The Safety-Critical Systems Club Newsletter

Safety Systems

Vol 29 No. 3 - Oct 2021

ENDGAME THEORY
Where are we now with dealing with Covid-19?

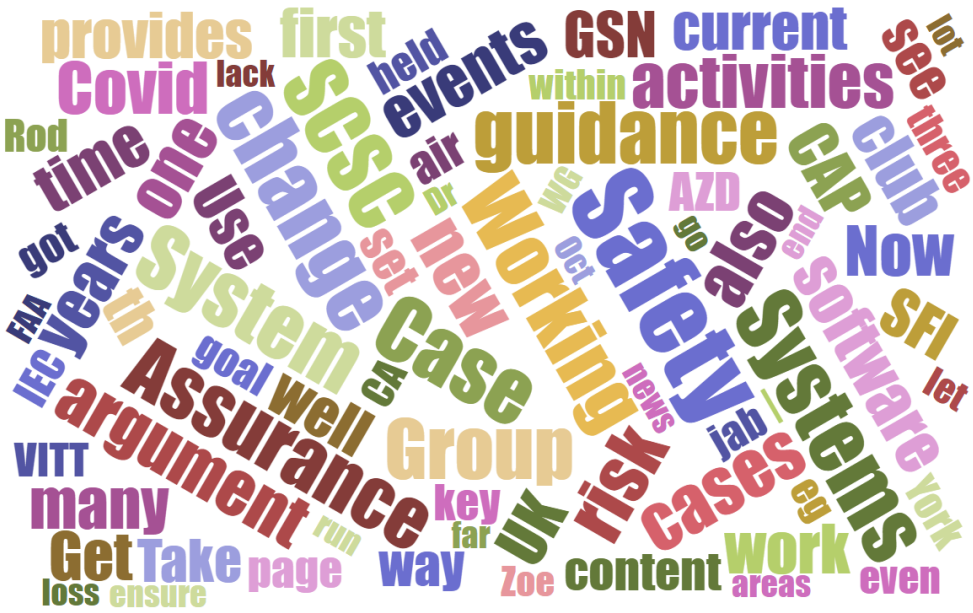
DEEDS OF TRUST
Developments in assurance case best practice

CASE FOR CHANGE?
How to assess change safety cases

For everyone working in Systems Safety

SCSC

thescsc.org



SCSC Publication Number: SCSC-165

Contents

SCSC

FOR EVERYONE WORKING IN SYSTEM SAFETY

Bookings at:
www.scsc.uk/events

This seminar is an opportunity to hear about quantification of risk in different application domains.

It will be useful for safety practitioners, safety managers, and for those involved in risk assessment and risk management.

Details at: www.scsc.uk

Can risks be usefully quantified in safety-critical Situations?

www.scsc.uk

THE SAFETY-CRITICAL SYSTEMS CLUB

Seminar: Can We Quantify Risk?

21st October 2021, Radisson Blu Edwardian Bloomsbury Street Hotel, London, UK and Virtually Online

This seminar will consider whether risks can be usefully quantified in safety-related situations. Some approaches to risk management in complex situations are apparently more successful than others, but some areas are notoriously difficult to quantify. This topic has polarised opinions among risk management specialists for some time.

Risk assessments which present a problem include those dealing with software, data, those concerning rare but severe events (e.g. 'Black Swan' events) or human-dependent risks (e.g. cyber-threats).

This seminar will feature a variety of speakers who will explain how risk is quantified (or not) in their sector, what justifications are typically used and what pragmatic approaches can be applied. Speakers are recognised leaders in engineering risk analysis. There will also be a speaker from the insurance industry explaining the pragmatic approaches taken to price risk appropriately.

When complex automatic and autonomous functionality is involved, e.g. machine learning, the situation becomes more complex, as it is not always known what learning may have taken place. How do we make risk-based judgements in such cases?

There will be an afternoon 'looking ahead' session where delegates can explore the topic and the possible solutions further.

Cost and registration: Club members: £195, including lunch and refreshments (no VAT). Non-members additional £125 for Club membership. Concessions: £95, which includes membership for one year. Streaming rate £95 (£35 concessions). Joining instructions and the programme will be sent to delegates before the event. Delegates must book their own accommodation (if required).

Editorial

Are we there yet? After eighteen months of unprecedented disruption to all our lives and having to find new and novel ways of working, it seems we are now seeing a return to the way things used to be – to the more traditional methods of meeting face-to-face and engaging with each other.

Our first in-person seminar entitled "Can we Quantify Risk?" (scsc.uk/e800) will be held in London on 21st October 2021 and the club is delighted be able to host this event and to perhaps, have the level of contact and interaction that is impossible with a purely online event. It's appreciated that we're not entirely out of the woods yet, especially as winter approaches, and so online access will also be available for those unable to attend in person. See opposite page for further details of the event.

This blended approach to events will continue to be adopted for the next few events including the annual Safety-Critical Systems Club Symposium being held in Bristol this year from 8th-10th February 2022 (scsc.uk/e797). As a reminder, this symposium marks the club's 30th Anniversary and so please attend if you can as there will be many special events, gifts and delegate hand-outs to mark the occasion. For example, delegates will receive the book "*30 Years of Safer Systems*" – an anthology of newsletter articles published over the last 30 years, each with new commentaries setting the technical and social context for each article.

But are we truly over the worst? In our first article: "Dealing With Covid-19: Where We Are" Peter Ladkin helps inform the answer to this question by assessing where we are in terms of understanding and technological prophylaxis in tackling Covid-19.

Despite the restrictions, our Working Groups have remained busy, and Phil Williams, in our second article, provides a progress update from the Assurance Case Working Group, and in particular, details of two new important publications from the group: version 3 of the Goal Structuring Notation Community Standard (scsc.uk/scsc-141C) and version 1 of the Assurance Case Guidance (scsc.uk/scsc-159). Continuing with the assurance theme, Stephen Barker and Andrew Eaton then describe another recently updated publication CAP 1801 (www.caa.co.uk/CAP1801) from the Civil Aviation Authority, providing guidance on assessing change safety cases.

Our fourth article is one of a new series of Newsletter articles called "How Do I Get Into Safety?" The path to developing a career in safety is not often a direct one, and we ask some of the SCSC Steering Group members to share their own personal experiences. For those embarking on a career in safety, help is also at hand, Zoe Garstang provides an update on the Safety Futures Initiative and provides details of the next meeting (scsc.uk/e856).

We have one event report covering the seminar in May on "Software Maintenance: Legacy and Archaeology" (scsc.uk/e817) and we are also launching a new SCSC forum (scsc.uk/f295) allowing members to be notified of new draft standards prior to their publication.

Our 60 second interview is with Dr Emma Taylor.

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

In Brief

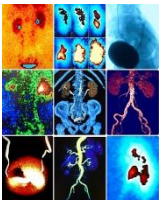
Confusing NOTAMs led overrun 747 crew to believe longer runway was unavailable

Investigators probing the overrun that destroyed a Boeing 747-400F at Halifax have highlighted the contribution of poorly-presented NOTAM information to the accident. *flightglobal.com*

Warship positions faked including UK aircraft carrier

A carrier strike group led by HMS Queen Elizabeth had its automatic identification system (AIS) position faked, researchers discovered. *bbc.co.uk*

Hundreds of AI tools have been built to catch covid. None of them helped



Many hundreds of predictive tools have been developed and trained on Covid-19 data to help doctors understand what they were seeing and to make potentially life-saving decisions.

None of them made a real difference, and some were potentially harmful.
technologyreview.com

Report details how Airbus pilots saved the day when all three flight computers failed on landing

Airbus is to implement a software update for its A330 aircraft following an incident in 2020 where all three primary flight computers failed during landing.

The result was a loss of thrust reversers and autobrake systems and the pilots having to use manual braking to bring the aircraft to a halt, just 30 feet before the end of the runway. *theregister.com*

FAA bans Virgin Galactic launches while probing Branson trip

The FAA said the rocketship carrying Branson and five Virgin Galactic employees veered off course during its descent back to its runway in the New Mexico desert on 11th July. During the flight, alerts appeared on the ship's console warning the pilots that their flight path was too shallow and the nose of the ship was insufficiently vertical. The deviation put the ship outside the air traffic control clearance area.
abcnew.go.com
newyorker.com

Dealing With Covid-19: Where We Are

It is almost 2 years since Covid-19 first entered the global consciousness and the world has since been busy dealing with its consequences as well as taking measures to prevent its continued spread. So, after all that time, where are we with tackling Covid-19 in terms of understanding and technological prophylaxis in developed countries? Peter Ladkin, leader of the SCSC Covid-19 Working Group, provides his assessment.

Joined-up Systems

I propose that our experience has shown that "joining up" heterogeneous systems has been, and likely still is, key to mitigating the pandemic. Examples of this are:

- **Personal Protective Equipment (PPE) preparedness and supply:** the UK had an undersupply of PPE, since pandemic-preparedness measures had been partly run down during "austerity", and found it both hard and expensive to resource it at a time when global demand was outrunning supply
- **Vaccine development, preparation and supply:** there were notable difficulties in the European Union (EU) January-April 2021 in ramping up preparation and supply, since ameliorated
- **Medical emergency logistic systems:** ambulance services and delivery to hospitals that could accommodate Covid-19 patients was severely strained in various places and at times almost to the point of non-performance during the first and second waves in the UK

Let me compare with another integrated-system non-performance. Under the rubric of "Understanding the System", I talked to the SCSC in London in April 2015 about the North American power outages in 2003. There were many operator/supervisor organisations involved. Each had a system; these systems interacted, and the interactions turned out to be essential to a correct operation of the whole. Let me call "the whole" the System. There was an information computer, a predictor/estimator of current demand, a "state estimator", run by one of the involved organisations, Midcontinent Independent System Operator (MISO). MISO's estimation a short while before the overload did not "resolve", because of a lack of veridical input from one key grid component. When rerun/restarted to "resolve" with the new input, it did "resolve" but did not proceed to update automatically, because of – let us say – misconfiguration. It thus did not update information about the ongoing demand-supply imbalance, and by the time the issue was identified it was too late to mitigate. The computer was, but had not been seen as, essential to complete-System functioning, and thus there were not appropriately sensitive operational procedures in place. A full-System hazard analysis across all the various organisations involved would have indicated the MISO estimator as one of two computer systems essential for continued functioning of the grid.

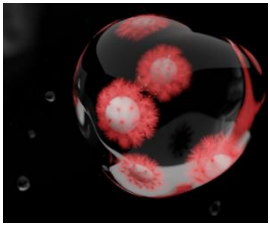
The lesson is almost always the same: the organisations involved hadn't perceived what the System was in its entirety, and had treated key System-components relatively nonchalantly. A solution is "joined-up System analysis".

