SCSC is its Own Boss!



After almost thirty years, the club has changed its organisational arrangements and is now a legal entity in its own right.

The Safety-Critical Systems Club was initiated in May 1991, holding its first meeting in July and publishing its first newsletter in September of that year. It was sponsored by the then Department of Trade and Industry and the Science and Engineering Research Council and was supported by the British Computer Society and the Institution of Electrical Engineers, who have since become the Institution of Engineering and Technology.

The task of running the SCSC was given to the Centre for Software Reliability at Newcastle University led by Professor Tom Anderson, with the invaluable assistance of Joan Atkinson and Felix Redmill. In 2016 the club was transferred to the University of York with Professor Tim Kelly in charge, assisted by our business manager Alex King and with Dr Mike Parsons coordinating the events programme. In 2019, following his ordination in the Church of England, Tim Kelly left the University and became Assistant Curate of Beverley Minster, at which point, Mike Parsons took over the role of SCSC Leader.

After so many years operating within a University context, and with the impacts of the pandemic, the club needed to have more autonomy and control over its operation.

Introducing the Safety-Critical Systems Club C.I.C.

A C.I.C. is a Community Interest Company, a special type of limited company, which exists to benefit a community rather than private shareholders. A C.I.C. has:

- A community interest statement that defines the beneficiaries – the community it serves – (see box opposite) and how it plans to benefit that community
- An 'asset lock' – a legal promise stating that its assets will only be used to achieve the community benefit objectives
- A constitution and Articles of Association as a limited company
- Approval by the Regulator of Community Interest Companies to whom it has to report achievements every year

"We will support Safety Practitioners working across all sectors and organisations".

This means that, as a distinct legal entity, the SCSC now has more freedom to operate and can legitimately do things such as make agreements with other bodies, seek funding to support the objectives and own copyright on documents. Up to now, all of these things would have been done via the University.

Seven members of the club's Steering Group have volunteered to be Directors of the C.I.C. and have taken on the legal responsibility of running the company.

What does that mean to the club and its members?

There is no change planned in the way we do things, or the membership we serve.

Staying the same:

- The SCSC exists to support Safety Practitioners
- The programme of events will continue and develop. We expect to continue with a blended face-to-face and online format. We are looking forward to SSS'22 in Bristol – our special 30th Symposium
- The working groups will continue and are also expected to continue to make use of online meetings
- SCSC membership for individuals and corporate bodies is uninterrupted
- The people currently filling roles in the operation of the club will remain in place
- The Website, Newsletter, eJournal and Symposium continue as before
- The office at the Department of Computer Science at York remains the business address.

Some small changes (now and in the near future):

- Payments for membership or event bookings will now be to the SCSC rather than the University of York. Payment details will need to be updated on corporate payment systems. Alex King has the bank details.
- Quotes and invoices will now come from the SCSC rather than the University of York
- The Safety-Critical Systems Club C.I.C. is now responsible for the personal data it holds about club members. There is no change in how this data is used or stored and members' rights under GDPR are unaffected.
- The SCSC copyright will appear on some parts of documents (authors will always retain their copyright for their contributions).

Directors

Managing Director:

Mike Parsons

Directors:

Alex King	Graham Jolliffe
Brian Jepson	Mark Nicholson
Dewi Daniels	Paul Hampton

Formal Text

The following provides the formal text associated with the SCSC C.I.C.

"Safety-Critical Systems Club" and "SCSC" are trading names of Safety-Critical Systems Club C.I.C. Safety-Critical Systems Club C.I.C. is a Community Interest Company limited by guarantee and registered in England and Wales with company number 13084663.

