The Safety-Critical Systems Club Newsletter

Safety Systems

Vol 31 No. 2 - May 2023



PORTRAITS OF WOMEN

Celebrating the women in System Safety

WELL MET!

Highlights of the 31st SCSC Symposium

HEAVY-DUTY SAFETY

Assuring Heavy-Duty Mobile Machinery

For everyone working in Systems Safety

SCSC

thescsc.org



SCSC Publication Number: SCSC-184

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

© SCSC CIC 2023 except where explicitly stated for specific articles, reports or images.

Front Image Portrait of Ada Lovelace by British painter Margaret Sarah Carpenter (1836) – public domain. Ada Lovelace (10 Dec 1815 – 27 Nov 1852) was an English mathematician and writer, chiefly known for her work on Charles Babbage's proposed mechanical general-purpose computer, the Analytical Engine. She was the first to recognise that the machine had applications beyond pure calculation, and to have published the first algorithm intended to be carried out by such a machine. As a result, she is often regarded as the first computer programmer.

Back image: artwork by Charisse Lin (age 7), reproduced with permission
In Brief images on page 4 may be subject to copyright – see scsc.uk/f138 for details.

Contents

WELCOME

Editorial 3

Opening words from the SCSC Newsletter Editor.

In Brief 4

Recent system safety news items from around the world.

FEATURES

International Women in Engineering Day (INWED) 5

Wendy Owen provides the female perspective through stories from some of the woman of SCSC.

SSS'23 Event Report 19

Paul Hampton provides highlights of this year's Safety-Critical Systems Symposium.

POSTER SESSIONS 33

The posters highlighting the work and developments of groups, such as the SCSC Working Groups, as presented at SSS'23.

Innovative Hydraulics and Automation Lab 47

The safety assurance challenges of highly automated heavy-duty mobile machinery.

REPORTS

The Future of Testing for Safety Critical Systems 51

Highlights from the seminar focussing on testing, held in December 2022.

STEAM GWR Museum Tech Trip Report 59

Mike Parsons reports from the last SCSC Tech Trip.

60 Secs with ... Jane Fenn 63

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

Recent Publications 65

Recent system-safety related publications.

GROUPS

Working Groups 68

Details of the SCSC Working Groups.

SCSC Steering Group 74

Who's who in the Steering Group.

EVENTS

Calendar 76

Events Diary 77

SCSC

FOR EVERYONE WORKING IN SYSTEM SAFETY

www.scsc.uk/sss

SSS'24

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

SCSC 32nd Annual Symposium

www.scsc.uk

The Safety-Critical Systems Club

32nd Safety-Critical Systems Symposium

13-15th February 2024, in-person in Bristol, UK

Invitation to submit an abstract

The Safety-Critical Systems Symposium in 2024 (SSS'24) will be held in Bristol, UK. This event comprises three days of presented papers, including keynote presentations, invited talks and submitted papers. There will also be a poster session, exhibition and evening banquet.

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

Suggested topics are:

Accident Analysis
Agile Methods
Artificial Intelligence
Argument Notations
Assurance Cases
Autonomous Systems
CAV
Certification
Change and Evolution
Complex Systems
Data Safety
Digital Twins
EMC/EMI
Environmental Safety
Human Factors
Internet of Things
Machine Learning
Methods and Tools
Model-Based Assurance
Modular Assurance
Multicore / Manycore
Ontologies / Formalisms
Regulation of Safety
Resilience
Robotics and Automation
Safety Analyses
Safety Culture
Safety Management
Safety Practice and Process
Services Safety
Software
Standards and Guidance
Systems-of-Systems
Through-Life Safety
Training and Training Data
Uncertainty and Risk
Validation and Verification

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

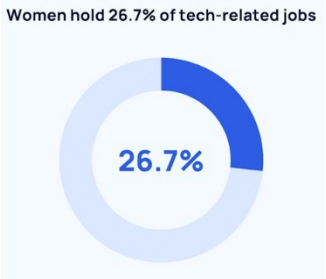
Authors for papers should submit a title and 200-word abstract to **mike.parsons@scsc.uk** by **30th June 2023**. Successful authors will then be asked to submit their paper for inclusion in the proceedings book by **30th October 2023**. Papers will be reviewed, and comments fed back during **November 2023**. Poster authors should submit a title with abstract to **mike.parsons@scsc.uk** by **30th November 2023.**

For **information, exhibition, sponsorship** and **booking** enquiries please contact: **alex.king@scsc.uk.** For technical aspects, abstract and paper submissions, please contact: **mike.parsons@scsc.uk**

Editorial

In 2017, my company was moving into its new prestige headquarters in London and there was a competition to name the new client-facing meeting rooms. I thought women had been poorly represented in the past, so my suggestions were all women.

I am proud to say that, not only is one of the rooms now named after my suggestion: Ada Lovelace (portrait as featured on the front cover), but also that there was a 50/50 split between men and woman chosen by the selection panel. If this was a sign of a new era of equity where everyone shared the same prospects, opportunities and treatment irrespective of gender, then it is certainly welcome but it has been a long time coming and I suspect there is much more work ahead to fully redress the balance – according to a recent survey, women hold just over a quarter of the tech-related jobs and there is a significant gender pay gap; a 2022/2023 sample of 15 of UK companies involved in system safety revealed, on average, women's mean pay is 15% less than men.



To coincide with International Women in Engineering Day on 23rd June 2023, our lead article from Wendy Owen focusses on the female perspective through the stories of 14 of the women currently working in system safety. Through a series of interviews, she asks how they came to be working in system safety, their career highlights and challenges and asks them for some wise words.

I then report the highlights of the 31st Safety-Critical Systems Symposium held in York in February this year. This was the first fully attended event since the Covid pandemic and so it was a very welcome return to the types of event we've enjoyed in the past. We also saw a strong submission of posters this year with 13 posters many of which were on display during the poster session where delegates could talk to group members to find out more about the presented topics. For the first time, all the posters have been included in the newsletter. The posters were intended to be printed in large A0 so apologies if some of the text is small, but if you are reading this in pdf format, you can click on the poster to get a full pdf download of the poster.

I provide highlights of the Future of Testing for Safety Critical Systems seminar held in December 2022. This was a fascinating event with interesting topics in areas such as fuzz testing, automated testing and the challenges of testing of autonomous vehicles.

Mike Parsons reports on the last Tech Trip to the GWR Steam museum. The next Tech Trip will be the National Space Centre in Leicester on Saturday 24th June 2023, which promises to be a fascinating and engaging event with special insights provided by those who have worked on some of the space missions.

Our 60 second interview is with Jane Fenn. Jane has over 30 years' experience in Safety Engineering and Engineering Management, and amongst many roles she is a SCSC Steering Group member and champion of diversity and inclusion.

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



In Brief



Norfolk Southern's Ohio Train Derailment Puts Railroad Equipment Sensors in Spotlight



The derailment of a Norfolk Southern Corp. train in a small Ohio town last month is putting renewed attention on the role of sensors that railroads use in a bid to prevent such accidents.

The railroad, in response, announced new safety initiatives, including adding 200 temperature detectors to parts of its tracks where existing sensors are at least 15 miles apart, starting near the derailment site in East Palestine. *wsj.com*

Air France and Airbus cleared of involuntary manslaughter over 2009 crash



The families of victims of France's worst air disaster said they were devastated after a Paris court cleared Air France and Airbus of manslaughter charges over the 2009 crash that caused the deaths of 228 people.

Giving its verdict on Monday, the court said that if there had been faults committed, "no certain causal link" with the accident had been demonstrated.

David Koubbi, a lawyer for the families of a number of passengers, said the court's ruling was "incomprehensible". *theguardian.com*

Toyota suspends sales of Yaris model in Thailand after safety test problem

Japanese carmaker Toyota Motor Corp has stopped sales and deliveries of its Yaris Ativ in Thailand, senior officials said on Monday, after its affiliate Daihatsu rigged part of the door in side-collision safety tests.

The problem may have occurred due to pressure on Daihatsu to shorten the development time of the Ativ, Masahiko Maeda, Toyota's CEO for the Asia region, said at a press conference in Bangkok. The vehicles customers were currently using were safe, he added. *reuters.com*

FAA System Outage



On 11th January 2023, U.S. flights were grounded or delayed as the Federal Aviation Administration (FAA) attempted to fix a system outage. FAA paused all flight departures until 9 a.m. The outage was the first time since September 11, 2001, that the FAA issued a nationwide ground stop in the United States.

A preliminary investigation of the incident demonstrated to FAA investigators that a "damaged database file" may have caused the outage of the FAA's Notice to Air Missions (NOTAM) system, responsible for notifying pilots of safety hazards. *wikipedia.org*

International Women in Engineering Day



International Women in Engineering Day (INWED) began in the UK in 2014 as a national campaign from the Women's Engineering Society (WES). Since then, it has grown enormously, receiving UNESCO patronage in 2016 and going truly global the following year. INWED promotes the amazing work that women engineers across the globe are doing and gives them a profile when they are still hugely under-represented. As the only platform of its kind, it plays a vital role in encouraging more young women and girls to take up engineering careers.

The Influence of INWED

INWED is International Women in Engineering Day, occurring on 23rd June every year. It is only in its 10th year, was relatively unknown in its early years, nor celebrated in the way it is today.

Safety engineering is still largely a man's world, as with engineering more generally. Yet, there are some women who have been in the field (and associated disciplines such as reliability engineering, human factors and systems engineering) for decades, challenging that status quo, finding their own niche, working on sites and in offices all over the UK and far beyond. They have contributed substantially in highly regulated sectors far and wide and to projects of many types, from small widgets to major infrastructure. In this article, a different perspective is therefore presented – specifically, that of the SCSC women. Here's a snapshot of their stories, in the form of short interviews.

"I would like to be remembered as someone who was not afraid to do what she wanted to do, and as someone who took risks along the way in order to achieve her goals."

Sally Ride

The responses to interviews have been unexpectedly but conveniently themed into those who accidentally fell into safety, those who gravitated towards it, and those who wanted to be involved in it from the outset.

Accidental Careers!



Ireri Ibarra, Global Head of Functional Safety, Dana Incorporated

How did you get into safety?

I was trying to find a research topic for my thesis, then I stumbled upon safety. Safety sounded interesting, at the same time terrifying given how broad the subject is. It turned out to be a great area to make a career in.

"Nothing in life is to be feared, it is only to be understood. Now is the time to understand more, so that we may be fearless"
Marie Curie

What would you highlight in your career to date?

It's difficult to choose a single highlight to date. I feel most fortunate for continuously being challenged to develop myself both technically and personally.

My current role has given me the opportunity to explore how cultural aspects impact organisations. From the early days as an international student; I learned and observed how big, diverse, and interesting our different cultures are. Today I have a global responsibility leading a multi-cultural organisation adapting to change. The result of several acquisitions led to the merging of different companies and their cultures, this in turn, made me take an interest on how people perceive and manage risk. I've had to learn that even if we agree to disagree, as long as the goal is common, we must move together in a positive direction.

Tell us about a current challenge you face?

An organisation with many stakeholders from very different backgrounds, both in their personal and working cultures. Reaching consensus is perceived as a simple task but, it is essential to be able to navigate an array of cultural nuances. Communication plays a big role in establishing a common understanding of the problem at hand; eventually encouraging people to propose or accept potential solutions; instead of dismissing them straight away.

I have gone through the whole cycle of doubting myself, wondering if I'm doing anything right, nearly giving up. In the end if you break your patterns and genuinely think outside of the box; all of these dark clouds become lighter.

Give us some wise words….

Be comfortable outside of your comfort zone, be yourself, ride the wave and enjoy it.



Carmen Carlen, Director of Safety Products, Edge Research (Germany)

How did you get into systems safety?

I had no intention of working as a safety engineer. I even did not know exactly what safety engineering was until I attended a seminar in the final year of my Bachelor studies, where I had to write a report on safety cases. Afterward, fate made it so that at my workplace I had to implement an editor for safety cases. Also, I was sent by my then-employer to the group of Professor Tim Kelly, at the University of York, to learn more about safety cases.

What would you highlight in your career to date?

The highlight of my career so far is that I did some research in the domain of safety case development and maintenance for about 10 years, contributing to the state-of-the-art, and now, while working on projects with industry, I get to transfer my research contributions into practice.

Tell us about a current challenge you face?

I am currently working on the development of trustworthy autonomous systems, scoping at reducing the epistemic and aleatory uncertainty associated with such systems, operating in complex environments.

Give us some wise words …

As safety engineers, we need to be suspicious and consider all worst-case scenarios. Still, we shall keep an open mind and think of solutions for enabling the usage of new technology, for which we still have not specified mature enough safety assurance practices.



Rhiannon Chilton, Software and Systems Dependability Specialist, DSTL/MOD

How did you get into safety?

By complete accident, although it played well to my personality. My early career moves were driven by fixed term contracts and redundancy before I discovered testing, safety, and assurance. Having said that, all of the industries I have worked in have been safety critical or safety related. I have always liked to feel that I am making a positive difference.

What would you highlight in your career to date?