"The lesson is almost always the same: the organisations involved hadn't perceived what the System was in its entirety"

Simon Whiteley reported at SSS'21 on his attempt to sketch the architecture of the UK government's pandemic decision-making "system". Simon's sketch wasn't complete, and some parts of the architecture were guesses from news reports. We can imagine that a full (correct) architecture of the system followed by some BPMN-style analysis [1] of weak points and their mitigation could well have improved decision-making. I think the following sections represent where we are in terms of pandemic-related knowledge and systems.

What Works and What Doesn't

It is more or less known what helps Covid-19 patients and what doesn't, from amongst the available medicines and medical procedures. Standards of care are fairly stable. Triage is no longer much of an issue, it seems (that is, in the early stages of symptomatic disease, distinguishing those at risk for hospitalisation from those who will get better on their own).



Concerning procedures, we have learned that what constrains Intensive Care Units in developed countries is not lack of equipment, but lack of personnel. (Recall the rush in Spring 2020 to design and build new mechanical ventilators, and to build new hospital facilities with some IC capacity).

We have also learned – relearned – that pandemic preparedness is essential for public security. The UK did not keep up its emergency supplies of PPE over the previous decade, and suffered disastrously from not having it available.

The Role and Efficacy of Vaccines

Western vaccines have been shown to be astonishingly, almost miraculously, effective, both the vector vaccines and the mRNA vaccines, and there are more on the way. The Chinese vaccines do not appear to be quite so effective, and it also seems the Russian Sputnik has garnered varied reports on its efficacy. Whatever one might think politically of the organisation and motives of capitalist Big Pharma, the companies came through on this one in terms of technology and distribution in those countries able to support it; some of them such as AstraZeneca laudably pro bono publico.

Antivirals

The lack of antivirals, especially for treatment of mild to moderate disease, is slowly being remedied. Regeneron-Roche's Ronapreve (a cocktail of casivirimab and imdevimab) has been approved by the MHRA [2]. The US BLAZE-1 trial of Eli Lilly's cocktail monoclonal antibody combination bamlanivimab + etesevimab on roughly 1,000 participants has shown that it helps [3]. AstraZeneca has an antiviral AZD 7442, which has shown excellent performance in avoiding Covid-19 in those for whom the illness is high-risk, in the PROVENT Phase III trial that involved over 5,000 participants [4].

On 1st Oct 2021, Merck announced an interim analysis of its Phase III trial MOVe-OUT of its oral antiviral molnupiravir developed with Ridgeback Biotherapeutics. The interim analysis suggests the drug, administered to patients with mild or moderate Covid-19 and at high risk of progression to severe disease, reduced the chance of hospitalisation or death "by approximately 50%" [5]. And more are on the way.

Public Health Measures

The public health measures are now well understood for airborne infectious disease. Masking, distancing, testing, test-trace-isolate, good ventilation inside buildings. Also increasingly understood is the public acceptance (or not) of various measures, including the effects of information and misinformation. One surprising, and to my mind not well understood, connection in some areas is with political parties and politics in general. (Not only in the US; in the current German national election we have candidates standing for political parties that have formed in opposition to public health measures to control the spread of Covid-19).

Schools and Teaching

Schools and their processes are still not well understood. In particular, almost everywhere there seems to be little interest in air filtering technology for poorly-ventilated classrooms (which, in the case of SARS-CoV-2, is pretty much all of them!) A recent study [6,7] of some 200 schools in the UK during presence teaching showed little difference between infection rates in schools that quarantined neighbours of infected children and those which allowed them to continue in school with negative tests. The general return to presence schooling in my state of North-Rhine-Westphalia has not led to any superspreading outbreaks; indeed, local experience in Bielefeld indicates that the infection rate in schools is inferior to the

community-transmission rate. We thus have just moved from quarantining of classroom neighbours to testing them, which has relieved the load on the city public health department somewhat. Of course, such observations are tentative, but they are bound to be more or less right (it is not as if you can miss high-spreading or superspreading events if they are occurring).

We know that on-line teaching/learning is indeed possible at large scale. Also, that the nature of much work can change, because it has. This has been enabled by digital communication technology. These digitally-enabled modes of learning and working can obviously get much better, if we can solve the cybersecurity issues.

Infodemiology

Misinformation is a massive political problem, and not just with Covid-19. Infodemiology is here to stay. The sociology of misinformation in the time of pervasive digitalisation of key forms of communications is very poorly understood. Even less well understood is the social psychology of correcting it.

Public certification of health status

Public certification of health status will inevitably go digital, for two reasons. One is that it is temporally dependent. If you have been jabbed, two weeks later you need the certificate. It is not like applying for a passport, which you can do months in advance of needing it. Second, the existing paper documentation may not be trustworthy. There are already newspaper reports in Germany of the rise of WHO-vaccination-booklet faking services. Both the EU vaccine certificate and the German smartphone app provide a QR code that links to the official record held by the Robert Koch Institute, Germany's public health institute. That is far harder to fake. However, as with any digital certification there are attendant privacy/validity/cybersecurity issues. It remains to be seen if these issues amplify like those with cybercurrency/ransomware, or if they stay socially low-level, as with (real) passport e-technology.

Communication Breakdown

How the AstraZeneca vaccine roll-out got into such a mess was well covered in The Guardian newspaper [8]. It appears, inter alia, that there was a mismatch between what the academics who designed the testing regime needed to see and know, and what various regulatory authorities were expecting from "polished" drug company submissions. It has changed names twice (first, it was AZD1222; then Covid-19 Vaccine AstraZeneca; now Vaxzevria).

"Public health requires public messaging and on vaccinations that requires more than medical-scientific expertise."

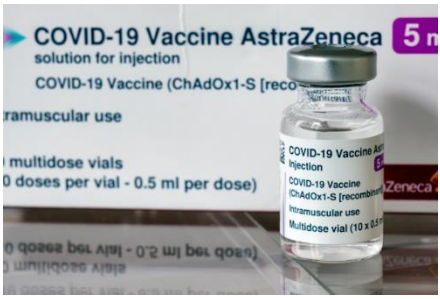
It turns out some catastrophic German politics resulted from this, and I think there are a number of lessons in it. Political decisions on vaccines were, and are, based on the recommendations of the Standing Vaccination Committee of the RKI (StIKo). The chair Prof. Dr. Thomas Meertens has told us that the task of the commission is to make the best possible vaccination recommendations for individuals and society, "*independent of the opinions and wishes of politicians and the pharmaceutical industry*" (my translation from e.g., [9], in German). Pure science, no politics.

But public health requires public messaging and on vaccinations that requires more than medical-scientific expertise. It requires politicians to formulate appropriate messages and get them through to the public in such a way that they stick. One message is: *Get your jab*. But there are different jabs; people will ask: *which jab*? To which the best answer is: *it doesn't really matter.* But that is not what the scientists on StIKo were saying (see below). What resulted was murky messaging, which was not well smoothed for consumption by the general public. StIKo recommendations and their history are available [10]. It happened as follows:

- on 14th Jan 2021, in the first StIKo recommendation the AstraZeneca vaccine AZD1222 was not yet approved by the European Medicines Agency (EMA)
- on 29th Jan 2021, in the second recommendation the AstraZeneca vaccine was approved for those aged 16-64, but insufficient data were said to be available for those 65 and over (I understand this was the StIKo; the EMA had approved it unrestricted as far as I know)
- by 12th March 2021, the restriction was lifted: AZD1222 was also recommended for all age groups for which it had been approved – but then came Vaccine-Induced Immune Thrombotic Thrombocytopenia (VITT)
- On 8th April 2021, the StIKo recommended that people under 60 who had one dose of AZD1222 receive a second dose of one of the mRNA vaccines
- On 12th May 2021, the StIKo recommended the vector-based vaccines (AZD1222 and the Johnson&Johnson/Janssen vaccine) only for those aged 60 and above.

It played out in public like this. We first heard BioNTech/ Pfizer and Moderna were good; nothing about AZD1222. Then, that AZD1222 was good if you were under 65. Most of the public knew nothing about the mid-March relaxation of the under-65 restriction. The news about VITT emerged in March 2021, and then Covid-19 Vaccine AstraZeneca (as it was by now called) was not for those under 60 anymore. It also came out that many people were reacting to their first dose of Covid-19 Vaccine AstraZeneca with flu-like symptoms, and being off work for a day was not unusual; examples were covered in the newspapers. (It turned out that there was often reaction to the mRNA vaccines also, but after the second dose, not the first, so this news arrived later).

The result of this was a mess; intelligent people of my acquaintance were saying *"I'll get a jab if it's BioNTech or Moderna but I don't know about this AstraZeneca stuff"*. (I personally benefitted. My state procured some 450,000 extra doses of Covid-19 Vaccine AstraZeneca and offered them over Easter to anyone over 60. I was on the booking WWW site 15 minutes before it opened on Easter Saturday and got my jab Easter Monday. Turns out there was more demand than supply).



Just as VITT emerged in a few people vaccinated with AZD1222, it turns out that some younger people vaccinated with the BioNTech/Pfizer BNT162b2 vaccine (now known as Comirnaty) contract myocarditis and/or pericarditis. However, VITT is a life-threatening event, whereas the heart problems associated with Comirnaty are said to be straightforwardly treatable, e.g., [11]. But here also there is need for political messaging. Human social networks are quite highly connected; it turns out none of us are very far from exceptionally rare adverse events: I have a friend whose friend's husband got VITT after an AZ jab; I have a colleague whose friend got myocarditis from a BioNTech jab. I learned of these by word of mouth, not Facebook or Twitter. Such cognitive "availability" of rare adverse events requires active management to emphasise the rarity of their occurrence, especially in the era of so-called "social media".

One could conclude from this that driving public-health policy purely by science is not ideal. Medical science sees new things about a new disease and its treatment constantly; effective public health messaging needs to be simple, consistent and preferably immutable. These two requirements can easily conflict.

Compounding this is the matter of data and its management. VITT was seen in Vienna and Germany in early March. By April there were some 31 cases in 2.6m first-vaccinations. In contrast, in the UK at the same time there were said to be 4 cases in some 13.7m vaccinations. And then, at the beginning of April the UK retroactively identified 22 firm + 8 more cases. There was a lot of noise in the VITT signal and it took hard work to extract it. In such a situation, formulating consistent public messaging can look all but impossible.

I see these situations as involving multi-system issues, where the requirements/expectations of each localised system (the scientific testing system; the drug approval systems in different states; the record-keeping on associated health problems; the necessary public health messaging and its ideal characteristics) were partly inadequate to the task and partly contradicting each other. Some system engineering could well help improve things.