The setup of the C.I.C required an official address to be nominated for the Registered Office for the purposes of receiving company related correspondence. A 3rd party mail service is therefore being used at a Winchester address. However, for all club related business correspondence, the following business address should be used:

Business Address

The business address and contact details for the club is now as follows:

Safety-Critical Systems Club
Department of Computer Science
University of York
Deramore Lane
Heslington
YORK
YO10 5GH

Email: office@SCSC.uk
Phone: +44 (0)1904 325402

Image Attribution
Door: ID: 61234713 © Volkovslava | Dreamstime.com
Nameplate ID: 44733146 © Andreykuzmin | Dreamstime.com

Copyright 2021 SCSC

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

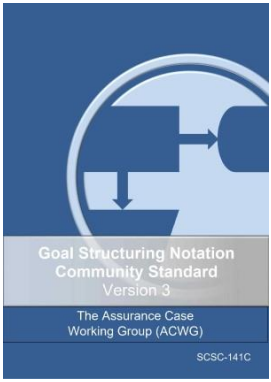
Advertising

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:

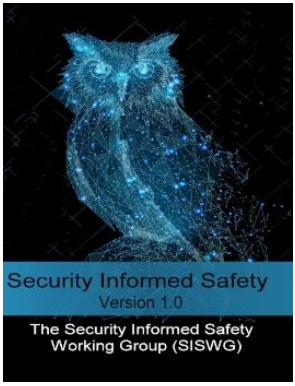
- Be broader than safety, and will address interaction and conflict between related topics
- Address aspects such as proportionality, rationale behind the guidance, focus on risk, confidence and conformance
- Consider the role of the counter-argument and evidence and the treatment of potential bias in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

One of the working group's initial activities is to take on board the maintenance of the Goal Structuring Notation (GSN) Community standard.

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

Lead Phil Williams phil.williams@scsc.uk

Security Informed Safety



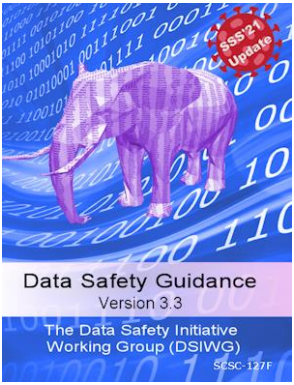
The Security Informed Safety Working Group (SISWG) aims to capture cross-domain best practice to help engineers find the 'wood through the trees' with all the different security standards, their implication and integration with safety design principles to aid the design and protection of secure safety-critical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

SCSC Working Groups

Data Safety Initiative



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

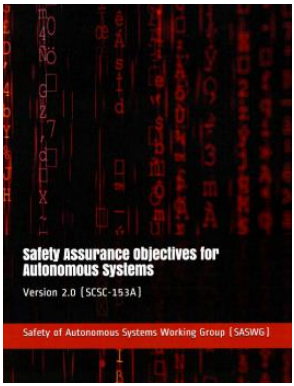
It is acknowledged that data has been a contributing factor in several incidents and accidents to date. There are clear business and societal benefits, in terms of reduced harm, reduced commercial liabilities and improved business efficiencies, in investigating and addressing outstanding challenges related 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 (v3.3) was published in Feb 2021: scsc.uk/scsc-127F

Lead Mike Parsons mike.parsons@scsc.uk

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.

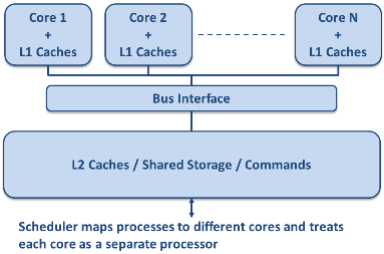
It is clear that autonomous systems can introduce many new paths to accidents, and that autonomous system technologies may not be practical to analyse adequately using accepted current practice. Whilst there are differences in detail, and standards, between domains many of the underlying challenges appear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

Lead Rob Alexander rob.alexander@scsc.uk

SCSC Working Groups

Multi- and Manycore Safety



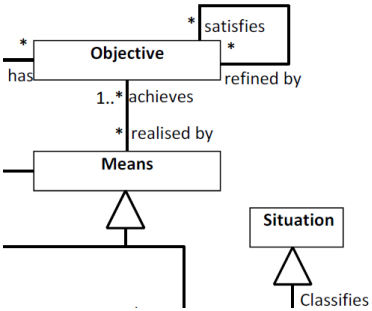
It is becoming harder and harder to source single-core devices and there is a growing need for increased processing capability with a smaller physical footprint in all applications. Devices with multiple cores can perform many processes at once, meaning it is difficult to establish (with sufficient evidence)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