I have been lucky to work on a number of very tangible platforms throughout my career and feel proud to have done so, protecting the various users and other stakeholders. Unfortunately a number of them aren't for open conversation but I love being able to see the output of hard work and (often difficult) decisions. More than once I've been privileged to find my way onto the bridge of a ship and see the navigation system I contributed to in action.

Tell us about a current challenge you face?

Balancing family and professional life is definitely a challenge, learning how to prioritise is a key skill(!), but it is incredibly rewarding to be part of both worlds.

Give us some wise words….

Value your enthusiasm and integrity. Nowhere is perfect all of the time but work takes too much of your life for it to not be fulfilling or for it to compromise your beliefs. The path forward may not be obvious, I never dreamt I'd have worked on most of the things that I have done, but there are so many areas where good people can make a difference.

Catherine Menon, Principal Lecturer, University of Hertfordshire



How did you get into systems safety?

My PhD was in category theory, and following this I moved from Australia to the UK to take up a postdoc at the University of York. Systems safety had been on the periphery of my experience – some of my PhD work touched very briefly on it – but I hadn't dived into it in any detail.

What would you highlight in your career to date?

I've recently begun to move into the intersection of ethics, safety and regulation. I'm pleased to be a member of the BSI committee working on ethics for robotics and autonomous systems. We've recently put out the updated BS 8611 standard which attempts to guide practitioners in this space. I've also been lucky enough to be involved with developing other standards and guidance documentation – not least the guidance produced by our own Safety of Autonomous Systems Working Group! I've also very much enjoyed working as a consultant to the MoD to get some more hands-on experience: the gap between theory of systems safety and how an 18-year-old squaddie "does" systems safety can certainly be eye-opening!

Tell us about a current challenge you face?

I'm currently involved in a number of cross-disciplinary collaborations to consider how safety and ethics interact when it comes to public-facing systems. The major challenge here is the public perception of autonomous systems as "magical" robots with science-fiction capabilities. I think as safety engineers there's a hugely important opportunity for us to speak up here and help educate the public about the risks and benefits provided by these systems.

Give us some wise words….

As safety engineers, one of our roles is to tell "the story of the system". Don't overlook the importance of narrative and argument, especially when it comes to public discourse systems safety is a very nuanced discipline, and the way we discuss systems should reflect that nuance.

Rita Dunne, Principal Consultant, Atkins

How did you get into systems safety?

I didn't consciously choose a career in safety. It chose me. I joined Rolls Royce and Associates (Nuclear) on graduating in Maths and was ushered into a huge room with many other new starters on the first morning, where we waited to be called to our departments. Each person's name was called out followed by the department they were joining. It was a total mystery to me where I would be heading – and where I would fit in to an engineering business with a Maths degree? In hindsight it was odd that I had no idea what department I was going to! Then someone called out my name followed by "Safety!" and I immediately knew this was going to be interesting and worthwhile. And it was.

What would you highlight in your career to date?

A really special time in my career was working for NATS (then our client) on the transition of Air Traffic Control (ATC) operations from the old to new Heathrow ATC Tower. I worked with an amazing group of human factors specialists and Air Traffic Controllers on what felt like the most exciting and innovative engineering/human-centred project in the UK at the time. I learned so much and to be part of a project that had international reach was thrilling.

Tell us about a current challenge you face?

It's a challenge – and saddening – to observe that organisations have such short memories when it comes to safety. Lessons in safety we may think have been learned decades ago are rarely embedded to the degree we may expect or hope. I wonder how the Grenfell disaster could have been allowed to happen when society knows so much about how to identify, eliminate and manage risk effectively. And I wonder what it will take to change our society's approach to safety so such disasters can never happen again.

Give us some wise words....

Working as a safety professional involves asking lots of questions that don't have easy answers and I have experienced the safety team being treated as a hindrance to project progress for that very reason. So my "wise words" are to keep asking those questions, even if the response from others is not comfortable. Your questions may save someone's life.

And apart from that, I rather like our late Queen Elizabeth's wise words "Take the long view".

Gravitational Forces!



Zoe Garstang, Engineer and STEM Ambassador, BAE Systems

How did you get into systems safety?

I wouldn't say it was pre-planned when I first embarked on my career. I joined BAE Systems as an engineering apprentice in 2016, and at the time, I didn't really know where I wanted to specialise. It was only by chance that I was assigned a placement in Airworthiness as part of my apprentice rotation and that started to give me a glimpse to some of the possibilities in system safety. It wasn't until the start of this year that I actually moved into a system safety role on the Flight Control Systems, after spending 3 years in Airworthiness.

"Life is not easy for any of us. But what of that? We must have perseverance and above all confidence in ourselves."

Marie Curie

What would you highlight in your career to date?

One thing I'd highlight in my career so far has been the variety, not least throughout my apprenticeship, but also continuously on a daily basis. Don't get me wrong, there have been lots of changes to adapt to in a short space of time, but in that time, it has also meant that I've gained a broad understanding in different areas and can see how they all interlink or affect one another.

Tell us about a current challenge you face?

I think the biggest challenge for me right now is coming up the steep learning curve in my new role. It's been a big challenge and there's so much to learn but it's one that I'm excited about.

Give us some wise words….

If you're a student or early in your career, where you can, try and give everything that you come across a system safety context or link. Specific system safety modules and topics are hard to come by in general engineering courses and I'd not seen system safety covered in the same depth as other topics within my academic career (BTECs, HNC and HND). I suppose what I'm saying is – get curious about system safety, even if it's not directly related to your role or studies at the moment.



Anusha Chellappah, Senior Safety Engineer, Ebeni

How did you get into systems safety?

During my undergraduate degree, I took a couple of HMI related modules, which I really enjoyed. These modules got me interested in Systems Safety which led me to choose a research Masters focusing on Safety Critical Systems, specifically Traffic Collision Avoidance System (TCAS). Together with my supervisor, I wrote a paper based on the results of my findings and the paper was chosen to be published by the IET. The field interested me and I was determined for my career to be in safety.

Soon after my MSc, I joined Logica's (now CGI) Graduate scheme. I started out as a tester in a Defence project but kept emphasising to my team lead that I wanted to be involved in Systems Safety. I approached the Safety Manager at the time (Mike Parsons!) and requested him to be my Staff Manager so that he could guide me to the right projects. Mike was very supportive and did all he could to get me involved within the safety teams of different projects and that is how I started out!

What would you highlight in your career to date?

I have been lucky enough to have been involved in a few interesting projects but my favourites to date were two projects I worked on in parallel.

I was a part of the Technical Contractor (TSC) team supporting the Office for Nuclear Regulation (ONR) during Generic Design Assessment (GDA) Steps 3 and 4 for the UK HPR1000 (a type of nuclear reactor). This involved me working directly with the ONR inspectors in charge, taking part in Level 4 meetings with the Requesting Party and reviewing documents against International Nuclear Standards. This was the first time I had been involved in the Nuclear domain and I gained a lot of knowledge from my peers and by working closely with the clients.

I also worked as a junior Independent Safety Authority (ISA) on Four Lines Modernisation (4LM). This involved me initiating meetings with London Underground (LU) and Thales, producing Safety Notices to record observations and drafting letters of Support for software commissioning.

I gained an incredible amount of technical knowledge on both these projects.

Tell us about a current challenge you face?

Most of the projects I was a part of had been running for a number of years, which makes it at times difficult to gain exposure to the initial safety activities e.g. being involved in creating Fault Trees. Also, there is a steep learning curve to get familiar with the project in a short period of time, particularly for complex projects.

Give us some wise words….

I was incredibly lucky in terms of the companies I worked for (CGI, Altran Praxis (now Capgemini) and now Ebeni) as I always felt supported as a female engineer and a parent and have always had a good work/life balance. So I would say to any woman, who is looking for a career in engineering to not let the lack of women in engineering or perceived work load put them off and to keep pursuing their passion.

Marea de Koning, TUNI (Finland)

How did you get into systems safety?



I intend to live my life by always moving forward and making choices that allow me to bring meaning to that which is important to me. Originally, I never intended to work in academia, let alone pursue a career related to systems safety and heavy-duty off-road machinery. My journey into systems safety wasn't pre-planned, it appeared as I progressed from my Bachelors in technical computer science from Amsterdam UAS in the Netherlands, to a Masters in Industrial engineering in Aschaffenburg UAS and from there moved forward towards Finland. It was in Finland that the concept of systems safety appeared as I became a PhD researcher in the department of Automation Technology and Mechanical Engineering at the University of Tampere. My journey is proving to be very exciting, one filled with many blessings and revelations as every day I discover and learn new aspects in this world of systems safety.

What would you highlight in your career to date?

One aspect that I would like to highlight is my ongoing appreciation for all the mentors that I have encountered up until now, all of whom have given me guidance, and advice that has proven to be truly fundamental for my personal and professional development. I would like to mention that, whatever journey you find yourself on, do not remain in isolation and try to do everything on your own; instead, reach out and share your knowledge, experiences, and learn from those around you – let it help others as it helped you.

Tell us about a current challenge you face?

I'm still very new to the safety field, but it is my aim to design, develop and integrate inherently safe design measures into the highly-automated heavy-duty off-road machinery that we are developing in close collaboration with several Industry partners. One of the current concerns addressed is the design, integration and validation of the safety-critical software-related parts of a safety function, especially when said function exceeds the scope of existing guidelines e.g. due to the incorporation of data-driven methods.

Give us some wise words …

I would like to share the immortal words of C.P. Cavafy "Keep Ithaka always in your mind. Arriving there is what you're destined for. But don't hurry the journey at all. Better if it lasts for years..."

Louise Harney, Chief Systems Specialist, Leonardo



How did you get into systems safety?

I joined a consultancy called Helios when I left university and they happened to have lots of safety work, which I found incredibly interesting. Managers regularly offered me the opportunity to do other kinds of work, but safety kept pulling me back in as it gave me the big picture. I moved into industry to get more involved in the end-to-end lifecycle of systems, which led me to me joining a new network in the SCSC and I never looked back.

What would you highlight in your career to date?

One of my career highlights has been working on the Tempest programme. For a time, I chaired the safety sub-group bringing together the safety leads of each Tempest partner organisation to facilitate knowledge sharing and ensure that close working relationships were maintained. The opportunity to learn from each other and start the partnership off as we mean to go on was a big highlight for me. It reminded me of the importance of soft skills in addition to technical skills, as workshop facilitation and safety communication are such key parts of being a good safety engineer. As an SCSC Steering Group member, I have found the ability to network and share ideas with peers has been invaluable, and I try to replicate that support in any team.

Tell us about a current challenge you face?

There are so many technical and design challenges, which is what makes working in safety so interesting. My biggest challenge at the moment is adapting to my new life as a working mum, especially in between two periods of maternity leave with our second baby already on the way. I've had to delegate more than ever, both at work and at home, to make the balance work. I have shared more knowledge with others than ever before, to ensure that our team can cover my role until I return, and I have enjoyed rising to the challenge.

Give us some wise words …

You can make an impact with a single conversation, so always be open to finding those opportunities to engage, whether it's with a system designer, a fellow safety professional, or anyone else.

Jenny Butler, Senior Safety Consultant, Ebeni



How did you get into systems safety?

It certainly wasn't pre-planned. My partner was working for a, then, very small company that was pioneering in system safety (this was 1988); formal methods were then being mooted as potentially a big thing, and I was coming to the end of my university degree course in mathematics. I was taken on as a new graduate, and learned about system and software safety as I went along, working with and learning from some very knowledgeable and experienced people along the way.

What would you highlight in your career to date?

I count myself fortunate to have been able, for the better part of 35 years and counting, to do work that I (mostly) enjoy, find interesting and be able to do it well – with the added bonus of great colleagues and clients. Perhaps the most satisfaction is when clients come back for further work!

Tell us about a current challenge you face?

I work part-time and have done for 14 years now. It can be challenging to manage client expectation around that.



Gill Kernick, ARUP

Here is a slightly different take on getting into safety, from Gill Kernick, who presented at the recent SSS on the Grenfell Tower accident.

How did you get into safety?

I don't really think of myself as 'in safety'. I fell into leadership and culture in the space of safety by a winding and unpredictable route. I'm fascinated by the complexity of preventing catastrophic events, where the social aspects such as hearing all voices is as important as the technical aspects.

What would you highlight in your career to date?

I have worked with some incredible teams to make dramatic improvements to safety performance by focussing on the gap between work as prescribed, done and imagined; and creating psychologically safe spaces and connections between executives and the front line to talk freely and safely about these gaps.

Publishing "Catastrophe and Systemic Change: Learning from the Grenfell Tower Fire" is a highlight although it's also, and always will be, the book I wish I'd never had to write.

Mostly, the highlights are memories of beautiful human interactions all over the globe.

Tell us about a current challenge you face?

About a year ago I started working as Transformation Director at Arup University. Learning how to navigate organisational complexity and politics in a large organisation is challenging and interesting. I'm particularly intrigued by how to bring kindness to my interactions and leave people with an experience that they matter even when things are challenging! I believe this is critical to creating a culture where people will speak up and tell you the bad news – something I'm passionate about nurturing.

Give us some wise words….