And Everything Else?

Much of the rest seems to me to fall into the category of political-social. For example, can countries "loosen up" without suffering a new severe wave? The UK tried in July 2021; Germany was not far behind. In Germany, we seem indeed to be into a fourth wave. In Bielefeld, "holiday season" ended mid-August for families with school-age children; daily new infections peaked two weeks later at the end of August; hospitalisation peaked two weeks after that, and deaths started to cluster a week after that. Current thinking seems to be that "opening up" has overburdened neither society nor the health services, and many are relieved at that.

Next, the sociology of continuing to wear masks. Do we or don't we, when and where? Much of it seems to concern what we may be doing and how old we are.

Third, how socially to handle various kinds of denialism (I read in the British Medical Journal a comment from an ICU doctor about dealing with people who are critically ill with a disease which they and their family refuse to believe exists).

I don't think systems scientists have much to say about any of these three issues at present.

End Game

How will this play out? Prognosis of Covid-19 is a mug's game and I am unwilling to enhance my reputation as one. Let me refer instead to some recent public comments.

On 1st October 2021, the Corona Protection Regulations in North Rhine-Westphalia were prematurely loosened (originally, they were valid until 8th October 2021). With Autumn/Winter in Northern Europe, people are generally more indoors with fewer wide-open windows. Both of these entail that conditions will be more favourable for transmission of airborne disease. Respected virologist, avid Covid podcaster and Christmas-ornament model Christian Drosten [12], is concerned that there will be an Autumn-Winter wave in 2021/2, and sees the signs already [13].

Professors Sir John Bell and Dame Sarah Gilbert spoke on 23rd Sept 2021. Sir John believes things "should be fine" once Winter 2021/2 has passed. Dame Sarah observed to the Royal Society of Medicine that viruses become weaker as they circulate, and there is no reason to expect a more virulent version of SARS-CoV-2 to arise [14].

The situation by next spring will likely be dependent on how the proportion of the population that is vaccinated rises. And that seems to be a political question that almost no one can currently answer.

References

[1] https://en.wikipedia.org/wiki/Business_Process_Model_and_Notation, accessed Sept 2021

[2] https://www.gov.uk/government/publications/regulatory-approval-of-ronapreve, accessed Sept 2021

[3] https://www.nejm.org/doi/full/10.1056/NEJMoa2102685, accessed Sept 2021

[4] https://www.astrazeneca.com/media-centre/press-releases/2021/azd7442-prophylaxis-trial-met-primary-endpoint.html, accessed Sept 2021

[5] https://www.merck.com/news/merck-and-ridgebacks-investigational-oral-antiviral-molnupiravir-reduced-the-risk-of-hospitalization-or-death-by-approximately-50-percent-compared-to-placebo-for-patients-with-mild-or-moderat, accessed Oct 2021.

[6] Young, BC, Eyre DW, et al, Daily testing for contacts of individuals with SARS-CoV-2 infection and attendance and SARS-CoV-2 transmission in English secondary schools and colleges: an open-label, cluster-randomised trial, The Lancet 14th Sept 2021, DOI: 10.1016/S0140-6736(21)01908-5, https://www.thelancet.com/journals/lancet/article/PIIS0140-6736(21)01908-5/fulltext, accessed Sept 2021

[7] Viner RM and Koirala A, The Lancet 14th Sept 2021, DOI: 10.1016/S0140-6736(21)02092-4, https://www.thelancet.com/journals/lancet/article/PIIS0140-6736(21)02092-4/fulltext, accessed Sept 2021

[8] Sarah Boseley, The Oxford vaccine: the trials and tribulations of a world-saving jab, The Guardian 26th June 2021, available at https://www.theguardian.com/world/2021/jun/26/the-oxford-vaccine-the-trials-and-tribulations-of-a-world-saving-jab, accessed Sept 2021

[9] https://www.rheinpfalz.de/politik_artikel,-impfkommission-rügt-politiker-_arid,5228866.html, accessed Sept 2021

[10] https://www.rki.de/DE/Content/Infekt/Impfen/ImpfungenAZ/COVID-19/Impfempfehlung-Zusfassung.html, accessed Sept 2021

[11] https://www.cdc.gov/vaccines/covid-19/clinical-considerations/myocarditis.html, accessed Sept 2021

[12] Drosten Rauchermann image, https://www.berlin.de/aktuelles/berlin/6773638-958092-drostenraeuchermann-unter-schutznachfrag.html, accessed Oct 2021.

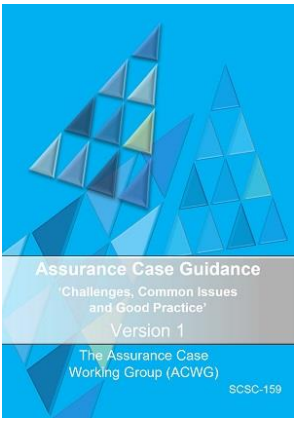
[13] Drosten: Corona-Herbstwelle deutet sich mancherorts an (in German), Die Welt, 24th Sept 2021 https://www.welt.de/newsticker/dpa_nt/infoline_nt/wissenschaft_nt/article234090426/Drosten-Corona-Herbstwelle-deutet-sich-mancherorts-an.html, accessed Oct 2021

[14] Indya Clayton, Oxford professor says Covid could be more like common cold by next spring, Oxford Mail, 24th Sept 2021, https://www.oxfordmail.co.uk/news/19603160.oxford-professor-says-covid-like-common-cold-next-spring, accessed Oct 2021

Prof. Dr. Peter Bernard Ladkin

Peter Bernard Ladkin works in system safety and software-based system dependability. He is retired Professor at Bielefeld University, and Managing Director resp. CEO of British and German companies, both called Causalis, providing services in engineered-system RAMSS. His method Why-Because Analysis (WBA) is used worldwide by some 11,000 engineers. His mandolin playing is improving.

Assurance Case WG – Guidance document and GSN Standard update



The SCSC Assurance Case Working Group (ACWG) has published its first version of the Assurance Case Guidance addressing 'Challenges, common issues and good practice' and an update to the Goal Structuring Notation (GSN) standard. Phil Williams, lead of the ACWG, introduces the updates and explores the relationship between the documents.

The ACWG was established in 2017 with an international cross sector membership from industry and academia. It was formed to provide guidance on all aspects of assurance cases including their construction, review and maintenance. It was envisaged that this be broader than safety and address interaction and conflict between related topics.

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

The products of the working group are made freely available under the creative commons licence.

Publishing the Assurance Case Guidance

The assurance case guidance publication has been created by the ACWG to address shortfalls in available guidance. It was decided early on that it should not attempt to repeat or replace established guidance, rather it should focus on topics that are perceived by the ACWG as containing weaknesses or poor practice and where no, or limited, guidance currently exists.

It is intended to be notation-agnostic and, whilst the experience in creating the guidance is predominantly drawn from the safety discipline, it is intended that the underpinning principles of assurance can be applied to any property – focusing on risk-related properties, for example: safety; security; availability.

The guidance is published as a freely downloadable publication on the SCSC website [1] and is also available for order in hard-copy from Amazon. It comprises:

- A framework that introduces the scope and context of assurance cases
- Topic papers, which each address a specific guidance topic
- Supporting information including terminology, references and acknowledgements

"notation-agnostic …focus on topics that are perceived by the ACWG as containing weaknesses or poor practice and where no, or limited, guidance currently exists"

Guidance topics addressed within the initial version are:

Avoiding Bias in Assurance Cases

Assurance cases are occasionally criticised for being biased in the way that they present their argument and evidence. This topic paper identifies several common biases to be aware of (and thus avoid) when constructing, reviewing and using an assurance case.

The paper addresses the perception that safety cases are biased, only considering the argument 'for' a system being safe. It argues that perhaps the case should instead be challenged to demonstrate that a system is not unsafe/unassured?

The paper sets out several types of bias and considers the potential impact on assurance cases. These include 'Cognitive', 'Confirmation', 'Disconfirmation' and 'Conservatism' biases, as well as the 'Observer-Expectancy' and 'Ostrich' effects.

It recommends cultural change to encourage a Hazard/Threat seeking culture, to seek disagreement and to seek, include and discuss counter-evidence.

Risk versus Benefit

This topic paper provides a discussion on the balancing of risk and benefit. It outlines the need to balance risk against benefit and how to tell when such an argument may be required. It provides examples where risk and benefit have been successfully balanced, and of the structure for a risk-benefit argument.

The paper highlights challenges in considering risk and benefit such as cases where risks may not be experienced by the same people as those who experience the benefit and where measures are subjective and use dissimilar units.

Modular Assurance

This topic paper deals with the structure and presentation of large and complex assurance arguments to support reader comprehension and addresses the benefits in managing the impact of change.

Two types of modularisation are considered: 'Basic' – when the author promises to the reader to come back to a side argument that is distracting to cover at this point; and 'Structuring for compositional arguments', which facilitates arguments created by disparate teams or suppliers.

Guidance is provided on: Structuring the argument; The need for clear assurance case module interfaces; The challenges of composing arguments; Presenting the argument case report; and Properties that are complex to argue in a modular way.

The Risk-Confidence-Conformance Approach

This topic paper introduces the concept of an approach that facilitates clear presentation of arguments structured around the three central themes of risk, confidence and conformance. It addresses the benefits of the approach and offers examples of how these can be presented.

Risk: Argument and evidence regarding risk

Confidence: Why the reader should have confidence in the arguments presented under risk or conformance

Conformance: Demonstration that requirements of standards, regulations and legislation have been met

Dialectic Arguments in Assurance Cases

This paper introduces the concept of dialectic arguments and shows how it can be used to add confidence to an assurance argument while it is being authored or during review/evaluation.

Dialectic arguments provide for the 'investigation of truth' through dialogue. It is a relatively new practice and addresses some of the concerns around bias by bringing counter-argument and counter-evidence into assurance cases.

Dialectic challenges can be characterised as:

- Rebuttal – argument and/or evidence that results in a conclusion counter to that intended by the assurance case
- Undercutting – challenges to the reasoning within the assurance case
- Undermining – raising doubts over the trustworthiness of supporting evidence

Future work

The ACWG is preparing to embark on a new series of activities including the preparation of guidance for the topics of 'Proportionality in Assurance Cases' and 'Assurance Cases across the Supply Chain'.

Updates to the GSN standard

The GSN standard was first published in 2011 by the GSN user community, its maintenance has subsequently been taken up by the Safety Critical Systems Club's ACWG. Version 2 provided an update to consolidate work in progress addressing clarifications from use of Version 1. The standard is complemented by a micro-site of the SCSC's website (https://scsc.uk/gsn), which provides supporting materials including relevant papers, argument patterns and a summary of the changes between version 2 and 3 of the standard.