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

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

Lead **Louise Harney** louise.harney@scsc.uk

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

SCSC Working Groups

Covid-19

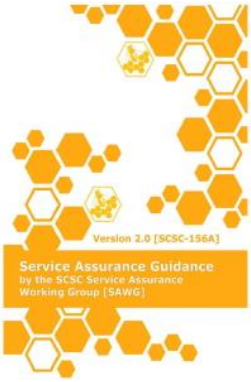


The Covid-19 Working Group is involved with discussion, analysis and assistance related to the Coronavirus. The group meets remotely to see what a systems and assurance view of the situation brings. The group has compiled an extensive range of Covid-19 related material and made this available on the 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

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.

In Feb 2021, the group published v2.0 of the guidance: scsc.uk/scsc-156A

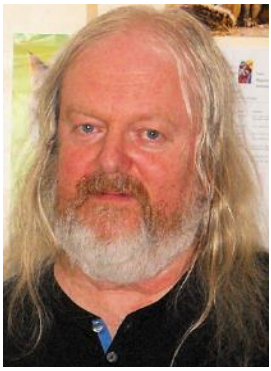
Lead Mike Parsons mike.parsons@scsc.uk

SCSC Safety Culture Working Group (SCWG)

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 within teams working with safety-critical systems. This is a well-researched area with a lot of guidance already in place, so the initial activities are considering what is working well, what is not effective, and where guidance is required. Meetings provide an opportunity to discuss any particular aspects attendees are interested in taking forward, and to help set future directions for the group.

Please contact michael.wright@greenstreet.co.uk if you are interested in joining this group.

60 Seconds with ... John Spriggs



John was a designer of avionics systems in the 1970s and '80s. In the 1990s, he became an assurer of equipment for Air Traffic Management and Airports. From 2000, he was the Safety Assurance Consultant for an innovations factory, and later provided assurance for air navigation services providers. John is now an independent author & presenter; he is author of the Goal Structuring Notation textbook. His latest venture is as editor of the new Safety Critical Systems eJournal, the first issue of which is expected later this year.

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

It was just another aspect of system engineering to me at the time the safety manager of the company for which I was working left for pastures new. He recommended that I take over from him, because he had liked the work that I had done for him. I became safety manager just as they were reorganising the company and wanted a formal Safety Management System...

"Someone once told me that my management style is like that of Hawkeye Pierce."

What aspect of your career are you most proud of?

Being published, and being repeatedly invited to provide articles and to present at seminars and symposia.

What advice would you give to yourself age 12?

Save your money and, in twenty years' time, invest it all in a company called Microsoft at their initial public offering...

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

Safety systems used to be specially developed for a purpose, using familiar components, largely transparent sub-systems, and specialist operators. Now they are being developed using general purpose system and service components via opaque interfaces, and it is service desks all the way down.

What's your most favourite quote or motto?

There is a craft workshop on Guernsey that has a sign on the wall saying, "Don't be afraid to ask dumb questions". That is the core principle of a safety culture.

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

I would like to draw and paint better.

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

Someone once told me that my management style is like that of Hawkeye Pierce; I am respected only by those in the organisation who know what we are meant to be doing. Professionally, I think I am more like Saga Norén; I want to get the job done properly, and completely, and I don't understand all the politics and socialising that people want to do instead. All that said, the answer to your question is Lazarus Long; he has more time to do stuff.

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

"Don't guess; ask!"

This has also been expressed as, "If you don't know, just say so; don't demonstrate it by waffling on".

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

I guess that some footballer has an autobiography called "A Game of Two Halves". Productivity was less when I had to work at home, so I was working longer hours. This was because colleagues who previously had been happy to drop me an e-mail now had to have Teams meetings, and management spent a lot longer than before checking up on things. In stark contrast, furlough and subsequent off-work periods enabled me to make up for having had too much to do for a sustained period before the pandemic. Actually having free time was brilliant! I have opened all the letters and magazines that had been put aside, reclaimed the garden from two or three years' growth of brambles, etc., and started writing again.