Particularly to women – don't try and fit the 'mould' – it's a biased model. Challenge the status quo – your perspective is unique, trust it.

The Chosen Path

> **"A ship in port is safe, but that's not what ships are built for."**
> **Grace Hopper**

Anne Seldon, Chief Engineer, Product Safety & Compliance, WAE



How did you get into systems safety?

I've wanted to work in the safety sector since I started studying engineering at university. Originally, I was keen to work in the air accident investigation space but I found my passion was for preventing such accidents from ever occurring in the first place. I was very fortunate to find a role in aviation safety shortly after graduating and I've continued to work in this space for the rest of my career.

What would you highlight in your career to date?

I'd say the career highlight for me was seeing the Boeing 777X take to the sky for its very first flight. I had worked on the safety and reliability case for the electrical systems on the aircraft for the best part of four years. Its complexity and scale challenged me more than anything I'd faced to date and required me to learn quickly and increase my technical knowledge dramatically. Seeing the aircraft's wheels leave the ground was an amazing reminder of why I became an engineer.

Tell us about a current challenge you face?

In the past year I've moved from working in a single industry, aerospace, to working in an organisation which works across multiple sectors. Whilst the principles are the same, the application of them differs from industry which is something I've never had to manage previously. To add to the complexity, I'm helping to design battery systems to decarbonise mining vehicles and they're operating at a power level that is transitioning to high voltage levels within occupied vehicles. There's very little standardisation and best practice to support us in this endeavour so it makes things much more challenging!

Give us some wise words…

Engineering can be a cruel mistress at times, and it will often demand increasingly more of your skill, time, and energy. Ensure you maintain a healthy balance. You can't advocate for the safety of your systems effectively if you're not maintaining your personal wellbeing.

Helen Smith, Lead Safety Engineer, Leonardo



How did you get into system safety?

I spent the early part of my career in the Supportability function, performing reliability predictions, FMECAs (Failure Modes, Effects and Criticality Analysis) and Fault Trees on a variety of complex products. Fault Tree Analysis (FTA) is a type of failure analysis in which an undesired state of a system is examined and I found that my analysis always tended to steer me towards what could go wrong on a system rather than assuming it would operate as designed. I've always had a big interest in accident reports and the ways in which the experts piece together all the evidence to find out what really went wrong, so I chose to use the

Challenger Space Shuttle disaster as my case study when I was interviewed for my Chartered Engineer qualification. After working in Supportability for around 7 years, there was an internal vacancy for a System Safety Engineer and I jumped at the chance to specialise in this area.

Tell us about a current challenge you face?

Part of my current role within Leonardo's Design Integrity function is acting as an Independent Technical Authority for complex, multi-box systems. As our systems become more complex, the traditional methods of proving they are safe become more problematic. As I had no prior involvement in the specific system development, my initial challenge was to review all the safety evidence for the system and sub-systems and form a judgement as to whether the safety requirements were appropriate and the system had attained an acceptable level of safety. A subsequent challenge was when I identified a shortfall in the safety argument or the evidence, as I cannot compromise my independence regarding the advice or feedback I provide to the project team.

What would you highlight in your career to date?

I would say that the main highlight of my career to date actually forms one of the core parts of my current role, where I have been given the delegated authority to sign the UK and EU Declarations of Conformity for our products that require the UKCA (UK Conformity Assessment) and/or CE (European Conformity) marking. It's just one part of my role that I take very seriously, as I'm taking the full responsibility for the product's compliance with the applicable UK/EU Laws. Prior to this, I received training on the legislation and underwent a competency assessment, so being given this delegated authority shows the confidence that Leonardo has in my knowledge and ability.

Give us some wise words…

Start each morning with a positive thought, and it can change your whole day!

As for me? Maybe one day I'll write an autobiography, but this'll do for now…



How did you get into systems safety?

I'm a case where it was probably inevitable. I've been doing safety since day one of my career, but the origins go further back. I was born the same week as the Aberfan disaster and my brother passed away on a June 23rd in the 1960s of hydrocephalus, shortly before safe shunts became available – INWED has thus become a welcome event in my life. The Chernobyl accident (and various other industry accidents) happened during my physics degree, so with a view to stopping anything like it happening again, my career began in the nuclear sector at UKAEA. I started as a safety analyst on Sizewell B, then on the UK's first civil SMR project (SIR, Safe Integral Reactor), followed by the UK's first computer-based nuclear plant trip system (for Dungeness B). The latter was where I really got into systems and functional safety, at a time when software reliability was in its infancy. I was trained by renowned experts in the Safety & Reliability Directorate (SRD), then part of UKAEA, and in 1992 was relocated to SRD to work on submarines. The rest is history.

What would you highlight in your career to date?

Top of the list is when I was elected a FSaRS. At the time I was only the 4th woman in 40 years to become one; and was shortly followed by a few others.

Of course, next on the list is being a co-author of SCSC's book "30 Years of Safer Systems"!

I would also highlight

- early on in my career, setting up a new regional office that became very successful
- starting a new team from scratch and getting us to £2.5m turnover within 2 years
- setting up global communities of practice in two companies
- the sheer number of projects and bids I have worked on in various sectors, including some fairly novel projects (not all of which came to fruition!)
- working all over the UK, also in Lithuania, France and Australia, and remotely in various other countries
- being a founder member of a LinkedIn group for Women in SET that now has ~18,000 members

Tell us about a current challenge you face?

My favourite challenges in industry have tended to involve "projects in distress", including ones where a regulator has refused an application for operations – sometimes there's nothing quite like a challenge being brought in after the event and sorting out scores of corrective actions!

Recently, it was a career diversion, leaving industry and spending a couple of years in a university research post in fusion. I had previously been a reviewer for the RAMI (reliability, availability, maintainability, inspectability) work on ITER's I&C (Instrumentation and Control) systems, but this was more safety focused. It well-utilised all my previous industry experience from various sectors.

At time of writing my current challenge is simply getting a job. Despite calls to arms for over-50s and women engineers in leadership positions, I've found it very hard to get a job if you're disabled, need to work part-time and/or can't travel. This is despite the fact when I was working full time in industry I was often working on several projects and bids in parallel, and remotely and internationally. Going the freelance/associate route seems to be the only way to deal with the situation. Watch this space?!

Give us some wise words ...

Always have a Plan B. Being a safety engineer is a reasonably secure livelihood, but don't assume you'll never be made redundant, get ill/incapacitated, or have some other work or life hazard thrown your way!

Don't be afraid to do the right thing. Don't put up with discrimination or unacceptable behaviour. Whistleblow on conflicts of interest. Don't let people put you down or push you around. Be prepared to walk away or go to court. Make things better for those following in your footsteps.

Remember to look up at the stars and not down at your feet (Stephen Hawking).

Final Words

> **"Your best and wisest refuge from all troubles is in your science"**
> **Ada Lovelace**

If you wish to know more about how women in systems safety work and can add value to teams, projects and company culture, invite them into a meeting, put their CV into a bid, give them a platform at a conference or on a panel, put them on a high-profile project, propose them for a board. Give them a place at the table, give them an opportunity, give them half a chance, let them be at their best, and they will often reward your team/company (and your company's finance department) ten times over – oh, and when they do, please ensure that they are appropriately compensated for their efforts and expertise.

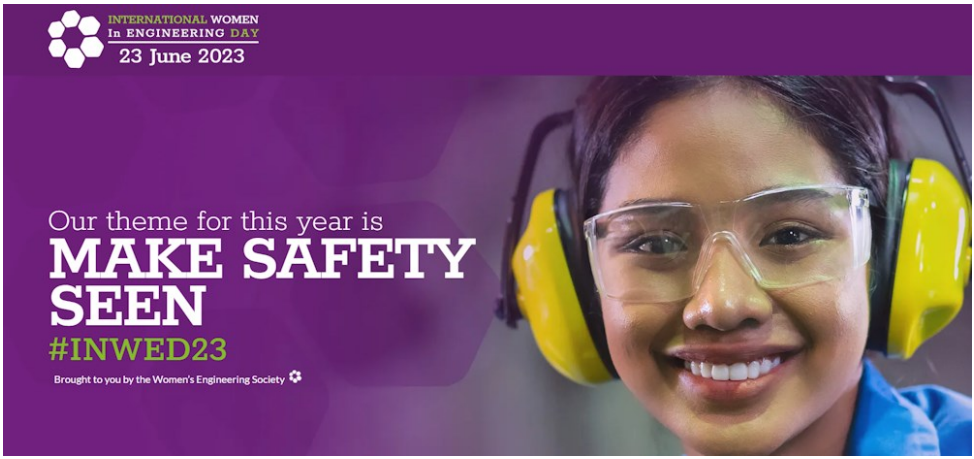
Well, we hope you have enjoyed reading this article for INWED. This article is dedicated to all the women engineers working in safety, their allies in the workplace, and their supporters behind the scenes. Also, Women in Science and Engineering (WISE) and WES.

See you on Ada Lovelace Day, for a special historic edition of women engineers in safety. In the meantime, take a tip from the Safety & Reliability Directorate's old motto – leave nothing to chance!

Wendy Owen

Wendy has nearly 35 years' experience in systems assurance across a wide range of highly regulated industries covering energy, defence, transport and process sectors. Her career has largely been in engineering consultancy, also with time in manufacturing and regulatory. She is a Fellow of WES and the Safety & Reliability Society.

The author retains copyright of this article.



Upcoming Tech Trip: Visit to the National Space Centre



The next Tech Trip will be to the National Space Centre, Leicester, UK on **Saturday 24th June 2023.**

https://spacecentre.co.uk/

This has some great exhibits and a large planetarium.

Cost is £14.95 per person, (the Jupiter Mission package) which includes a 30-minute planetarium show.

Arrival time is 1pm, the planetarium show is at 3:50pm.

The event is open to everyone – so all friends and family members are welcome!

SSS'23 Event Report



In February 2023, the Safety-Critical Systems Club's annual Symposium returned to a fully in-person event hosted at the Principal Hotel in York. With over 100 attendees, the event enjoyed the type of attendance not seen since pre-Covid years and hosted over three days, the event once again, provided an exceptional and diverse range of talks. Paul Hampton, SCSC Newsletter Editor, provides highlights of the event.

While Covid has not entirely disappeared, there was a definite feel this year that we had returned to the type of event we'd enjoyed in the past, with the high attendance giving the event a real buzz and with lots of new features such as "Room 101", the crossword and roving video interviews, the event was one of the best we've seen in my memory. The talks were also of the highest quality covering many of the pressing challenges we have in the industry today. The keynote speeches are summarised below.

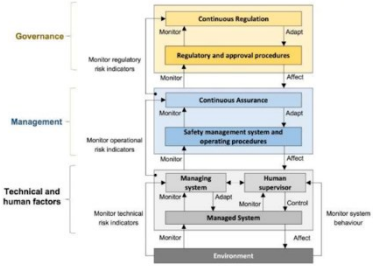
Safe, Ethical and Sustainable: Framing the Argument

Professor John McDermid, Director of Assuring Autonomy International Programme at the University of York, opened the conference with a talk developing some of the ideas he'd presented at the previous year's symposium where he introduced the mantra of "Safe, Ethical and Sustainable", and aimed to link three strands of thought:

- Ideas on how to govern safety of complex systems and their emergent properties
- How to develop an ethics assurance argument drawing on tenets of biomedical ethics
- The mantra – that broadens safety considerations to include society and environmental impacts

Governing Safety

John first covered the governance of safety and introduced a model showing a hierarchy of three layers. Technical and human factors at the bottom covering day to day safety management, a management layer looking at the owning organisation & supply chain and then the governance at the regulator level. There are feedback loop aspects with continual iterations but John stressed the process needs to operate a lot faster to manage the complexity and emergent technology.



Safe, Ethical and Sustainable

While the ambition of the mantra is clear, John said that there are challenges in how one actually frames an argument balancing these three quite diverse areas, as there will be trade-offs required between them.

John first covered ethics with an illustration of the type of assurance case drawn from biomedical disciplines. In this argument, along with standard non-maleficence concerns, beneficence and human autonomy also need to be balanced to give an overall "Justice Assurance" argument.

John then covered the sustainability aspect by describing associated models such as the UN Sustainable Development Goals (SDG), which describes 17 "goals" although he noted they are really a mix of different things. He also introduced the concept of "Doughnut Economics" that show a middle area that is sustainable, with poverty in the middle and overconsumption on the outside. There are other versions that enumerate specific concerns. These models help identify and inform the range of concerns that have to be considered – there will be trade-offs, but the aim is to remain in the green band.





John also mentioned a worrying aside where he noted that although electric vehicles are good for the environment at point of use, they have a bigger carbon impact than conventional vehicles in their construction and require the use of metal and rare earth metals that have limited supply.

An illustration

John illustrated framing such an argument through an example where a local authority was considering replacing a fleet of 45 city buses with autonomous vehicles. John showed that the choice of vehicle had different impacts on the environment and utility to different types

of travellers. For example, large buses can carry more people but have poorer safety performance against smaller vehicles because of their mass, shape and risk to vulnerable road users. From a different perspective, smaller vehicles are good and efficient for lone travellers but not good for larger families possibly with additional equipment such as buggies for small children.