"Version 3 of the GSN standard provides a major update to address several important extensions to the notation"

Version 3 of the GSN standard [2] provides a major update to address several important extensions to the notation:

Modular Notation Enhancements

Several updates and additions to the definition and guidance associated with modular notation have been included. New terms for module content views have been introduced to clarify the difference between the structure of an argument in GSN and the modules that contain GSN arguments. To reinforce the conceptual differences, some of the modular symbols have been changed to provide greater differentiation. This separation of concepts of structure has also enabled more clarity on how to represent 'containment' of an argument in nested modules – which in turn allows information hiding such that the details of a low-level argument do not need to be made visible in a high level abstracted view of the overall argument.

The update also addressed aspects of the practical use of modular argument that are part of the foundational concepts but were missing from earlier versions of the standard. These include the explicit definition of a module's interface, the formation of inter-module contracts, and the significance of context when forming away-goal relationships between modules.

Confidence Argument Support

New notation extension has been included to support the use of an 'Assurance Claim Point' (ACP) that allows arguments of confidence to be separated from arguments of risk or conformance. These help with providing focus to the thread of the argument in hand without ignoring important side discussions and build on the conceptual work published by Richard Hawkins. See the related discussion of Risk-Confidence-Conformance arguments in the Assurance Case Guidance.

Dialectic Argument Support

A new notation extension has been introduced to support the Dialectic argumentation approach. This allows challenges to the arguments created to be explicitly captured and reasoned about. The challenges may present counter-evidence or counter-argument and record how these impact the original argument. This is a key enabler for the important new approach addressed in the Assurance Case Guidance.

Patterns & Templates

Patterns have been part of the standard from the beginning and defined the graphical symbology and semantics but did not address the wider meta-data associated with a pattern definition from Tim Kelly's original work. This broader definition of a pattern has now been introduced. Templates have also been introduced as a special case of a pattern. A template allows a common repeated pattern in a fully developed argument to be represented by a graphical structure combined with an instantiation table.

General Updates

Several clarifications have been made to the content of the standard, with structural changes to emphasise the core and extension notational elements without the extensions appearing too specialised. These updates are intended to aid readability and provide clarity on the intent of the notation and its use.

Future work

The ACWG is preparing to embark on a further update to consolidate the normative elements of the standard, reinforcing the underlying meta-model and its relationship to the Structured Assurance Case Metamodel (SACM) [3]. It will also address the informative aspects, showing the interrelationship between the core and various extension notations.

The users of the GSN standard and Assurance Case guidance are invited to contribute to the updates to these documents by advising of topics that need to be addressed, or by directly getting involved with the working group. Comments can be registered at the forum (https://scsc.uk/f144). The ACWG can be contacted via its page at https://scsc.uk/gc.

References

[1] SCSC-159, "Assurance Case Guidance - Challenges, Common Issues and Good Practice", Published by SCSC/ACWG, August 2021, Version 1, ISBN: 9798451238592. see https://scsc.uk/SCSC-159

[2] SCSC-141C, "Goal Structuring Notation - Community Standard", Published by SCSC/ACWG, May 2021, Version 3, ISBN: 9798451294949 http://scsc.uk/SCSC-141C

[3] Object Management Group (OMG), Structured Assurance Case Metamodel (SACM), URL: http://www.omg.org/spec/SACM

Note: The version of these documents published on Amazon carries a x.1 version number to signify that there are formatting differences to fit to the standard SCSC hardcopy publication format. The content is essentially the same as the freely available pdf version on the SCSC website.

Phil Williams, Engineer for Safety Limited.

Phil is an independent system safety consultant. He is a Chartered Engineer and Fellow of the Institution of Engineering and Technology. He has over 30 years' experience designing and certifying safety critical systems. He has supported several cross-industry system safety initiatives. Phil is a member of the Safety Critical Systems Club (SCSC) Steering Group and chair of the SCSC's Assurance Case Working Group. Phil is an active member of the BSi GEL65/1 and IST/15 committees; the IEC TC65A MT61508 (developing edition 3 of IEC 61508) and IEC TC65A WG18 (developing IEC 63187 where he is deputy-convenor and principal UK expert). Phil is the lead author of The IET's Code of Practice for Cyber Security and Safety, published in 2020 and available for free download due to the support of the National Cyber Security Centre.

SCSC

FOR EVERYONE WORKING IN SYSTEM SAFETY

Bookings at:
www.scsc.uk/events

This seminar presents the latest thinking regarding adoption of multicore and manycore architectures in safety systems.

It will be useful for safety practitioners and for those involved in the assessment and certification of multicore applications.

Details at: www.scsc.uk

Use of multicore and manycore in safety-critical situations

www.scsc.uk

THE SAFETY-CRITICAL SYSTEMS CLUB

Seminar: Safe Use of Multicore and Manycore Processors

Thursday 11th November 2021, TBC Hotel, London, UK and Virtually Online

This seminar will consider the current state of the art regarding use of multicore and manycore architectures in safety-critical situations. These types of processors offer improved performance characteristics and enhanced functionality and hence are desirable in many safety-related sectors, particularly aviation; there is also pressure from the supply chain to adopt them. Regulatory authorities have provided some guidance on achieving certification but there is more to do.

This seminar will introduce the topic, provide an overview of the roadmap to achieve certification goals, and address specific technical issues.

The speakers will cover various current topics including: an overview of the SCSC working group activities and progress in this area, constructing safety arguments involving multicore, timing analysis and the influence of scheduling on certifiable systems, use of bare-metal virtual machines to improve partitioning, independent verification of the effectiveness of RTOS hypervisors at reducing interference, and finally certification aspects of multicore from a regulators point of view.

There will be Q&A and plenty of opportunities for discussion where delegates can explore the issues and the possible solutions further.

Assessment of Change Safety Cases

Stephen Barker discusses a recent publication from the Civil Aviation Authority (CAA) that provides guidance on the assessment of change safety cases. The guidance is Civil Aviation Publication 1801 (CAP 1801) and is freely downloadable from the CAA website.

CAP 1801, a guide on reviewing safety cases, recently received a minor update. As its original publication wasn't publicised, this opportunity has been taken to make its existence more widely known to the safety community.

The Guidance

The guidance in CAP 1801 is not specific to aviation, to ensure comprehensive coverage, and so is applicable in other industries. It makes no assumptions about the rigour or structure of the safety case being reviewed, and so includes a range of review checks that reflect the likely content of a range of safety cases, from basic arguments and evidence to the more onerous backing arguments that may only be present in safety cases addressing higher levels of risk. Part of the assessment evaluates how the risk acceptability criteria are justified, so supporting whatever approach is appropriate in the application domain.

"CAP 1801 is not specific to aviation, to ensure comprehensive coverage, and so is applicable in other industries"

Whilst CAP 1801 is focussed on review at the point of approval, by inherently defining the required content of a change safety case the material is informative for planning and development stages, and so can support review at these earlier project lifecycle stages.

CAP 1801 coherently addresses multiple concerns in an integrated method. Its assessment method allows for coordination of multiple assessors, accommodating proportionality issues by providing for reviews of varying rigour to reflect the varying content of safety cases addressing different levels of risk. The assessment process is structured to build understanding of the change and the change safety case in a logical sequence, and permits the assessment to be terminated early if it becomes apparent that the change safety case is inadequate.

The method recognises that it is almost always impractical to submit a complete safety case, including all supporting evidence. A safety case report is usually submitted, comprising descriptive material and only an extract of the safety case. Some key evidence items may be included as part of the submission.

Whilst CAP 1801 presents a systematic method, it provides no tutorial material, and assumes the competence of the assessors in all matters, including the application and regulatory domains.

The rest of this article mainly comprises material extracted from CAP 1801, showing the approach behind the design of the guidance, and providing an overview of the assessment method.

Approach and background

A Competent Authority (CA) assesses a change safety case to reduce the probability of an unsafe change entering service, by confirming that the change safety case is valid and that the claimed level of safety is acceptable. The change safety case assessment determines whether the change safety case has significant deficiencies, and hence whether it should be accepted or rejected.

Generically, a valid safety case is a structured argument, supported by a body of evidence that provides a compelling, comprehensible and valid case that a functional system is safe for a given application in a given operating environment. As well as arguing that the service provided by the changed functional system will be provided safely, change safety cases also need to demonstrate that feasible transition plans are in place to implement the planned change. If services are provided while changes are being implemented, then the change safety case must argue that the services can and will continue to be provided safely during this change implementation.

CAP 1801 considers that a change is implemented as one or more 'transitional stage'. Each transitional stage must be justified by the change safety case. The last transitional activities are completed in the final transitional stage, leaving the functional system and service in the

final operational state. The final transitional activity could be just to implement new procedures such that the service is changed.

The change safety case is mainly an argument about the predicted safety of the service that will be provided by the functional system. Although many of the development and safety assurance processes for the change may go through many iterations, only the change and safety assurance established upon completion of all these iterations is relevant to the submitted change safety case.

To argue that the changed service can and will be provided safely, for each transitional stage, the nature of a change safety case is that (in outline) it provides a structured, compelling, comprehensible and valid argument that a valid set of safety criteria has been set for a service and demonstrates that they have all been satisfied. However, this simple argument structure rapidly becomes more complex when taking into consideration different parts of the architecture of the system, the technologies deployed in each part, and the contractual boundaries involved in the provision of the parts.

To be convinced that the changed service can and will be provided safely, the CA must be satisfied that:

- the change safety case addresses the complete scope of the change
- the service(s) to be changed and its constituent systems, subsystems, components, environment and context are specified sufficiently such that a safe change could be designed
- there is sufficient evidence to support the correctness of the specifications, for the operational configuration
- safety criteria for acceptable safety performance of the changed functional system/service have been established, and appropriate safety requirements derived
- the safety performance of the changed functional system/service has been predicted
- the predicted safety performance of the changed functional system/service is acceptable because it meets the safety criteria
- uncertainties do not undermine the change safety case
- the proposed transitional activities are feasible
- the transition activities will be undertaken safely
- there is sufficient evidence that the arrangements to implement the change will be provided
- when the functional system/service is changed, it will be made safe should the change not be successfully completed
- there is sufficient evidence that the arrangements to support the operational system will be provided
- justification that the change is a good change.

However, while a CA needs to be convinced on these points, it is very unlikely that they will be evident as specific claims in the safety case submission due to the complexities of the argument structure. Consequently, CAP 1801 defines a process to identify the elements of the safety arguments that address the above points, and organises the review process around these elements.