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: £35
- 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



Nikita Johnson

nikita.johnson@scsc.uk



Graham Jolliffe

Honorary member



Tim Kelly

Honorary member



Alex King

alex.king@scsc.uk



Mark Nicholson

mark.nicholson@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

emma.taylor@scsc.uk



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 & Nikita Johnson 2019-

Calendar

May '21

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 '21

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 '21

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 '21

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 '21

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 '21

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 '21

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 '21

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 '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						

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	

Events Diary



5 May 2021
SCSC Working Group

Ontology Working Group #55

Online (Webex)

scsc.uk/e824

6 May 2021
SCSC Seminar

Software Maintenance: Legacy and Archaeology

Online (Zoom)

scsc.uk/e817

18 May 2021
SCSC Working Group

Data Safety Initiative Working Group #61

Online (Zoom)

scsc.uk/e821

17 June 2021
SCSC Working Group

Multi/Manycore Working Group Plenary

Online (Zoom)

scsc.uk/e795

1 July 2021
SFI Event

Safety Futures Initiative: "Get To Know You"

Online: 12pm and 6pm

scsc.uk/e828

7-10 Sep 2021
Conference

SafeComp 2021: 40th International Conference on Computer Safety, Reliability and Security

York, UK + Online

safecomp2021.hosted.york.ac.uk

23 September 2021
SCSC Seminar

Can we quantify risk?

London, UK + Online

scsc.uk/e800

11 November 2021
SCSC Seminar

Safe Use of Multi-Core and Manycore Processors

London, UK + Online

scsc.uk/e812

2 December 2021
SCSC Seminar

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

London, UK + Online

scsc.uk/e825

8-10 February 2022
SCSC Symposium

30th Safety-Critical Systems Symposium (SSS'22)

Bristol, UK + Online

scsc.uk/e797

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

SCSC

FOR EVERYONE WORKING IN SYSTEM SAFETY

www.scsc.uk/sss

SSS'22

SCSC 30th Annual Symposium

Details of this and other events at: www.scsc.uk

www.scsc.uk



THE SAFETY-CRITICAL SYSTEMS CLUB

30th Safety-Critical Systems Symposium

8-10th February 2022, in-person in Bristol and blended online

Invitation to submit an abstract

The Safety-Critical Systems Symposium in 2022 (SSS'22) will be held in Bristol and blended online as a live-streamed event. This event comprises three days of live presented papers, including keynote presentations and submitted papers.

This is our 30th Symposium and will feature talks looking back at the past 30 years, and also special anniversary events.

The Symposium is for all of those in the field of systems safety, including engineers, managers, consultants, students, researchers and regulators. It offers wide-ranging coverage of current safety topics, focussed on industrial experience. It includes recent developments in the field and progress reports from the SCSC Working Groups. It covers all safety-related sectors including aerospace, defence, healthcare, highways, marine, nuclear and rail.

Suggested topics are:

Accident Analysis
Agile Methods
Artificial Intelligence
Argumentation Notations
Assurance Cases
Autonomy
Change and Evolution
Data in Safety Systems
Digital Twins
EMC/EMI
Human Factors
Independent Review & Audit
Internet of Things
Machine Learning
Methods and Tools
Model-Based Development
Modular Assurance
Multicore / Manycore
Ontologies / Formalisms
Regulation
Robotics and Automation
Safety Analyses
Safety Culture
Safety Management
Safety Practice and Process
Security-Informed Safety
Service-Oriented Safety
Software
Standards and Guidance
Systems-of-Systems
Training and Training Data
Validation and Verification

Authors for papers should submit a title and 200-word abstract to **mike.parsons@scsc.uk** by **30th June 2021**. Successful authors will then be asked to submit their paper by **30th October 2021**. Papers will be reviewed, and comments fed back during November 2021. Poster authors should submit a title with abstract and/or short paper to **mike.parsons@scsc.uk** by **30th October 2021.**

The hard-copy proceedings book will be available at the event. The book, posters, videos and papers will be posted online.

For **information, exhibition** and **booking** enquiries please contact: Alex King, Dept of Computer Science, University of York, Deramore Lane, York, YO10 5GH. Tel: 01904 325402; **alex.king@scsc.uk**

For **technical aspects, abstract and paper submissions**, please contact: **mike.parsons@scsc.uk**