John concluded that:

- The work is illustrative and not put in practice yet, but other work such as Rawls reflective equilibrium could be used to help make the justice argument
- There are many ethical principles. The biomedical principles seem to be appropriate as it spans most of the concerns but needs interpretation for a particular context
- For sustainability models, the SDGs are quite different and have surprising omissions such as "human autonomy"
- John said that no one can be expert in all concerns and multi-disciplinary teams are essential. The role of the safety engineer is changing to be more of a facilitator as well as an expert in hazard and risk analysis

Rising to the Challenge of Certifying Automated Vehicles

Jamie McFadden presented the second keynote talk of the day. Jamie is from the Vehicle Certification Agency (VCA), which is responsible for the oversight of vehicle type certification for use on UK roads.

Jamie said that the fullscale deployment of autonomous vehicles is a challenge, but the first steps have already been taken with, for example, the introduction of the Mercedes "Drive Pilot" in 2021 of automatic lane keeping on certain sections of autobahn in 13,000km of pre-approved German motorway.

Jamie said that the type approval process comprises:

- Around 70 tests covering emissions, crash, lighting and tyres
- Conformity of production: can the vehicle manufacturer maintain the type certification approval in full production

Jamie talked through some of the key safety and security aspects and noted that functional safety is part of the type certification approval process.

Two case studies were described that galvanised the views of regulators on the effectiveness of type approval:

- In Sep 2015, Volkswagen were found to have installed software on vehicles that could detect that they were being tested for emissions and allow non-compliant vehicles to pass the test. This impacted 11m vehicles worldwide, and was known as "Dieselgate".

This called into question the regulatory approval practices and resulted in revisions to the regulatory framework brought into force in 2018.

- Researchers exploited a security vulnerability in an internet connected infotainment system to remotely brake and steer a moving Jeep vehicle. 1.4m vehicles were affected and this is known as the "Jeephack" and was a wakeup call for the industry to the risks of connection to vehicles.

This has resulted in improvements in industry working practices and standards and increased security of software and the need to keep software up-to-date.

In 2015, the need for a new set of technical regulations was identified by the UN economic community for Europe and culminated in three new regulations in 2021: UNEC 155 (cyber security), UNEC 156 (software updating) and UNEC 157 (automated lane keeping systems).

Jamie then summarised the regulatory requirements:

- The system shall be free from unreasonable risk for the occupants and other road users

Jamie broke this down into:

- Monitor the design domain environment and driver
- Execute longitudinal and lateral control
- Monitor for failures and degraded operational conditions

This shows the more open and objective-based approach to achieve approval rather than the historical test-based approach.

- The system shall not cause any collisions that are reasonably foreseeable and preventable

Guidance is provided in the regulation to cover the types of issue to be addressed, as a starting point, such as road users and objects blocking the lane, vehicles cutting in and the reveal of objects when vehicle peel away.

- Activated systems shall comply with traffic rules including responding to emergency and enforcement vehicles

There are no explicit list of scenarios to comply against. Regulators want to see a robust assessment process that manufacturers have performed to understand and characterise the traffic rules the system needs to be developed against, the implementation of that system in the design and how these are maintained as rules change.

These might need to consider aspects such as Smart Motorways, a wide range of enforcement vehicles (not just police) and filtering motorcycles etc.

There is a need for collaboration between organisations as no one organisation can know all traffic rules for all markets of Europe.

- The manufacturer shall demonstrate their Cyber Security Management System across the vehicle's lifecycle

Approval also needs cyber security approval and the need for a Cyber Security Management System for Development, Production and Post-production phases. Focus not only on the security of the vehicle but how the manufacturer has gone about securing the vehicle over the lifecycle of the vehicle.

- The manufacturer shall identify critical elements and shall identify risk appropriately

This involves the assessments of the manufacturer's risk assessment process and evidence.

The Automated and Electric Vehicle Act of 2018 that states that the Secretary of State must prepare a list of vehicles that can safely drive themselves. Critical to this will be the monitoring and control test:

Can the system safely control the vehicle.

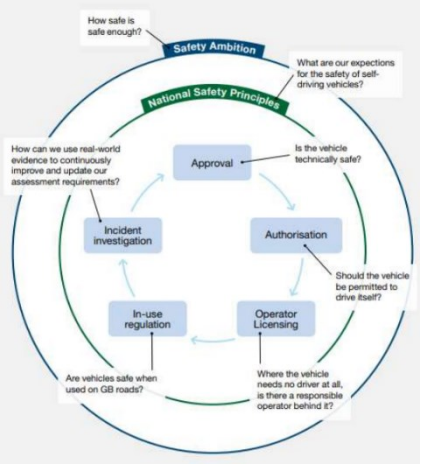
Can it be shown the vehicle can act without a human monitoring it:

- comply with traffic rules
- avoid collisions that a human can, treat others with reasonable consideration
- avoid putting itself in a position where it can cause a collision
- recognise when it is leaving its operational design domain

Jamie concluded by saying there are two significant challenges as they are not truly addressed by the regulation.

- Safety assurance of machine learnt systems bias, interpretability of results and robustness of decision making
- Appropriate use of modelling and simulation

The UK government published its "Connected and Automated Mobility 2025" document and expects that self-driving vehicles should be held to equivalent standard of behaviour as a human driver: competent and careful. There is currently a consultation that will result in a set of national safety principles and a safety framework.



Jamie said that regulators are aiming to address these challenges through:

- Objective based requirements for system safety, machine learning and modelling and simulation
- A foundation of management systems to establish confidence in the system development, production and deployment
- Application of risk assessment to appropriately treat risk
- A new legal framework as an enabler

What the First 100 Years of Railways Can Teach Us …

Tom Anderson presented the last keynote speech of the day with possibly the longest titled talk ever! "*What the First 100 Years of Railways Can Teach Us about the first 10 years of self-driving road vehicles".* Tom discussed what lessons can be learned from previous railway accidents and how these can be read across into the emerging autonomous automotive vehicle industry. Tom referred to various books such as "Red for Danger" by LTC Rolt, which provides a history of British railways disasters and from these, 15 accidents were selected to:

- Understand why the accidents occurred, what the consequences were and what lessons could be learned for today's systems
- Emphasise particular key issues for autonomous automotive vehicles.

Tom discussed 3 accidents:

Parkside (1830) This covered one of the first ever fatalities on a railway when a number of VIPs were being transported during the opening of a line for the Liverpool & Manchester Railway. When the train stopped to take on water, many passengers disembarked and walked onto the track of an oncoming train. One individual, William Huskisson, an MP and former member of the Cabinet, failed to clear the track in time and was hit and mortally wounded by the train. Tom said that one of the key lessons learnt from this accident was that people don't expect new hazards from new technologies, some may ignore safety practices and reduced mobility of a system user can cause additional issues.

Winchburgh (1862) In this accident, maintenance work required single track operations and a train was being used as a pilot engine acting as a token. This pilot engine would normally be a smaller distinct vehicle but had been swapped with a larger engine as the smaller pilot engine had other duties at the time. A ballast train was then mistaken for the pilot engine and was let through to collide with another train. Lessons from this accident where:

- Safety procedures must be understood and followed correctly
- Maintenance situations offer different environments (eg. single track working) that need equal consideration to the norm. Autonomous vehicles will also need to adapt to maintenance situations.

Quintinshill (1915) The Quintinshill signal box controlled two passing loops, one on each side of the double-track. At the time of the accident, both passing loops were occupied with goods trains, and a northbound local passenger train was standing on the southbound main line.

Neglect of the rules by two signalmen, such as failure to apply locking collars, led to the presence of the local passenger train that had been reversed onto the southbound line was overlooked by the signalmen. A southbound troop train was cleared for passage and collided with the stationary train. A minute later the wreckage was struck by a northbound sleeping car express train travelling north. Over 200 people were killed in the accident.

Tom said, lessons from this accident were:

- Accidents arise from multiple causes and failure to adhere to safety practices
- If an AV sees an accident, it could report this to reduce the risk of further accidents

Tom concluded by saying that there were 75 individual items that could be read across into the autonomous automotive industry and recommends that an independent body is required to investigate AV accidents.

Room 101

Roger Rivett hosted a new event called 'Room 101' for System Safety: What would you get rid of? This mirrored the popular UK TV show of the same name where individuals are invited to discuss their pet hates and provides an argument for why they should be 'put in the bin'. The audience then votes on whether the particular gripe should indeed be disposed of. This was an entertaining session with a number of items agree by consensus to be consigned to the dust bin!

Working Group Meetups

Day two started with an early morning get together of working group members. This included a demonstration in the main hall of the "RADISH" tool for helping to manage data safety risks. More details of the RADISH tool are given in the Feb 2023 edition of the newsletter scsc.uk/scsc-182

Special Events

The morning then continued with a number of special events:

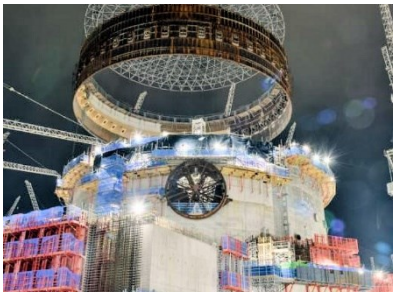
- Visit to the Institute of Safe Autonomy
- Guided City Walk
- York Minster Tour
- York Railway Museum

These were hugely popular with an additional trip to the Railway Museum being organised to accommodate everyone.



How Nuclear New Builds Incorporate Lessons Learnt

The second day's keynote was given by Tom Hughes from EDF discussing the Hinkley C new nuclear power station that is being built in Somerset. The focus of the talk was how the build was incorporating lessons learnt from other accidents and incidents in the nuclear industry.



Tom first described the Hinkley Point Power Station that will produce 3260MW of electrical output from the world's largest turbine generators and account for 7% of the UK's electricity.

Tom described the main characteristics of nuclear plants – the "3 C's"

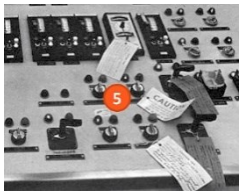
- Control: the rate at which stored energy is released needs to be controlled
- Cooling: even when the reaction is shutdown the fuel continues to produce decay heat so needs to be cooled
- Containment: by-products are radioactive so need to be contained to protect personnel, the public and the environment

Tom gave three specific examples to illustrate the application of lessons learnt:

Three Mile Island (TMI)

On 28th March 1979, a cooling malfunction caused part of the TMI-2 reactor core to melt – the reactor was destroyed.

Tom explained how a mixture of operator and latent errors in the system conspired to cause the accident. The lessons learnt included:



- **Being intolerant to defects & poor quality**. Issues that seem inconsequential now could later compromise layers of the 'defence-in-depth' model
- **Performing work to the highest standards** and in accordance with the approved designs / instructions / procedures – whilst maintaining a questioning attitude
- **Embracing learning** (internal and external) – review relevant Operational experience and close actions meaningfully, ensure training programmes equip personnel for all situations (combination of skills and knowledge)

Chernobyl (1986)

The accident occurred as a result of a failed safety test. Operators mistakenly (and somewhat unknowingly) placed the reactor into a highly unstable state. However, the reactor design was fundamentally flawed. Several factors led to a huge power surge that destroyed the reactor core and released a radioactive plume. Causes were both human and technical in nature.



Tom noted that there are significant design differences in cooling and containment between the Chernobyl RBMK system and Hinkley Point C (HPC), making HPC much safer. The key lessons learnt were:

- **Culture**: Whilst the HPC environment is very different, cultural failings that played a huge part at Chernobyl (Time Pressures, Cost Pressures, Management Blindness and (lack of) Questioning Attitude) could affect any plant, anywhere

Fukushima Dai-Ichi (2011)

In 2011, the Fukushima Dai-Ichi (a 6-Unit Boiling Water Reactor (BWR) power plant) was struck by a magnitude 9.0 earthquake (larger than the plant was designed for). Units shut down automatically (as expected) and shutdown cooling systems started. However, the subsequent tsunami overwhelmed sea defences and flooded numerous sensitive plant areas. Electrical supplies were completely lost, resulting in loss of cooling to nuclear fuel and core damage.



Although the UK EPR system already had design improvements from the older-generation reactors at Fukushima, following the accident, a number of additional modifications were made to the UK EPR design including:

- **Seismically protected water storage building** with additional diesel driven pump capability
- **Increased runtime** of all diesel generators and severe accident batteries
- **New plant configurations** that ensure provision of cooling water to the reactor and spent fuel pool at all times.

Tom concluded with some key points:

- It is nearly always better to 'engineer out' the hazard or error potential than rely on individuals to follow complex safe systems of work perfectly
- People must be trained to work to the highest standards and in accordance with the approved designs / instructions / procedures – whilst maintaining a questioning attitude
- Accepting poor conditions or poor behaviours makes these the 'norm'
- Operational Experience is of huge value – review relevant experience, conduct investigations, set good actions and close them properly
- Make safety & quality personal – never work on the assumption that another 'layer' of the defence-in-depth model will catch an error. What seemed trivial today could cause a problem tomorrow

Poster Session



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

See page 33 for more details of the poster sessions and for copies of the posters as presented.