CAP 1801 offers guidance on planning and conduct of the assessment. It provides the topics that an assessment should investigate in a safety case. Whilst this guidance is written as if

the assessment is to be conducted by a single assessor, it is structured in a way that can be applied concurrently in a coordinated manner by a team. Assessors must be competent to interpret the generic guidance of CAP 1801 in the context of a specific change.

CAP1801 is not specific to any one particular application domain. It therefore encompasses everything that might be necessary to check any change safety case, without regard to whether it is proportionate for the change in question. Consequently, it might at first sight appear inappropriately onerous for some situations. The guidance addresses this by including planning activities during which appropriate assessment activities are defined, according to the circumstances prevailing. The approach used by the guidance to 'modulate' the assessment according to the risk is overviewed at the end of this article.

The generic method in CAP 1801 could be instantiated for changes in a specific domain or context, or for specific types of change. Such instantiation could usefully include incorporating any specific regulatory provisions or risk criteria for the domain.

The assessment should also be conducted in accordance with applicable regulations and internal procedures. In particular, the CA will need procedures that address:

- receipt of change notifications
- deciding whether a change safety case should be reviewed
- receipt of change safety case submissions/resubmissions
- instigating an assessment of a change safety case using this guidance
- the actions taken following the conclusion of the assessment.

Summary of assessment method

The assessment method in CAP 1801 comprises six Phases:

1) In the first Phase of the assessment, the assessor gains an understanding of the nature and scope of the change, and the structure and organisation of the change safety case. The assessor gains an understanding of the stages in which the change will be implemented, and what the change safety case claims is the scope of the change at each stage, and how this was determined. As part of this process, the assessor identifies and records where key topics are addressed to support later assessment activities. In doing so, the assessor confirms that the change safety case is likely to address a sufficiently wide part of the functional system and is suitable for assessment.

2) As it is impractical to undertake all the candidate assessment activities in CAP 1801 for the complete scope of the change, it is necessary to determine the parts and amount of the change safety case that will be assessed, and which assessment activities will be undertaken. The assessor's obligations govern the strategy for modulating the assessment activities so that some overall objective is achieved, such as seeking the most serious errors in the safety case or gaining confidence in the safety performance predictions. To implement this strategy, the risks associated with the change need to be determined.

Phase 2 establishes the risks used to plan the extent of assessment activities. This is determined from the characteristics of: the changed service, the project, operational/organisational aspects, the change, and the change safety case.

It is possible that, for the lowest grades of risk, the assessment inherently undertaken during Phase 1 could be judged to be sufficient to assess the adequacy of the change safety case, so that no further assessment is required.

3. Plan and assess transitional stage independent parts of the change safety case

3) The planner prepares a plan of an appropriate set of assessment activities to assess the material in the change safety case that is not specific to one of the transitional stages. The risks identified in Phase 2, and the assessment modulation strategy identifies the parts and amount of the change safety case that will be assessed, and which assessment activities will be undertaken.

The assessor then undertakes the assessment activities in the assessment plan, judging whether the change safety case addresses the topics defined in the assessment plan satisfactorily.

If, during the assessment, the assessor determines that the initial planning was based on an incorrect understanding of the risks associated with the change, then the risks are re-assessed (Phase 2) and the assessment plan is revised. The assessment then resumes according to the revised assessment plan.

4. Determine whether the planned change is credible

4) This Phase determines whether the change(s) can and will be made as planned. This confirms that the functional system is likely, in actuality, to exist in the states supported by the change safety case.

This Phase also provides an understanding of the transitional activities that should appear in the safety analyses of the services during each transitional stage, which are assessed in Phase 5.

5. Plan and assess transitional stage dependent parts of the change safety case

5) This assessment Phase assesses the change safety case material for the transitional stages. Each individual transitional stage is assessed using the following Steps:

1) Confirm risk associated with the transitional stages and activities
2) Plan and assess descriptions, declared Safety Management System and claim of safety for the stage
3) Plan and assess the scope of the change
4) Plan and assess specification and safety analysis material (safety criteria, safety requirements and evaluation of acceptability of predicted safety performance)
5) Plan and assess justification of specification elements (arguments of verification)
6) Plan and assess safety of transitional activities
7) Ensure assessment of the transitional stage is adequately completed.

Should any part of the assessment in this Phase result in significant new information about the risks associated with the change, the assessment should revert to either Step 1 of this Phase, or even Phase 2 of the assessment process.

6) The concerns recorded during the assessment are collated and categorised either as a comment or, if the assessor considers that the change safety case would be unacceptable if the concern remained, as a deficiency. An internal CA report and records of the assessment activities are then filed for use in subsequent processes for communication and resolution of the review findings, according to the regulatory context for review of changes.

6. Findings and reporting

Modulation of assessment according to risk

CAP 1801 provides the means to vary the assessment of any change safety case according to the associated risk factors, by choosing activities that have appropriate rigour, varying the sample size, etc. Methods for doing this are outlined, but are not formally defined, as it is not yet sufficiently understood how this can be achieved.

The overall approach implemented in CAP 1801 is that relevant aspects of the change, the change project, the change safety case, etc are considered and used to identify the 'risk factors' that govern the assessment.

"CAP 1801 provides the means to vary the assessment of any change safety case according to the associated risk factors, by choosing activities that have appropriate rigour, varying the sample size, etc."

Given that a complete assessment is impractical, the assessment is planned to reflect the risks associated with the identified risk factors. In principle, greater rigour is used when assessing:

a) change safety cases for which there is greater risk, as identified by the identified risk factors
b) the parts of a change safety case relating to the risk from the identified risk factors.

The assessment is planned by selecting from the candidate assessment activities defined in CAP 1801 for each topic of the change safety case (e.g. the specifications), at the same time defining the scope (e.g. of the system, safety argument) for each activity, resulting in a review that is modulated in accordance with the risk factors. Planning is conducted incrementally as the assessment progresses, so that the assessment activities are planned on the basis of the latest, most complete understanding of the change and the change safety case.

Conclusion

The guidance consolidates many different facets of the assessment problem into an integrated and flexible approach. It is based on real-life experience, coupled with a desire to identify how safety cases can be improved by identifying what an assessor needs to determine whether it is acceptable. It is hoped that this guidance for assessing safety cases will assist other organisations wishing to establish a systematic approach to conducting risk-based assessments, as well as informing those preparing safety cases for assessment.

CAP 1801 was written by Stephen Barker and Andrew Eaton, and is freely downloadable from the CAA website [1].

References

[1] "CAP1801 Guidance: Assessment of Change Safety Cases": https://www.caa.co.uk/CAP1801, CAA, June 2021, Issue 1.1

Stephen Barker and Andrew Eaton

Following 20 years' experience in electronics and software development, safety and reliability consultancy and third-party inspection for various industries, Stephen Barker has for more than 20 years been a Safety Assessment Engineer for the Safety and Airspace Regulation Group of the United Kingdom Civil Aviation Authority. Whilst specialising in assessing software-based systems, he has conducted various oversight activities relating to the safety of air traffic control in the UK, with an emphasis on En-Route air traffic services. Stephen recently retired from the CAA.

For the past twenty-eight years Andrew Eaton was a National Requirements & Strategy Specialist for the Safety and Airspace Regulation Group of the United Kingdom Civil Aviation Authority. His field of responsibility was safety assurance of safety related Air Traffic Control and Management services. In this role he was responsible for advancing the UK's capabilities in these areas and sat on several international standards and regulatory committees. Andrew has an MSc in safety critical systems engineering from the University of York and is now an independent consultant.

THE SAFETY-CRITICAL SYSTEMS CLUB

SCSC
FOR EVERYONE WORKING IN SYSTEM SAFETY

Seminar: Managing 'Black Swans':

Handling Rare and Severe Events Now and in the Future

2nd December 2021, TBC Hotel London and Streaming

Bookings at:
www.scsc.uk/events

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

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

Details at: www.scsc.uk

Managing Unexpected Events Now and With Autonomy

www.scsc.uk

This seminar will consider how to manage recovery from 'Black Swan' events in a safety context, ie. events which are rare, unexpected and have high impact. Events such as Fukushima Daiichi nuclear disaster or the loss of Malaysia Airlines Flight 370 might be examples. However these events can occur in any sector.

Sometimes an organisation has an idea that these types of events might occur but is unprepared due their rarity or low likelihood. There are several aspects to the management of such events: i) Establish the nature and scale of the problem; ii) Stabilise the problem; iii) Avoid a cascade of failures; iv) Assess risks; v) Continue with a limited or contingency service where necessary; iv) Engage management and vi) Recover operations.

One key element is how to assess risk in an urgent and critical situation. Communication, reliable information and rapid assessment are important, and perception is key. Hard data will be limited, and human factors, organisational experience and safety culture come into play.

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

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

Cost and registration: Club members: £195, including lunch and refreshments (no VAT). Non-members additional £125 for Club membership. Concessions: £95, which includes free membership for one year. Streaming rate £95. Joining instructions and the programme will be sent to delegates before the event. Delegates must book their own accommodation (if required).

How Do I Get Into Safety?

It is sometimes difficult to plan a career: so many things have to align together for each step on the ladder to take place, whether it is the correct training, organisation, job or assignment, or simply just being in the right place at the right time. We are sometimes asked: "how do I get into safety?"

The answer isn't straightforward. In fact, it is doubly difficult to plan a career in safety engineering, assurance, or consultancy as a solid background in the underlying technologies (such as software, architectures, or databases) and sector knowledge (eg. aviation, nuclear or rail), plus the right opportunities all have to be present.

Safety is often a second career, taken on by engineers or consultants who have already got several years of experience doing other things. Also, there is the issue that not many safety staff are required for most jobs: often there is only one safety engineer on smaller projects; if that role is already taken, there is little chance of a junior gaining relevant experience.

With this situation in mind, in this, the first of a series of articles to be published over the next few newsletter editions, some members of the SCSC Steering Group have shared their experiences of 'getting into safety'. Some of the routes taken are definitely not linear!

Please read and compare with your own 'safety story'. Of course, these experiences are based on events some time ago, and the situation has definitely improved as the industry has matured. For example, there are now courses (at post-graduate level) on safety-critical systems such as those at the University of York, there are competency frameworks for safety roles, and the SCSC has started a new programme called the "Safety Futures Initiative" with the aim of developing young and early-career staff so that they can take on full safety roles.

The messages that come out of these experiences however, are that sometimes you do just have to be in the right place at the right time, and with the right underlying characteristics. All safety roles require the ability to be able to assess risk, to understand some difficult technical arguments, to follow (and create) workable processes, rules and regulations, to know the standards and guidelines relevant to the job in hand, to be able to communicate well, work in a team with colleagues, and very importantly, to be assertive and take a strong position when needed.

Graham Jolliffe

Although it's an awful pun I got into safety by accident (groan). I was an Air Engineer in the Fleet Air Arm (FAA) posted to Boscombe Down to undertake some software integrity tasks on aircraft weapon systems. It was thought I would be good for this task because of my recent experience implementing IT systems. Of course, the two roles had little in common with each other as I soon found out. I subsequently spent a substantial amount of time arguing with industry to take software integrity seriously and not always successfully. I subsequently returned to the FAA for a few more years before retiring from the Royal Navy and accepting a civilian role back at Boscombe Down.

My new role had similarities to my previous experience, but I found that industry was now even less willing to incur the costs associated with high integrity software. What I needed was a systems approach to arguing for appropriate software integrity. The challenge closest to me at the time was being able to demonstrate that the Merlin digital Flight Control System (FCS) was fit for purpose. There had been a long running debate regarding whether Static Code Analysis should be used with no clear decision. It was at this time that I was introduced to Goal Structuring Notation (GSN). By using GSN it was easier to communicate the need for additional evidence to support the use of the FCS. There was some urgency as there was less than a year to go before the aircraft was due to become operational. However, GSN proved its worth and together with identifying an expedient means of conducting a limited analysis of the FCS code, we were able to provide a convincing argument that the FCS code was acceptably safe.

Realising the potential of GSN was like a light coming on, and when mixed with a degree of pragmatism, it enabled the communication of safety to be much better understood by those in authority. This was a turning point in my career, and I've not looked back.

Tom Anderson

My personal interest in safety issues was largely driven by an appreciation of causality with reference to accidents in the railway sector, initially triggered by reading LTC Rolt's lucid treatment in "Red for Danger". However, as an academic at Newcastle University my work was on the generic issues of system dependability, but with a focus on dynamically tolerating faults – especially faults in the design of a system. We established a connection with Bev Littlewood at City University, and that led to the establishment of the Centre for Software Reliability (CSR) in 1984. From the outset CSR actively engaged with industrial and commercial practitioners and this motivated the establishment of a UK industry-based Software Reliability and Metrics Club (which held its first meeting in October 1984).

At that time, the level of control of infrastructure and plant given to embedded computing devices was rapidly increasing and also becoming much more prevalent; this naturally gave rise to significant safety concerns. In response, government, institutions, industry and academia developed a number of initiatives with the aim of raising awareness and addressing the risks to safe operation. The (then) DTI (Department for Trade and Industry) and EPSRC (Engineering and Physical Sciences Research Council) issued a call for proposals to develop

a UK community addressing the safety of computer-based systems. Working closely with the BCS (British Computer Society) and the (then) IEE (Institute of Electrical Engineers), CSR put forward a proposal for a Safety-Critical Systems Club; this proposal was awarded three years' funding, but the Club was required to be financially self-sufficient thereafter. A very successful inaugural meeting was held in Manchester in July 1991, attended by 256 delegates. Now, after having had oversight of 25 years of successful operation of the SCSC from its original base in CSR at Newcastle University, it is a pleasure to observe the Club's continued development and growth in recent years while based at the University of York, and now moving to a formally incorporated independent status as a Community Interest Company.

Mike Parsons

I worked on safety systems early in my career – but didn't know it! My first industrial job was a software developer on Gamma camera systems (body scanners used in hospitals looking at things like heart function), but this was way back in time when there was no mention of standards or a safety process. Around 1993, I decided I really wanted to work in the Space sector (my childhood dream was to be an astronaut!) and so joined Logica in 1995 on a very safety-critical project – trajectory monitoring for the Ariane space launcher, working on software quality, configuration management and installations. I wasn't doing safety as such, but was aware of some of the safety analysis being done, and was amused to see probabilities of component failures coming out as negative due to rounding errors!

I got my big break in safety on a space project producing a GPS (Global Positioning System) safety overlay in 2000; I was chosen by the then project manager to do safety as I "had the right attitude" – whatever that meant! I was sent on safety courses and learned the ropes; devising tools and techniques to automate analyses and metrics. It was about this time that I became aware of the SCSC and attended my first Symposium, which I thought was great! From then on it was more and more safety: taking on bid roles, further project safety roles, developing new safety processes, and finally managing all the safety projects in Logica UK, as well as looking after a safety team.

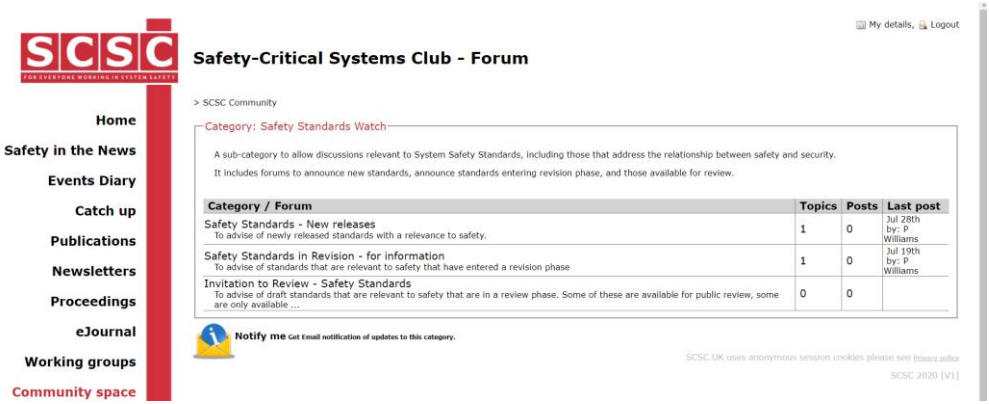
I took on some SCSC roles during this period: I was invited to join the Steering Group by Tom and Joan and later suggested the Data Safety Initiative was formed, becoming the Working Group Leader. I also took on the SCSC Events Coordinator role taking over from Chris Dale.

I had a 3-year spell at NATS (National Air Traffic Services) working on assurance of new cloud-based systems before returning to Logica to cover safety on various healthcare projects. When Tim Kelly left to take up his new life in the Church of England, I took on the SCSC Director role as well. My latest role is on the Assuring Autonomy International Programme at University of York.

Throughout my career I have found the SCSC an invaluable resource, the events interesting and relevant, and club members always helpful and willing to give advice and support. It is a really useful network of like-minded people! My one bit of career advice would be to take any openings you are presented with – you won't get a second chance!

Stories from other members of SCSC Steering Group will appear in future editions. See also Dr Emma Taylor's 60 second interview on page 43 for insight into her career journey.

Safety Standards Watch



A new community forum has now been set up called the "Safety Standards Watch". This will allow members to be notified when new draft standards are available for review prior to their formal publication.

Accessing the Forum

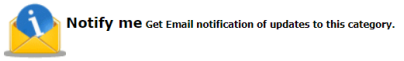
To visit the Forum, logon to the SCSC website and select the **Community space** menu option on the left-hand side.

You can also go straight to the forum through this web link: https://scsc.uk/f295. There are three forum subcategories:

- **Safety Standards - New releases**: To advise of newly released standards with a relevance to safety
- **Safety Standards in Revision - for information**: To advise of standards that are relevant to safety that have entered a revision phase
- **Invitation to Review - Safety Standards:** To advise of draft standards that are relevant to safety that are in a review phase (participation in the reviews is an exclusive SCSC member benefit)

Registering for Alerts

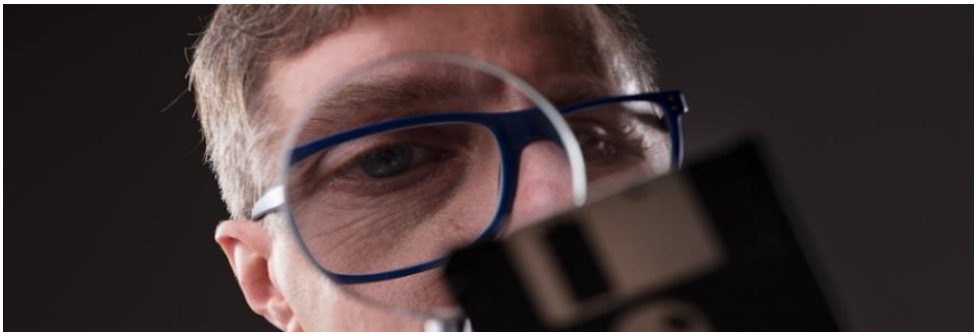
To be notified by email when new items are added to any of the forum categories, simply click on the "Notify me" button at the bottom of the page. You can cancel your notification alerts at any time by selecting "Cancel notification".



Contributing

Registered users are encouraged to contribute to the forums – so if there are important developments in a standard you become aware of, then please use the forum to let the community know.

Software Maintenance: Legacy and Archaeology Event Report



This online seminar held on 6th May 2021 considered how to carry out software maintenance for legacy software that is still fulfilling a safety function. Much legacy software is not properly documented and historically poorly maintained, so what strategies are available to ensure changes can be properly assured?

Mike Parsons introduced the seminar speakers and opened by noting that many safety systems are old, yet the software still needs to be modified in a safe manner. Many changes such as security related changes can be tricky; and it is not just code modifications that are an issue; tests, documentation and associated analyses are also of concern.

It was never designed to do that!

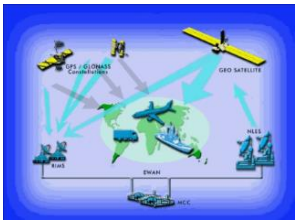
Simon Scutt from Thales, provided a brief history of the Watchkeeper Unmanned Aerial System (UAS), which was based on a design originally introduced in 1998 and commissioned almost 10 years later, with full operational capability in 2018. He noted the platform has been used successfully, but there have also been some notable accidents. Simon covered the regulatory framework and the programme organisational structure, noting that the regulator (The Military Aviation Authority) was established after the programme was started.

Simon explained that changes are classed as minor or major and that classification determines the level of approval required. All changes must be submitted by Thales as the overall coordinating design organisation with Defence Equipment & Support (DE&S) acting as the overall Technical Approval Authority. Changes are impact assessed using a proprietary change classification focussing on impact against the type certification basis.

This results in a Modification Assurance Report – something akin to a delta safety case. The level of supplier assurance is determined by the impact of the subsystem/component on airworthiness and safety, the criticality of the component and the maturity/experience of the supplier.

Independent audits are also undertaken by the regulator and the overall authority as required by DO-178B (Software Considerations in Airborne Systems and Equipment Certification) for a DAL B software system. Simon noted that safety cases tend to be deltas rather than full re-releases and concluded by saying that the main issues are with getting access to suppliers' proprietary information.