Banquet

The day concluded with the symposium's banquet and Les Hatton from Oakwood Computing gave an amusing after dinner speech.



Making the Water Visible: A methodology for exploring Systemic Change

A fish is swimming along one day when another fish comes along and says: "Hey, how's the water?" The first fish stares blankly at the second fish and then says, "What's water?"

Kania J, Kramer M, Senge P, 2018, The Waters of Systems Change, FSG

Gill Kernick, Transformation Director at ARUP University, gave a moving account of how she witnessed first-hand the Grenfell Tower fire of 2017. At the time of the fire, she was living in an adjacent block and having previously lived on the 21st in Grenfell Tower, she knew several people, some children, who died that night. In response to the fire, Gill was committed to ensuring an event of this nature never happened again. She thought the desire to improve would be shared, but found this to be far from the case, and this led her to ask why this failure to learn makes sense.

The Grenfell Tower Inquiry concluded that:

"... each and every one of the risks which eventuated at Grenfell Tower, on that night, were well known by many and ought to have been known by all who had any part to play. As a result, you will be able to conclude with confidence that each and every one of the deaths that occurred in Grenfell Tower on 14 June 2017 was avoidable."

Gill said the heart of the matter was a failure to understand the nature of complexity and a piecemeal versus systemic approach to change.

Complexity: many of the traditional top-down bureaucratic and mechanistic ways of thinking are grounded in mythical cause-and-effective narratives and are becoming redundant – and yet, responses to disasters largely come from this paradigm.

Piecemeal v Systemic Change: Gill provided a comparison between these two different approaches to change:

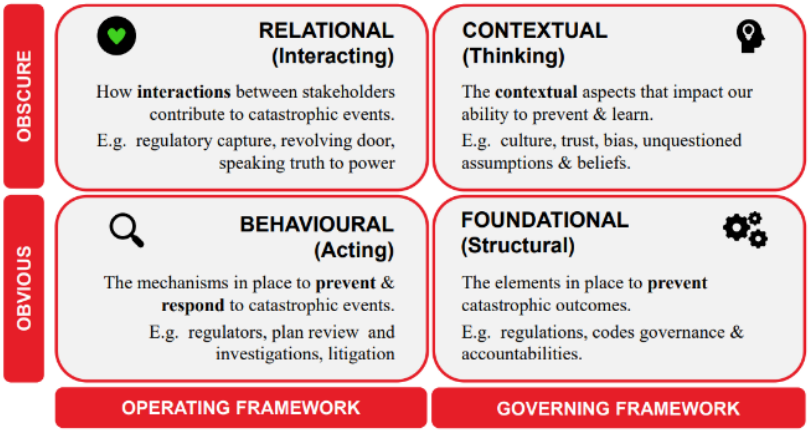
	Piecemeal Change	Systemic Change
Intent	Solving a piecemeal issue	Shifting the conditions holding the status quo in place
Question	What's wrong with a discrete part of the system?	What is the system perfectly designed for?
Assumption	Controllable, predictable world	Complex, emergent world
Access to change	Fix what is wrong	Make the Water Visible: grapple with the messy kaleidoscope
Approach to change	Technical Solutions *(if I do x, y will happen)*	Disrupting the status quo, experimenting *(if I do y, what will happen?)*
Leadership Style	Bureaucratic, command and control, rules based	Organic, emergent, values and principles based
Requires	Traditional Expertise	All Stakeholders - tacit expertise *(validating different ways of knowing)*

Gill used the analogy of the conversation between the two fish presented earlier to demonstrate the desire to "make the water visible" and set out the following principles:

- Traditional bureaucratic, linear, cause and effect ways of thinking and leading are ineffective
- Piecemeal solutions don't cause systemic change and can have unintended consequences
- The system is functioning perfectly to produce what it is producing
- Systemic change requires disrupting the status quo

Gill then set out an approach and framework for exploring systemic change. The approach is grounded in "Enquiry" as distinct from a more formal Inquiry, inhabiting the space of the not knowing, and "Sense-making", distinct from analysis, interpretation or exploration and not demanding neutrality. The key enquiries being:

- Why does our failure to learn make sense?
- What will it take to enable systemic change?



Gill presented the supporting framework against which the following questions can be posed:

- What are the known issues?
- What myths are contributing to our inability to learn?
- What are the conditions holding our inability to learn in place?
- How might we enable systemic change?

Gill concluded by discussing the transformative power of grief and the hope offered through the democratising of change where ordinary individuals are more empowered to effect change through purposefulness and connectedness with one another.

The Language of Risk and the Risks of Language

A pre-recorded talk from Catherine Menon from the University of Hertfordshire was then shown. Catherine said she works with assistive robotics and ethically-informed safety cases, but is also a published author. Catherine showed the different perspectives of risk language drawing out the differences between the language used in formal safety argumentation and the more common layperson's perception of the language. For example, a lay person has a very different understanding of what an "argument" is from a safety engineer.

She said we need to understand how our use of language will be perceived to our readership and the dangers of using metaphors.

She gave an example of the Byzantine General problem where a number of generals need to coordinate a decision to attack a city or retreat with the knowledge that one general may be a traitor and deliberately give false instructions.

Catherine discussed the results of a study where members of the public (a group of actors) where asked what was important about the Byzantine General problem. For safety engineers, "consensus" was important but for the actors it was that the "generals want to attack" showing quite different perceptions of the problem.

Catherine said while metaphor is the main mechanism through which we comprehend abstract concepts and perform abstract reasoning, our language choice can govern our thinking. For example, using the expression "**facing** significant risk", presents risk as an adversary. Safety arguments can also be presented in different ways depending on the language – it can be adversarial or more a form of partnership with the reader.

Catherine concluded with the idea of skilful storytelling with examples of how even a six-word story can have connotations:

"For sale: baby shoes. Never worn."

She warned that it is possible to be too convincing and that word choice, argument structure and explanation of context are important and asked how we assess the risk associated with ourselves.

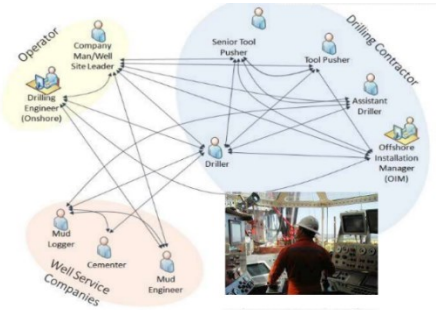
Resilience in Safety Critical Systems – Offshore FRAM

David Slater from Cardiff University starting off his talk by discussing what we mean by "safety" and argued that nothing is absolutely "safe" as freedom from accidents cannot be guaranteed. He suggested that (as proposed by Erik Hollnagel) we should stop using the word "safety" and start using the word "safely".

Accepting that a system cannot be entirely free from risk, David said that the natural response is defensive – to put up "barriers" in depth so that a number of natural or designed defences need to fail before there is an accident. He noted however, that these can be subject to common cause failures with barriers failing as a group or one failure triggering the pulling down of others like dominoes.



David then focussed on the Macondo Blowout (aka Deepwater Horizon explosion) of April 2010, where an offshore drilling rig experienced a blowout from a drilling well that led to a fire, many fatalities and loss of the platform. He first described the sequence of events that led to the accident and showed that all the barriers somehow failed on demand. He said that traditional forms of analysis such as Bow Tie that assume sequential and entirely independent failures can give quantitative failure probabilities on demand that are extremely low suggesting an accident is all but impossible, but an accident occurred nevertheless.



David explored the reasons for this by making the distinction between "Work as Imagined" and "Work as Done". David noted that the operators had all the information they needed to tell them something was wrong but they rationalised it and assumed they could "normally" work around abnormal indications.

David modelled the "Work as Done" that illustrated the complexity of the interactions between the various organisations such as the Operator, Drilling Contractor and Well Service Companies.

He observed that:

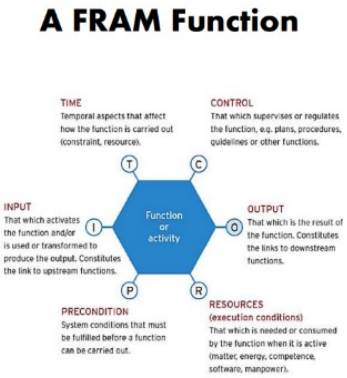
- The interaction complexities would be difficult to model using Fault Trees
- The ownership of particular barriers is unclear
- Is the Driller really in charge/control of all the Key Variables?

And he asked how all the critical interdependencies can be shown/traced.

David said we need to move forward to establish a new paradigm in thinking from "Determinism" to coping with uncertainty and to:

- Operate in the real world, not an idealised, standardised environment
- Move away from expecting linear, predetermined, prejudiced, sequential, "as designed" outputs and behaviours
- Live with Nonlinear, interdependent, unexpected, as necessary, emergent outputs and behaviours
- Establish better models to support the safety engineer aspects

David then looked at what modelling tools might be more suitable to support this new way of thinking. He referred to Leveson's System Theoretic Accident Model (STAMP) and said it was a conventional, (hard wired) "control" diagram of the system. He then detailed Hollnagel's proposal that envisages a system as a collection of interacting, interdependent "Functions" (The Functional Resonance Analysis Method - FRAM) and gave an example of the model from a medical Trauma team.



He said the FRAM method allows you to build a model of an actual complex sociotechnical system and then showed a FRAM model of the Macondo case showing the instantiation for the procedure being operated.

He noted that:

- System behaviours "emerge", they are not predetermined
- The supply of services is a crucial aspect of almost every "safety" function

David's assessment of the case study listed several proposed contributing factors:

- There was no single, simple "Root Cause", component failure
- The system was too complex (pushing the boundaries: record water depth, etc.)
- BP was not directly in control due to a culture of contracting out risks
- The "services", equipment suppliers and maintenance activities that the drillers relied on, were "variable" in quality
- Perhaps complacency assured the drillers that normally, all these minor variabilities could be worked around

He said that when all these normal variabilities "resonated", the system became unmanageable.

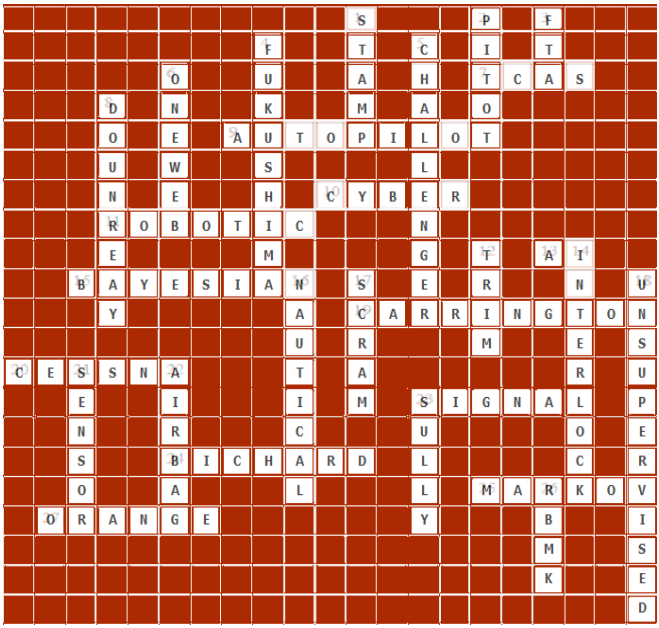
David finally introduced the idea of "resilient" safety-critical systems where behaviours are more predictive rather than reactive, that is, not so much monitoring and responding, but learning and anticipating. He said that to be more responsibly resilient we need to develop proactive design approaches and tools and offered FRAM as a possible solution.

Crossword Competition

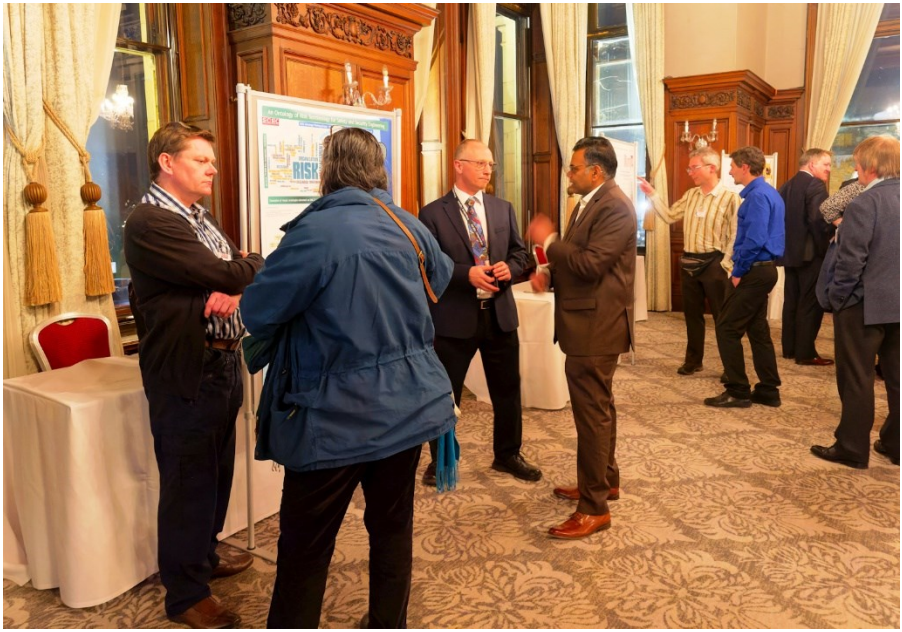
The SCSC Safety System crossword was first published in the Oct 2022 edition of the newsletter and was also given to delegates to complete during the symposium. There were 5 correct entries, and the winner was drawn from the 'hat' by arguably the SCSC's youngest member – Charisse Lin (aged 7), who also produced the remarkable piece of artwork on the back of this edition of the newsletter!



The answers to the crossword are given below.



SSS'23 POSTER SESSIONS



As mentioned in the SSS'23 Symposium Report, the second day's talks concluded with a poster session where delegates were able to see a visual snapshot summarising the work and developments of particular groups such as the SCSC Working Groups. Each poster was attended by representatives from the group, who were happy to discuss the work with delegates in more detail.

Each poster is reproduced in the following pages for reference and a full pdf version of the poster can be seen by clicking on each image. The posters are:

- Anticipating Accidents through Reasoned Simulation (Craig Innes – University of Edinburgh, Andrew Ireland, Yuhui Lin – Heriot-Watt University)
- An Overview of IEEE Std 1848-2020: Standard for Techniques and Measurement to Manage Functional Safety and Other Risks with Regards to Electromagnetic Disturbances (Davy Pissoort - KU Leuven, Keith Armstrong – Cherryclough)
- Engineering safety-critical systems with open-source software (Paul Albertella – CodeThink)
- Build, monitor, and measure your live safety case in nLoop (Carmen Carlan - Edge Case Research)
- SCSC Working Group developments: Data Safety Initiative, Multi-Core, Systems Approach to Safety of the Environment, Service Assurance, Safety Culture, Security Informed Safety, Safety of Autonomous Systems, Ontology and Assurance Cases.

Anticipating Accidents through Reasoned Simulation

Craig Innes[1], Andrew Ireland[2], Yuhui Lin[2] and Subramanian Ramamoorthy[1]

[1]School of Informatics, University of Edinburgh
[2]School of Mathematical and Computer Sciences, Heriot-Watt University

Overview:

- System-Theoretic Process Analysis (STPA) [4] extends traditional hazard analysis techniques to include a range of causal factors that can affect system safety.
- A key goal of STPA is the identification of causal factors that give rise to unsafe control actions, which in turn could lead to hazards and ultimately an accident, i.e. a *loss scenario*.
- Building upon the benefits of STPA, our aim to provided mechanized support to assist engineers in identifying potential loss scenarios.

Ultimately, engineers must be responsible for any safety related decisions. What we are proposing is an approach that assists engineers by providing them with simulated scenarios to review that are realistic and accessible.

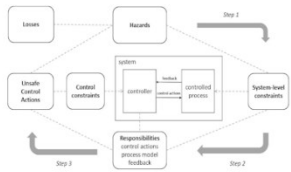
Proposed approach:

- STPA is relatively informal in comparison to formal modelling. To bridge between the *informal* and the *formal* we use the notion of a problem frame [3]. Specifically we use the notion of a problem as a substitute for the STPA notion of a *control structure*.
- In terms of formal logic, the problem frames approach is relatively agnostic. Our case study is quite simple, so we opt for classical propositional logic - specifically we use *Extended Logic Programs* (ELP) [2]. ELP extends the normal notion of a Logic Program (LP), such as Prolog, with explicit negation (-). Similar to LP, a program in ELP is a collection of clauses in the following format:

$$L \mathrel{:-} A_1, \ldots A_n, B_1, \ldots B_n.$$

  while it allows literals in the body, e.g. A_i and B_i to be negated, e.g. $\neg A_i$ and $\neg B_i$.
- Formal modelling is suited to relatively abstract models where the state space is small and can be exhaustively explored. In contrast, simulation allows one to selectively explore large state spaces. In terms of simulations, we have used Car Learning to Act (**CARLA**) [1], which is a simulation platform for testing the performance of automated vehicle systems.

System-Theoretic Process Analysis (STPA)



The diagram above shows the first 3 steps of the STPA hazard analysis process – from the definition of losses and hazards through to defining control actions and identifying how unsafe control actions can lead to hazards.

A Motivating Example

We use an automatic car door locking example to illustrate our proposed approach. Specifically, we consider the design of a Door Lock Control Unit (DLCU) that is required to ensure the locking and unlocking of doors occurs at the right time, i.e. locked when the car is moving and unlocked while stationary. A fundamental design assumption will be that when the car is moving the wheels will be turning. From the perspective of STPA, the controlled process involves the locking mechanism for the car's doors and the car's wheel sensors. The DLCU receives feedback in the form of *wheel-pulse* signals from the sensors when the wheels are turning. In terms of control, the DLCU will be able to send *lockDoors* and *unlockDoors* signals to the doors.



STPA Perspective (Steps 1-3)

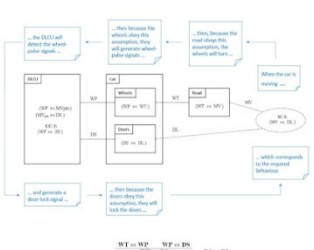
Losses: L-1: loss of life or injury.
Hazards:
H-1: a passenger opens their door while the car is moving.
H-2: a passenger is unable to open their door while the car is not moving.

System-level Constraints:
SC-1: if the car is moving then the doors must be locked (MV ⇒ DL). [**H-1**]
SC-2: if the car is not moving then the doors must be unlocked. (¬MV ⇒ ¬DL) [**H-2**]
SC-3: the car is moving if and only if the doors are locked (MV ⇔ DL). [**H-1, H-2**]

Control Actions:
CA-1: lockDoors (when door-lock signal then DS is true).
CA-2: unlockDoors (when door-lock signal ¬DS is true).

Control Constraints:
CC-1: if wheel-pulse feedback then door-lock signal (WP ⇒ DS) [**CA-1**]
CC-2: if no wheel-pulse feedback then no door-lock signal (¬WP ⇒ ¬DS) [**CA-2**]
CC-3: wheel-pulse feedback if and only if door-lock signal (WP ⇔ DS) [**CA-1**, **CA-2**]

A Provably Safe Control Scenario – *Proving consistency between CC-3 and SC-3.*



$$\frac{\mathrm{WT} \Leftrightarrow \mathrm{WP} \quad \mathrm{WP} \Leftrightarrow \mathrm{DS}}{\mathrm{WT} \Leftrightarrow \mathrm{DS}} \qquad \frac{\mathrm{DS} \Leftrightarrow \mathrm{DL}}{\mathrm{WT} \Leftrightarrow \mathrm{DL}}$$

$$\frac{\mathrm{MV} \Leftrightarrow \mathrm{WT} \quad \mathrm{WT} \Leftrightarrow \mathrm{DL}}{\mathrm{MV} \Leftrightarrow \mathrm{DL}}$$

Car/Wheels	Car/Doors	DLCU	Road
wp :- wt. wt :- wp.	ds :- dl. dl :- ds.	wp :- mv_pm. mv_pm :- wp.	mv_pm :- ds. ds :- mv_pm.	mv :- wt. wt :- mv.

SC-3

```
violation :- mv, -dl.          /* C1 */
violation :- mv, dl.           /* C2 */
-violation :- not violation.   /* C3 */
:-violation.                   /* C4 */
```

Clauses C1 and C2 define how **SC-3** can be violated. Note that the satisfaction of ¬dl and ¬mv requires explicit evidence for the negated propositions, i.e. failure to satisfy dl and mv is not sufficient to conclude that their negations hold. Clause C3 defines an explicit violation in terms of the failure satisfy violation. Clause C4 encodes the top-level proof: explicit evidence that there are no violation implies **SC-3** it true. The Extended Logic Programming demos are available via the **Web-resource-ELP(see the QR code).**

Identifying Loss Scenarios (STPA Step 4)

We focus here on how loss scenarios could occur as a result of *flawed assumptions*. Specifically, we will focus on assumptions relating the environment in which a controller (i.e., DLCU) operates.

In the case of our car example, the following proposition is equivalent to the violation of system-level constraint **SC-3**:

$$(MV \wedge \neg DL) \vee (\neg MV \wedge DL) \tag{1}$$

Note that the left disjunct of (1) relates to **H-1**, a passenger opens their door while the car is moving, while the right disjunction relates to **H-2**, a passenger is unable to open their door while the car in stationary. Here we focus on the left disjunct, i.e.

$$(MV \wedge \neg DL) \tag{2}$$

The verification proof given in above relies upon three assumptions. The violation of each assumption gives rise to a distinct loss scenario that satisfies (2). Two of the scenarios correspond to component accidents, i.e., a wheel-pulse signal failure and a door-lock signal failure. Below we focus on the third assumption, i.e.

$$(WT \Leftrightarrow MV) \tag{3}$$

Specifically, we consider the case where (3) is replaced by:

$$(WT \Rightarrow MV) \wedge \neg(MV \Rightarrow WT)$$

This violation of (3) gives rise to a loss scenario where the car wheels are not turning but the car is moving, i.e.

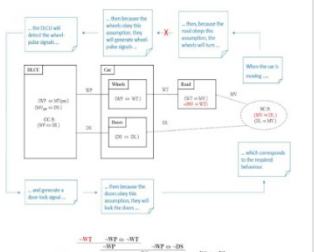
$$(\neg WT \wedge MV)$$

So formal modelling provides a mechanism for generating abstract loss scenarios. However, it provides no insight into the feasibility of the generated loss scenarios. We use simulation to provide such insight. Simulators are rich in terms of their knowledge about real-world phenomenon. What we propose is to leverage this knowledge in order to elaborate an abstract loss scenario. In so doing, we are exploiting synergies that exist between formal modelling and simulation, and providing engineers with more realistic and accessible loss scenarios to consider. CARLA provides various mechanisms to assist a developer to define a simulation. In terms simulation parameters, these are classified as follows:

- **Physics of a vehicle:** includes concepts such as torque, drag and friction.
- **Traffic behaviour:** predefined behaviours are provided, i.e. cautious, normal, aggressive, but a developer is free to define the behaviour of the vehicles within their simulation.
- **Perception:** weather conditions and the attributes of sensors, e.g. accuracy in poor lighting.

Given that the simulation space is significantly richer than the formal model, additional guidance is required in order to constrain CARLA. That is, we need access to domain knowledge about how stuff fits together as well as how stuff behaves in accordance to the laws of physics. Such knowledge could be represented in terms of an *ontology* – an ontology provides a means of representing and reasoning about domain knowledge.

A Violation of the Safe Control Scenario – *Inconsistency between CC-3 and SC-3.*



$$\frac{\neg\mathrm{WT} \quad \neg\mathrm{WT} \Leftrightarrow \neg\mathrm{WP}}{\neg\mathrm{WP}} \qquad \frac{\neg\mathrm{WP} \Leftrightarrow \neg\mathrm{DS}}{\neg\mathrm{DS}} \qquad \frac{\neg\mathrm{DS} \Leftrightarrow \neg\mathrm{DL}}{\neg\mathrm{DL}}$$

$$\frac{\mathrm{MV} \quad \neg\mathrm{DL}}{\mathrm{MV} \wedge \neg\mathrm{DL}}$$

Car/Wheels	Car/Doors	DLCU	Road
wp :- wt. wt :- wp.	ds :- dl. dl :- ds.	wp :- mv_pm. mv_pm :- wp.	mv_pm :- ds. ds :- mv_pm.	mv :- wt. wt. mv.

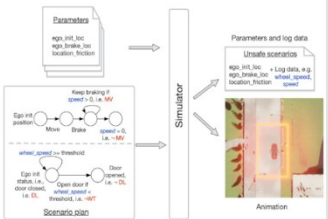
SC-3

```
violation :- mv, -dl.          /* C1 */
violation :- mv, dl.           /* C2 */
-violation :- not violation.   /* C3 */
:-violation.                   /* C4 */
```

The consequences of violating the design assumption, i.e., (WT ⇔ MV), are shown above. Firstly, the informal argument diagram shows where the verification proof breaks. Secondly, the violation is represented as a sequent proof. Lastly, the ELP formulation of the violation is given.

Car Learning to Act (CARLA) Simulator for Autonomous Driving

Exploring a loss scenario in simulation: $\neg WT \wedge MV$



The inputs above on the left include:

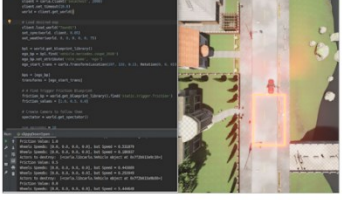
i. setup parameters for the simulation, and
ii. template scenarios that encode the abstract loss scenario identified by the formal modelling.

Note that while a graphical notation is shown, the developer uses a Python API to specify the inputs. The output from the simulator takes the form of:

i. an animation of the loss scenario, and
ii. a log of all the relevant parameters.