Still improving after 20 years of maintenance



Peter Niemann from CGI discussed the European Geostationary Navigation Overlay Service (EGNOS) Check Set. EGNOS is a satellite-based augmentation system providing corrections and integrity information for GPS systems and is actively being used to land aircraft. Peter described the Check Set component that checks the main processing and ultimately protects users from hazardously misleading information. The Check Set is therefore developed to documents based on Level DAL B of the DO-178B guidance.

ESA has overall responsibility for EGNOS and the service is operated by the European Satellite Service Provider (ESSP). The system was developed from 1999 with open service in 2005 and safety of life service from 2011. There has generally been one release per year and the code has grown from 60,000 to 87,000 lines over a period of 20 years. Peter discussed the main drivers for maintenance changes:

Standards Clarification: What was certifiable against DO-178B historically may not meet expectations in 2021, as a result of clarifications of ideas and objectives and global lessons learnt from its evolution to DO-178C. For example, management of derived requirements, control and data coupling, tool qualification etc. This has had a positive impact and strengthened the product with improved compiler warnings, options and exception; strengthened development processes and resulted in better tracing to address expectations.
Bugs: When defects are discovered, systematic checks for similar bugs are undertaken and analysis and lessons learnt on processes carried out.
Perfective: changes have come from algorithm enhancements and refinements.
Adaptive: hardware and software obsolescence.
Peter said that EGNOS has a strong track record of managing the challenges of changing a complex legacy system and noted the following key success factors:

- Co-operative analysis amongst all stakeholders: prototyping, analysis and evaluation before implementation eliminating unsuccessful enhancement candidates. However, the process can take 4-8 years.
- Test data selection: include live real capture where possible, regular updates based on operational data, coordinated with stakeholders, independence.
- Expertise retention: succession planning, training, up-to-date documentation, retaining expertise.
- Good practices: metrics, coding standards, reviews and configuration management.

Peter concluded that maintenance has generally improved the product but some decisions cannot be undone, for example in the use of tools and design representation.

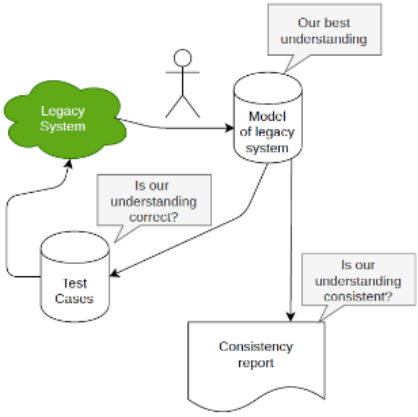
But I only changed 5 lines of code!

Chris Hobbs explained that Blackberry QNX produces operating systems and hypervisors certified to standards such as IEC 61508[1], IEC 62304[2], ISO 26262[3] and CENELEC[4] standards. Chris said the company's operating systems are widespread and can be found in many devices that we all use today, such as in cars and network routers and used in many different domains such as medical, railway and automotive. He said that although these are certified, there is a lot of legacy code, some dating back to 2002.

Chris illustrated two types of errors the "Bohrbugs"[5] – often obvious and the "Heisenbug", which only manifest themselves infrequently and under subtle timing conditions such as race conditions. He noted that even in legacy code, new bugs are still emerging, and gave a recent example where a race condition arose when the number of processors in a multicore solution was increased.

Chris referred to IEC 61508-3-1 'proven in use' requirements and said that this sets the bar high and was not usually practicable for legacy code.

He illustrated that even the simplest program has too many states to test, and gave an example of an incremental change to code that may initially yield correct results thus increasing the level of confidence, but would eventually fail in unexpected ways.



Chris asserted that testing can never be exhaustive apart from where formal proof is used, it otherwise only results in increased confidence-in-use.

Chris argued that testing can be more effective by reducing the number of states to be tested and introduced Combinatorial Testing[6], which exploits the fact that human written code has few sub-conditions in a conditional statement.

Chris concluded by describing an approach to assure significant structural changes being made to some legacy code, which was not fully documented. The approach was to build a model (and simulation) of the part of the legacy system that was to be changed. This allowed test cases to be created automatically to validate the model. A model of the changed system was then built and combined with the previous model to generate test cases and a consistency report on whether the system would meet the requirements. This revealed issues with the design, and found potential "Heisenbugs" that might otherwise have been missed.

[1] Functional safety of electrical/electronic/programmable electronic safety-related systems
[2] Medical device software — Software life cycle processes
[3] Road vehicles – Functional safety
[4] European Committee for Electrotechnical Standardization
[5] en.wikipedia.org/wiki/Heisenbug
[6] en.wikipedia.org/wiki/All-pairs_testing

Modern verification meets old code...

Rod Chapman from Protean Code Ltd has worked in a wide range of sectors, such as air traffic control, railway, military and commercial aviation and said that these tend to have software systems that are very long lived. Systems typically tend to be in service much longer than originally expected, sometimes over a decade. Rod considered two questions:

- what would he do if he was asked to reactivate and make a change to a legacy system?
- what would he do now to help future maintainers of the software in the long term?

Reactivating an old legacy system

Rod said the main problems with legacy systems are obsolescence of technology, platform, suppliers and people but modern technology can help, such as through the use of increased computer resources, including cloud, Infrastructure-as-Code (IaC), formal/static analysis and aggressive testing.

Rod said that generic compute resources are extremely cost effective now and resources can be rented not bought and easily scaled to more powerful systems as required. IaC can also setup virtual environments repeatably and make environments more readily available to developers including making representative target production environments.

Formal/Static Analysis tools have hugely improved and will find bugs but generally is "best efforts" and won't find all bugs. Application to legacy code also results in lots of warnings and false alarms. However, a "don't get any worse" strategy could be adopted, or eliminate warnings one class at a time until all are resolved.

Rod said if there is no specification or test cases then there are lots of tools now that will test code automatically and others like AddressSanitizer[7] for C/C++ that can monitor running code and detect issues such as resource usage. Some tools can simply run random data through the program (called "Fuzzing") and will find bugs.

What to do now to help future maintainers?

Rod said that the main challenge is economics – most current software has a short half-life and it is hard to make commercial decisions now that will pay off in many years and so software for the long-term is a niche market. He recommended the following:

- Beware of fashion; look for systems and companies that have a long pedigree
- Choose formal languages – their meaning doesn't change over time
- Exploit virtualisation and cloud for everything
- Freeze/snapshot virtual machines at every release point of a system
- When shutting down a project, have a re-activation plan and dry run this with someone with no previous knowledge of the system
- Commit to a long-lived architecture or deploy in a Field Programmable Gate Array
- Plan and build with multiple versions of all tools

Report by Paul Hampton, SCSC Newsletter Editor

[7] https://en.wikipedia.org/wiki/AddressSanitizer

Getting to Know You
An update from the Safety Futures Initiative

Zoe Garstang, lead for the Safety Futures Initiative (SFI), gives an update on the progress made by the SFI and provides details of future events.

Get To Know You Event

On the 1st of July 2021, the Safety Futures Initiative (SFI) held their first virtual engagements to showcase the group, its aims, and gather the input of prospective members to understand the elements that they would like to see from the SFI. There were two events held over Zoom; one at lunchtime and one in the evening to maximise availability.

Each event began with an ice breaker activity to learn more about the attendees in the session, followed by an overview of the SFI and then the floor was opened to questions and comments from the delegates as part of a brainstorming session. The brainstorming was a successful activity, and a number of great suggestions were put forward – from mentoring schemes to technical and career workshops. The suggestions either reinforced the need for existing ideas or gave the SFI new food for thought to take forward.

As a result of the positive feedback following these 'Get to Know You' events, the SFI will be holding regular lunchtime sessions (12:00-13:00) for new and existing SFI members to network and discuss any aspect of the SFI in a welcoming and safe environment.

The next "Get To Know You" events will take place on 24th November 2021

If you are interested in attending any of these free events, please sign up via the link below. A more detailed agenda will be sent to registered delegates nearer to each event.

Looking Ahead

Activities within the SFI are picking up. The current projects include developing a series of podcasts on career and technical topics, as well as working on our first workshop to support members in developing technical and/or soft skills. The SFI is also working closely with the SCSC Steering Group to develop the club's Equality, Diversity and Inclusion strategy.

If you would like access to these upcoming events and resources, please consider following the SFI via the link: https://scsc.uk/gf

If there is anything you would like to see from the SFI, in order to support Early Career Professionals, please do get in touch with the SFI – all suggestions are welcome. Also, if you would like to contribute to the management of the SFI, please do make your interest known to us at: zoe.garstang@scsc.uk

Zoe Garstang, Airworthiness Engineer and SFI Lead

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

Connect

The Newsletter and eJournal

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

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

The SCSC Website

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

Facebook

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

www.facebook.com/SafetyClubUK

Twitter

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

LinkedIn

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

www.linkedin.com/groups/3752227

Advertising

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

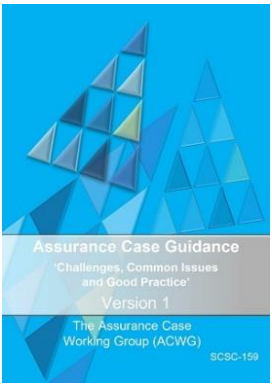
SCSC Working Groups

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

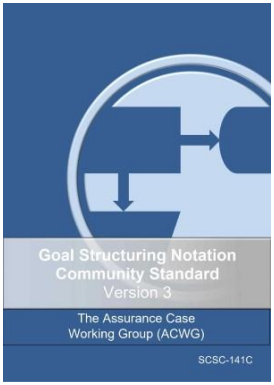
Assurance Cases

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

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



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



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

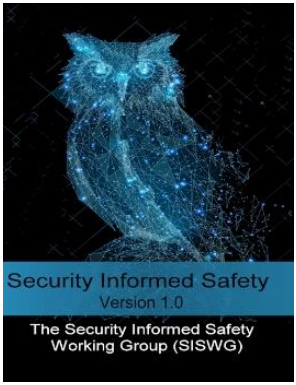
See scsc.uk/gsn for further details.

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

Lead Phil Williams phil.williams@scsc.uk

SCSC Working Groups

Security Informed Safety



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

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

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

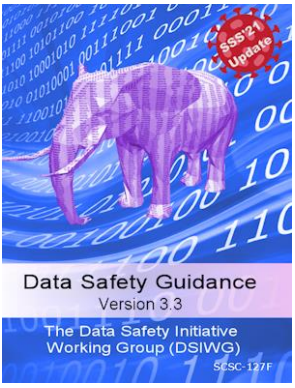
Lead **Stephen Bull** stephen.bull@scsc.uk

Data Safety Initiative

Data in safety related systems is not 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.