Note that a demo of the case study simulation is available via the **Web-resource-CARLA (see the QR code).** which includes the animations generated by CARLA.

A user's view of the CARLA simulator



References:

[1] Dosovitskiy, A., Ros, G., Codevilla, F., Lopez, A., & Koltun, V. CARLA: An open urban driving simulator. *Conference on robot learning*, (pp. 1–16), 2017.
[2] Gelfond, M., & Lifschitz, V. (1991). Classical negation in logic programs and disjunctive databases. *New generation computing*, *9*, 365–385, 1991.
[3] Jackson, M. *Problem frames: analysing and structuring software development problems*. Addison-Wesley, 2001.
[4] Leveson, N. G., & Thomas, J. *P. STPA Handbook*. http://psas.scripts.mit.edu/home/materials/, 2018.

Web-resource-CARLA

Web-resource-ELP

The research reported in this paper is supported by the

UKRI Trustworthy Autonomous Systems Node in Governance and Regulation

(EPSRC grant EP/V026607/1).

UKRI Research Node on *TAS Governance & Regulation*

KU LEUVEN

KU Leuven Bruges Campus
Faculty of Engineering Technology

An Overview of IEEE Std 1848- 2020: Standard for Techniques and Measurement to Manage Functional Safety and Other Risks with Regards to Electromagnetic Disturbances

Keith Armstrong (Cherry Clough Consultants Ltd) and Davy Pissoort (KU Leuven)

What is IEEE 1848 about?

IEEE 1848 provides guidance on the assessment and application of techniques and measures that can reduce the risks associated with the interfering effects of electromagnetic disturbances on digital electronic systems, especially safety- or mission-related systems. These techniques and measures would be applied where electromagnetic disturbances could cause errors, malfunctions, or failures leading to unacceptable risks over the lifetime of equipment, whether safety or any other kind of risk is to be managed.

Why is IEEE 1848 needed?

All electronic and electro-mechanical technologies can suffer errors, malfunctions, or failures due to electromagnetic interference (EMI), which can be caused by electromagnetic disturbances..

Compliance with electromagnetic immunity test standards (for example, those listed as providing a presumption of conformity to the EMC Directive) **does not** demonstrate safety performance, and traditional immunity testing cannot validate equipment's safety performance to the confidence required for safety applications!

There are several reasons for this:

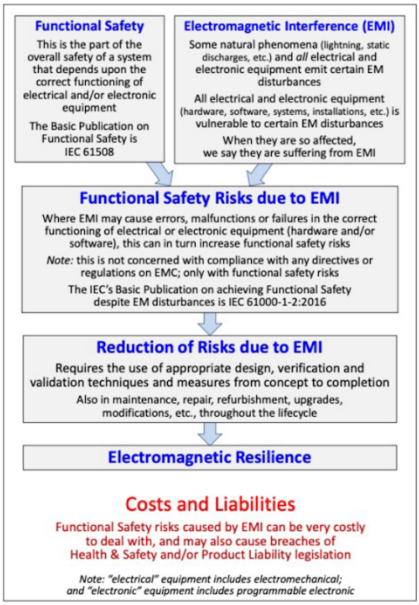
1. Programmable digital systems (hardware and software) have far too many possible digital states to ever be thoroughly tested. Even once.
2. They are also non-linear, so we can't interpolate. This means we can't test a percentage of digital states and assume that the results suggest anything about the behaviour of the untested states.
3. The inherent and unavoidable unpredictability of programmable digital systems is why they cannot ever be shown to be safe enough by any possible test programme.

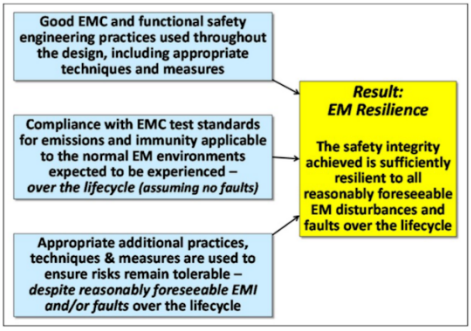
IEEE 1848 introduces the concept or "electromagnetic resilience"

IEEE 1848 introduces the concept of eletromagnetic resilience, by which we mean that *the device can adjust its functioning prior to, during, or following an interference event and maintain its critical capabilities and services in these unanticipated conditions.*

Think of electromagnetic resilience as follows:

1. Application of risk-based EMC engineering ensures (in a cost-effective way) that most EM disturbances don't cause actual EMI
2. But extreme, unusual, unforeseen EM disturbances and/or degradations in EM mitigations mean that EMI can still occur during the full lifetime
3. EM Resilience means additional techniques & measures to:
    1. Detect EMI-induced errors, malfunctions, or faults in signals, data, control,…
    2. Correct these errors so that operation continues safely-enough, perhaps with some functional degradation
    3. Or switch the system into a safe / minimum risk state





Download IEEE 1848 from https://standards.ieee.org/ieee/1848/7221/

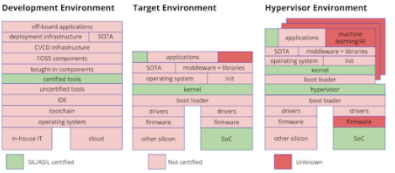
Engineering safety-critical systems with open source software

Problem statement

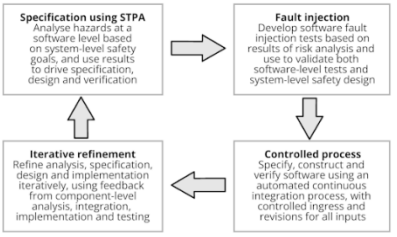
1) Open source projects do not typically apply the formal software engineering processes (notably quality management, requirements specification, design) expected by safety and related standards.

2) If changes are made to open source software (or documentation or tests are extended or added) in order to achieve safety certification for a product, and these improvements are not shared with the originating projects, this defeats some of the key benefits of the open source model.

3) The use of increasingly complex, software-intensive systems in safety applications makes 'traditional' component-oriented approaches to assurance increasingly difficult with respect to *all* types of software



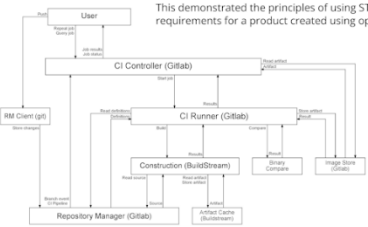
A new approach



A New Approach To Software Safety Using Statistics and Fault Injection
first proposed in May 2021 at ELISA Workshop [1]

DCS: First application of the approach

This approach was applied in the development of a software tool (Deterministic Control Service), which was certified by Exida against the applicable requirements of ISO 26262. [2]



This demonstrated the principles of using STPA to derive and specify safety requirements for a product created using open source software components.

DCS implements the controlled process that is described in ***Automation*** below. Building on the work of the *Reproducible Builds* project [3], it provides a build process that can achieve *binary reproducibility* for a complex software product. This property can be used to verify that:

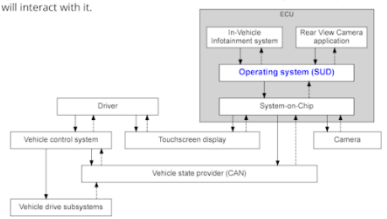
- tool updates do not impact the build process
- all inputs are under control
- build environments is isolated from external factors

Detailed approach: Risk Analysis, Fault Injection and Automation (RAFIA)

1) Risk Analysis

Augment software-level development processes by using hazard and risk analysis at the system level to drive specification, architectural design and testing, and selection and verification of existing software components.

a) Use System Theoretic Process Analysis (STPA) to specify the target system's safety goals, analyse the associated hazards, and model the roles and responsibilities of the *software under development (SUD)* and known or assumed system components that will interact with it.

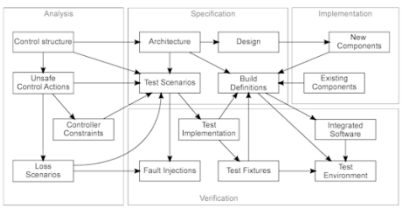


b) Analyse existing software component candidates for integration as part of the *SUD* and evaluate the risks of using them in the system design based on the STPA results and the available evidence from supplier or open source project.

c) Select and analyse development processes and supporting tools to achieve the required levels of safety integrity by mitigating the identified risks, using STPA to inform tool qualification where required. (See **DCS** above)

d) Use STPA results from (a) as the basis of a system specification and derive:
- Detailed safety and nominal requirements for the *SUD*
- System-level test scenarios to verify both nominal and safety requirements
- Architecture and design materials to support test implementation, impact analysis and defect investigation

e) Integrate, implement and verify the software based on the specification, including:
- implementing test fixtures to support execution of system-level test scenarios
- selecting existing components based on the results of (b)
- running existing component-level tests as part of construction
- extending component-level tests where required based on the results of (a) and (b)



2) Fault Injection

Augment software verification and system validation activities by developing software fault injections based on risk analysis.

a) Use *loss scenarios* identified in (1a) as the basis for creating fault injections to:
- validate the effectiveness of tests implemented in (1e)
- support verification of the safety design and system-level safety mechanisms that are *not* implemented by the *SUD* in the target system context

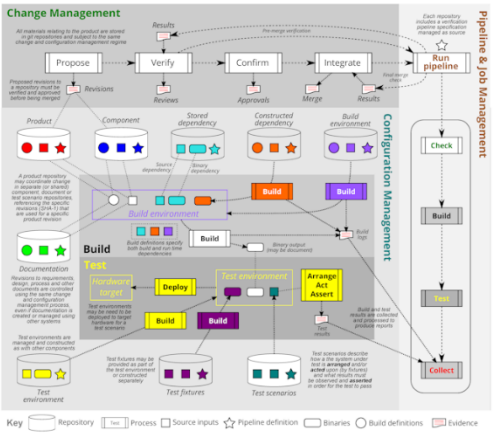
b) Use results of fault injection testing to inform further risk analysis and refine specification, architecture, design, implementation and tests.

3) Automation

Automate the integration, construction and verification of software and the production of the associated documentation and process evidence.

Establish and maintain a unified change and configuration management process controlling all inputs to this process, including requirements and all other documentation. A separate *product* repository is used to manage integration and approval of revisions of all inputs across different repositories.

For open source components, the repositories are *mirrors* of the originating repositories, which are under our direct management and maintained on infrastructure that we control. This means that unexpected changes to the originating repositories can be detected, and deleted or rewritten revision references that we rely upon can always be preserved



4) Iteration

Iterate steps 1 and 3 to refine the software, process measures and supporting evidence until they are sufficient to meet the defined safety and process integrity goals.

References

[1] New approach talk: https://elisaworkshopmay2021.sched.com/event/j3T7
article: https://www.codethink.co.uk/articles/2021/new-approach-to-safety/
[2] DCS certificate: https://www.exida.com/2021/COD_19-12-002_C001_V1R2_Tool_Qual_-_DCS.pdf
article: https://www.codethink.co.uk/articles/2021/deterministic-construction-service/
[3] Reproducible builds project: https://reproducible-builds.org/

Contact: Paul Albertella (paul.albertella@codethink.co.uk)

Copyright Codethink 2023 - All Rights Reserved

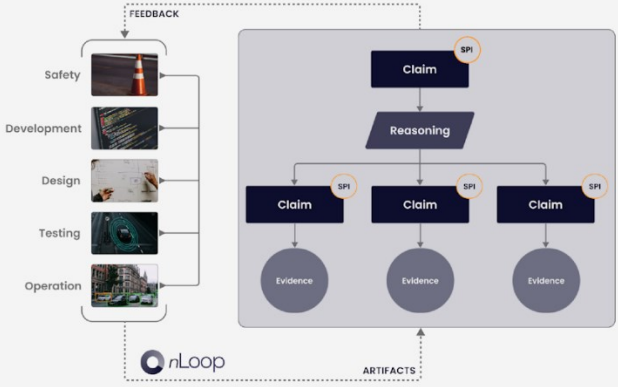
nLoop from Edge Case Research

A connected platform that uses aggregated, cross-functional data to manage, measure, and communicate risks posed by autonomous vehicles, providing confidence that such vehicles are safe to be deployed.

Build *Don't start at square one.*

Support for modeling structured safety cases, in compliance with different languages, such as GSN, CAE, and SACM.

The **nLoop Safety Case Framework** offers you: structured argument templates, in compliance with UL 4600, ISO 24118 PAS (SOTIF), MIL-STD-882E and other standards, associated safety performance indicators, an overarching strategy and development philosophy, and lower-level supporting artifacts, including process definitions, requirements checklists, and related guidance.



Measure *Stay up to date with your progress.*

Measure the validity of your safety claims using validity indicators, such as process metrics, or safety performance indicators (SPIs).

nLoop supports safety argument change impact analysis as the validity indicators of higher-level claims take into consideration the validity status of lower-level claims. Given updates to the available safety evidence, the validity status of the claims in the safety case is rechecked. nLoop encourages continuous improvement of the system, based on feedback provided by the validity status of claims in the system safety case.

Monitor *Be certain you are safe.*

Connect static and real-time data from multiple tools and sources for ingestion and assessment and report to a safety case.