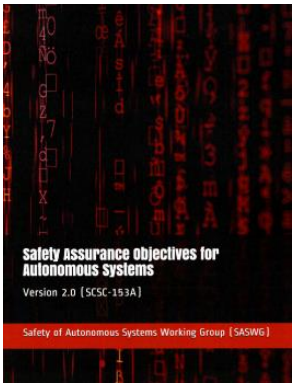


An update to the guidance (v3.3) was published in Feb 2021: scsc.uk/scsc-127F

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

SCSC Working Groups

Safety of Autonomous Systems



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

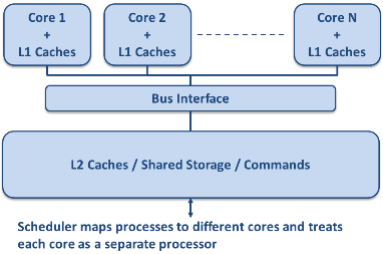
It is clear that autonomous systems can introduce many new paths to accidents, and that autonomous system technologies may not be practical to analyse adequately using accepted current practice. Whilst there are differences in detail, and standards, between domains many of the underlying challenges appear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

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

Lead Rob Alexander rob.alexander@scsc.uk

Multi- and Manycore Safety

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



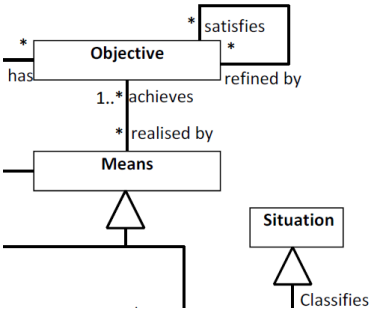
Parallel processes need to access the same shared resources, including memory, cache and external interfaces, so they may contend for the same resources. Resource contention is a source of interference which can prevent or disrupt completion of the processes, meaning it is difficult to know with a defined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

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

Lead Lee Jacques Lee.Jacques@leonardocompany.com

SCSC Working Groups

Ontology



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

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

The Data Safety Working Group (DSIWG) developed the core aspects of the Risk Ontology, which has been migrated to this working group. The Risk Ontology will form the upper ontology to the Data Safety Ontology that the DSIWG will continue to develop.

Lead Dave Banham ontology@scsc.uk

Covid-19

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

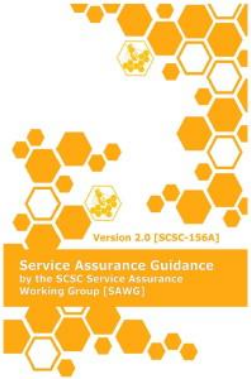
The group has compiled an extensive range of Covid-19 related material and made this available on the working group's website pages along with ongoing developments in the thoughts and ideas of the group.

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

Lead Peter Ladkin ladkin@causalis.com

SCSC Working Groups

Service Assurance



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

The group has published v2.0 of the guidance: scsc.uk/scsc-156A

Lead Mike Parsons mike.parsons@scsc.uk

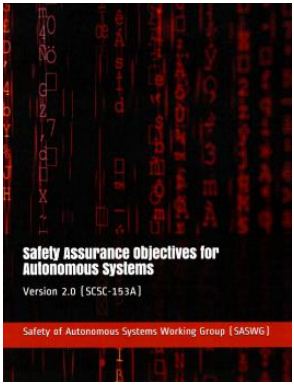
SCSC Safety Culture

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

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

Lead Michael Wright michael.wright@greenstreet.co.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

60 Seconds with … Dr Emma Taylor

Dr Emma Taylor is Head of Digital Safety at RazorSecure, a rail cyber security solutions company, and a Chartered engineer with 30 years' experience across aerospace, energy and transport. She is a Visiting Professor at Cranfield University, a Fellow of multiple Professional Engineering Institutions and holds a number of industry awards e.g. this year's Computer Weekly Top 50 Influential Women in UK Tech.

She is a Past-Chair of the Safety and Reliability Society, and an honorary member of the SCSC Steering Group, and, as a cross-sector safety and risk engineer, she works too – most recently in a series of RSSB-hosted podcasts in response to the RAIB Cambrian ERTMS incident. She works closely with a number of organisations across the UK rail supply chain, including commercial, university research, governmental and related agencies, and engages with SCSC Working Groups wherever resources allow, including Security Informed Safety WG and Service Assurance WG. Emma expresses her personal views in this edition's 60 second interview.

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

I was working in the field of System Safety from age 18 as an undergraduate systems engineer with British Aerospace Space Systems, I just didn't realise it at the time. When I was looking at resilience of satellites and space stations under space debris impact, or working out whether a satellite would collide with another and so increase the overall risk in orbit, I was taking a system perspective and ensuring safe operations for myself and others. Everything connects back to a system safety mindset in one way or another. Now of course I'm working in the rail industry where regulatory oversight and system safety is front and centre, you can see clearly and directly the contribution you are making and the expectations on you and your projects.

What aspect of your career are you most proud of?

That's a tough one to answer! I think it's switching sectors and developing the technical knowledge, whether Oil & Gas platforms or rolling stock and infrastructure on the train network. System safety skills are of course cross-sector and we usefully learn a lot by looking at other incidents in other sectors. But, the tough truth is that in order to make a useful contribution you need to master the technical underpinnings. With that in mind, starting my cybersecurity career at age 50 with a Venture Capital funded, GCHQ accelerator enabled, rapidly growing scale up, definitely counts as the thing I am most proud of, to date at least.

What advice would you give to yourself age 12?

Take advice from a wide range of sources. The best path isn't always the linear path. As a mentor, I am always encouraging others (and myself) to do skills gap analysis and to look at alternative ways to get the experience to fill that gap. You don't necessarily need to have a job with a specific title to develop yourself.

How do you feel about being shortlisted for the 2021 most influential woman in the UK?

It's all a bit surprising really, as it's by Computer Weekly, for women in tech, and I'm only 4 months into my cybersecurity role. But it does reflect the increasing importance of understanding the role of what I call digital parts (whether embedded software, network systems etc.) play in overall operations. I foresee growth in digital accidents and investigations, and this is what I'm focussing my Visiting Professorship at Cranfield on.

What's your most favourite quote or motto?

"Model the way". It was taught to me by a coach nearly ten years ago now when I was involved in the crisis management, recovery and rapid growth of a consultancy team. It helps me translate ideas and plans into actions, and to get practical. What do I need to do today and tomorrow to move things forward, changing and updating as needed.

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

Fly (a plane). I like the idea of mastery. This is a tall order, given that I can barely ride a bike and don't have a driving licence! My spatial awareness isn't that good, so I think it's best that this goal stays in my imagination.

How important do you see the work of the SCSC?'

The SCSC occupies an important and unique niche by providing a rich network of system safety professionals. I particularly appreciate the opportunity to share experience and ask "what if?" questions and the culture of trust and collaboration. I am a better system safety professional as a result of my engagement with my SCSC colleagues.

"The SCSC occupies an important and unique niche by providing a rich network of system safety professionals"

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

I like *Avengers Assemble* because it highlights how we all bring different skills to the technical party and how a team is greater than the sum of its parts. People are also themselves, with all their unique characteristics, positives and flaws too. I'll leave it to others to decide which of the characters is closest to me!

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

Make a plan. It doesn't matter if it's just half a page, and you can change it afterwards, plans always change. The advice was from my first mentor back in 2000. Despite his encouragement, I never did it. I've learnt better now, it's amazing just how the act of writing something down and leaving it to rest helps focus your activities. I have 6-month plans, 5-years plans and more.

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

Stephen Bull

stephen.bull@scsc.uk

Jane Fenn

jane.fenn@scsc.uk

Paul Hampton

paul.hampton@scsc.uk

James Inge

james.inge@scsc.uk

Graham Jolliffe

Honorary member

Alex King

alex.king@scsc.uk

Mike Parsons

mike.parsons@scsc.uk

Roger Rivett

roger.rivett@scsc.uk

Emma Taylor

Honorary member

Sean White

sean.white@scsc.uk

Robin Bloomfield

Honorary member

Dewi Daniels

dewi.daniels@scsc.uk

Zoe Garstang

zoe.garstang@scsc.uk

Louise Harney

louise.harney@scsc.uk

Brian Jepson

brian.jepson@scsc.uk

Tim Kelly

Honorary member

Mark Nicholson

mark.nicholson@scsc.uk

Felix Redmill

Honorary member

John Spriggs

john.spriggs@scsc.uk

Phil Williams

phil.williams@scsc.uk

Club Positions

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

Managing Director

Mike Parsons 2019-

Tim Kelly 2016-2019

Tom Anderson 1991-2016

Steering Group Chair

Roger Rivett 2019-

Graham Jolliffe 2014-2019

Brian Jepson 2007-2014

Bob Malcolm 1991-2007

Programme & Events Coordinator

Mike Parsons 2014-

Chris Dale 2008-2014

Felix Redmill 1991-2008

Manager

Alex King 2019-

Newsletter Editor

Paul Hampton 2019-

Katrina Attwood 2016-2019

Felix Redmill 1991-2016

University of York Coordinator

Mark Nicholson 2019-

eJournal Editor

John Spriggs 2021-

Administrator

Alex King 2016-

Joan Atkinson 1991-2016

Website Editor

Brian Jepson 2004-

Safety Futures Initiative Lead

Zoe Garstang 2019-

Nikita Johnson 2019-2021

Calendar

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	

May '22

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

June '22

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

July '22

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

August '22

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

September '22

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

Events Diary

21 October 2021 SCSC Seminar **Can we quantify risk?** **London, UK + Online** scsc.uk/e800	**9 November 2021** **Conference** **High Integrity Software Conference** **Online** www.his-conference.co.uk	**10 November 2021** SCSC Working Group **SCSC Service Assurance Working Group Meeting #37** **Portsmouth, UK + Online** scsc.uk/e858	**11 November 2021** SCSC Seminar **Safe Use of Multi-Core and Manycore Processors** **London, UK + Online** scsc.uk/e812
24 November 2021 SCSC Working Group **SFI: Safety Futures Initiative "Get To Know You" event x2** **Online** scsc.uk/e856	**2 December 2021** SCSC Seminar **Managing 'Black Swans': Handling Rare and Severe Events Now and in the Future** **London, UK + Online** scsc.uk/e825	**9 December 2021** SCSC Working Group **Multi/Manycore Working Group Plenary #15** **Online** scsc.uk/e843	**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

Safety-Critical Systems Club

SSS'22 PROGRAMME

scsc.uk/e797

30th Safety-Critical Systems Symposium

BLENDED CONFERENCE

8th - 10th February 2022

SCSC

FOR EVERYONE WORKING IN SYSTEM SAFETY