Data connectors allow the ability to extract data in real time from varying internal and external tools and sources, such as static files, databases, process management tools, requirements management tools, model-based system engineering tools, or the internal Virtual Test House (VTH). VTH is an in-house developed testing platform, which offers a central location for creating test cases compatible with multiple test platforms and view results. With scenario specification, test automation, and test results analysis, the platform provides full test traceability from hazards to test results and management across simulation, test-track, and on-road testing operations.

Let's talk! Here's how to get ahold of us:

EDGE CASE RESEARCH
www.ecr.ai

US Office
2555 Smallman Street, Suite 120
Pittsburgh, PA, 15222, USA

European Office
Karl-Theodor-Straße 55
80803 Munich, Germany



Carmen Carlan
ccarlan@ecr.ai



Michael Wagner
mwagner@ecr.ai



Data Safety Initiative Working group (DSIWG)

SCSC

www.scsc.uk/gd mike.parsons@scsc.uk

SCSC-127H

Started: January 2013 **74 Meetings** **88 Members**

Mission Statement:
"To have clear guidance on how data (as distinct from the software and hardware) should be managed in a safety related context, which will reflect emerging best practice."



"Were entering a new world in which data may be more important than software"
Tim O'Reilly

Example Data Problem

The What3Words app is a widely promoted system that is used for location sharing. It works by dividing the world up into three-by-three-metre squares. This app has been adopted by the emergency services as an easy way to pin-point locations, however, it has been found to use some homophones (similar sounding words), which, if incorrectly communicated or heard, will lead to the emergency response going to the wrong location, especially when the phone signal is poor, or someone is speaking in distress.

1



Friends go for a walk through a woodland.

2



One person falls over and breaks their leg. Their friend calls 999 for an ambulance.

3



The friend uses What3Words, to help the ambulance call handler pin point their location. The words are: **steam.rivers.abode.**

4



The ambulance call handler mishears the word sequence to be: **stream.rivers.abode.** Steam and stream sound similar so are easily confused.

5



The ambulance goes to the wrong location (over 50km away), and the patient has to wait a very long time to be reached.

Recent Data Safety related accidents



2020 - Covid-19 test results silently deleted by Excel
Importing Covid-19 test results into an Excel file truncated the data after 65536 records



2018/9 - Boeing 737 MAX-8 crashes
On two occasions, a single faulty Angle-of-Attack sensor repeatedly caused the control software to command the nose down, leading to the aircraft crashing, killing all on board





2017 - Loss of Soyuz-2.1b rocket carrying Meteor-M 2-1 weather satellite
The launch vehicle and satellite were lost because programmers entered coordinates for the wrong cosmodrome



2017 - Cambrian Line Data Loss
Speed restriction data failed to be passed to trains, placing pedestrians on level crossings at risk

"There is a forest of data and we need to create a path through"
Tom Adams

Poster sponsored by



"Data really powers everything that we do"
Jeff Weiner

Multi-Core Working Group

Vision

To better understand the safety implications of multi- and manycore implementations, including characterisation and bounding of interference, impacts on timing and how to recover from errors.

To produce an SCSC publication that provides guidance on assuring the safety of multi- and manycore implementations.

Input


EASA

AMC 20-193

AMC 20-193 Use of multi-core processors

1. Purpose

1.1 This AMC describes an acceptable means, but not the only means, for showing compliance with the applicable airworthiness specifications for aspects related to multi-core processors (MCPs) contained in airborne systems and equipment used in product certification or ETSO authorisation. Compliance with this AMC is not mandatory, and an applicant may elect to use an alternative means of compliance. However, the alternative means of compliance must meet the relevant requirements, ensure an equivalent level of safety, and be approved by the Agency on a product or ETSO article basis.

1.2 This AMC provides objectives for the demonstration of compliance with the applicable airworthiness specifications for airborne systems and equipment that contain MCPs, according to the applicability in Section 2 of this AMC.

2. Applicability

2.1. This AMC may be used by applicants, design approval holders, and developers of airborne systems and equipment, which contain MCPs, to be installed on type-certified aircraft, engines, and propellers. This also includes developers of ETSO articles.

This AMC applies to systems and equipment that contain MCPs with two or more activated cores for which the item development assurance level (IDAL) of at least one of the software applications hosted by the MCP of the hardware item that contains the MCP is A, B, or C. The deactivation of cores is handled through the applicable airborne electronic hardware (AEH) guidance.

This AMC does not apply when the IDALs are all Level D or E.

If an applicant modifies the use of the MCP (such as by activating one or more additional cores or adding software of IDAL A, B, or C), then the applicant should reassess the applicability of this AMC.

Section 5.7 of this AMC describes the objectives that apply according to the assigned IDAL (A, B, or C) of the hosted software or of the hardware item that contains the MCP.

2.2. Aspects not covered by this AMC

The following aspects are not covered by this AMC. This does not constitute an exemption, i.e. the objectives of this AMC are still applicable if an applicant uses these features.

Any applicant who uses these features should describe how they are used so that the behaviour of the MCP is not altered, and determinism is still guaranteed.

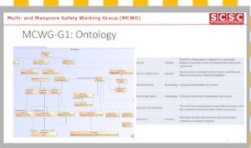
In their planning activities, the applicant should present the methods employed to cover these aspects and satisfy the objectives of this AMC, or show compliance with the applicable airworthiness specifications if they propose an alternative to this AMC on part of it.

Annex to ED Decision 2020-002/R

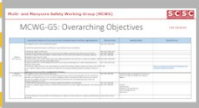
Page 001 of 078



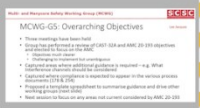
Activities


Multi- and Manycore Safety Working Group (MCWG)

MCWG-G1: Ontology


Multi- and Manycore Safety Working Group (MCWG)

MCWG-G5: Overarching Objectives


Multi- and Manycore Safety Working Group (MCWG)

MCWG-G5: Overarching Objectives

- Three meetings have been held
- Group has performed a review of CAST-32A and AMC 20-193 objectives and decided to focus on the AMC
  - Objectives much clearer
  - CAST-32A document not unambiguous
- Captured areas where additional guidance is required – e.g. What interference channels should be considered
- Initial set of guidance / assurance is expected to appear in the various process documents (17.4, 17.6)
- Proposed a template spreadsheet to summarise guidance and drive other working groups (next slide)
- Next session to focus on any areas not current considered by AMC 20-193


Multi- and Manycore Safety Working Group (MCWG)

MCWG-G4: Safety Argument and Assessment

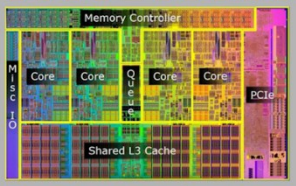
- An initial assurance argument was drafted and reviewed
- Good progress was made but the argument had issues due to the lack of context
  - Some elements of the claims were too specific to an un-stated (implicit) context
  - Some claims were undeveloped as the desk was in the detail
- G4 then considered appropriate architectures to give context before the argument was revised
- It was agreed that considering the whole of CAST-32A was too much so Resource_Usage_3 was assessed in further depth
- The next stage is to focus on a very simple use case


Multi- and Manycore Safety Working Group (MCWG)

Sub Group 6 – Process for Meeting Standards and Guidance

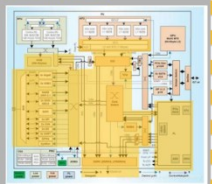
- Group activity has focused on what modifications are required to a traditional development process to meet the objectives in CAST-32A and AMC 20-193
- Initial work has considered how the objectives, assessed as difficult, could be achieved
- Next step is focus in on a development phase to split this task into manageable subtasks with consideration to the interfaces items available
- The key Goal is to gain agreement with the Authorities on the process modifications

Context



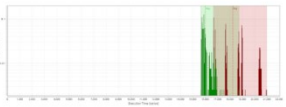
Challenges:

- Sharing of IP
- No usable case studies
- Significantly more complexity
- Solution dependent on specific hardware knowledge

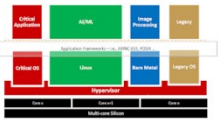

Xilinx ZYNQ UltraScale+ MPSoC

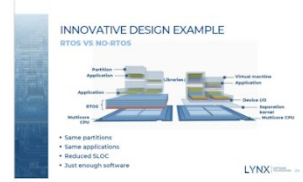
LYNX

L2R Multicore Interference



Using Virtualization




INNOVATIVE DESIGN EXAMPLE

RTOS VS NO-RTOS

- Same partitions
- Same applications
- Reduced SLOC
- Just enough software

LYNX

RAPITA

WINDRIVER

Copyright Wind River. All rights reserved.

Chairs: Louise Harney and Lee Jacques
35 Members
7 Sub Groups

MCWG-G1: Ontology Michael Ward	MCWG-G2: Literature Review Louise Harney	MCWG-G3: Review of Existing Standards and Guidance Guillem Bernat
MCWG-G4: Safety Argument and Assessment Iain Bate	MCWG-G5: Overarching Objectives Lee Jacques	MCWG-G6: Processes for Meeting Standards and Guidance Dave Speed
MCWG-G7: Case Studies *No Lead*		

THE FUTURE OF SAFER SYSTEMS SAFETY CRITICAL SYSTEMS CLUB

THE SYSTEMS SAFETY COMMUNITY AND CLUB

SCSC

Systems Approach to Safety of the Environment Working Group

https://scsc.uk/ge

Mission Statement

To produce clear guidance on how engineered systems should be developed and managed throughout their entire lifecycle so as to preserve, protect and enhance the environment

Why are we doing this?

- There are some real and important differences between systems safety in a traditional specific safety sector (aviation, rail, etc.)
- Idea is to apply Systems Safety approach to systems which are embedded within the natural environment
- We are focussing on harm to the environment, which has a wider and more encompassing basis then traditional safety engineering



The Problem Space

- Systems have been a contributing factor in major accidents (Bhopal etc)
- The impact of systems is not sufficiently addressed in current environmental safety management practices and standards
  - which tend to be prescriptive and regulation-based
- Emergent behaviours of systems and eco-systems are not currently assessed and managed from a multi-dimensional perspective
  - Could introducing systems thinking to specifically manage environmental risks due to systems
- There are business, societal, and wider environmental benefits, in terms of reduced harm, reduced liabilities, and improved business efficiencies, in improved management of systems risk related to safety of the environment
  - Current commercial / legal penalties do not mitigate environmental risk (e.g. dumping of sewage after recent heavy rains)
- Could a safety case approach with claims and arguments be more appropriate than rules-and-regulations in isolation

Audience

- Regulators
- Developers of systems
- Managers of development projects
- Operators / maintenance
- Procurers / Commercial
- Government / Local Government
- Environmental Groups
- Those impacted by the system

Applicability: Categories of Systems

- Fixed 'assets'
- Mobile systems
- Systems moved to different environments (which were not envisaged)

National / Cultural Factors

- Local sensitivities
- Historical sites
- National / Cultural / Religious issues
- Cultural awareness across nationalities

Differences with Standard Safety Engineering - 1

- Harm Not Immediately Obvious: long-lasting and difficult to assess; likely a longer time frame for harm to materialise
- Potentially Broader Boundaries: systems have potentially wide scope and with more affected parties (for instance pollution in the ocean due to shipping)
- Increased Complexity: there can be more interactions and relationships between element (and stakeholders)
- Ambiguity of Scope: systems may have less well-defined and 'leaky' boundaries
- Multiple Stakeholders: many competing demands with stakeholders from commercial, governmental, national, local, campaign groups, NGO and individuals

Differences with Standard Safety Engineering - 2

- Trade-offs Exist Across Multiple Aspects: There may be an implicit or explicit weighing of benefits (e.g. economic) and losses; when should a change be made to minimise environmental impact?
- Unknowns: There are more unknowns and 'Dark Consequences', i.e. we don't know what the effect will be in the future, particularly on human health
- Long-Term Aggregation of Harms: Cumulative effects and combinations can be significant which normal risk assessment doesn't tend to cover; 'Ecological Ceilings'.
- Wider Societal Aspects: There are business, legal and ethical issues to be considered, e.g. shipping domestic waste to Turkey.

Approach of SASEWG

- Introduce the use of our toolbox: safety analyses, formal assurance, safety case paradigm, etc.
- Need to consider risk models such as Black Swans, Grey Swans, Perfect Storms (things combining together), Dragon King events, etc. as these may be appropriate
- Clearly need to survey before introduction of new system into a context
- Need stick like ALARP, but not the same
- Awareness of legal implications is useful

Analyses

- Analyses need to cover temporal element (ie, now, +1 year, + 10 years, etc
- Need to cover wider impacts (local area, national, international)
- Factor-in special sensitivities
- Allow for significant uncertainties (emergent and social behaviours)

Produce new guidance to improve the situation
Can feed into other SCSC groups to influence direction

Differences with Standard Safety Engineering - 3

- Current Focus on Regulation: Existing methods for environmental safety tend to be more regulation and compliance-based
- Wider Set of Effects: Include emergent behaviours, chains of events and knock-on effects
- Need to be 'holistic' - systems of systems approach needed; a whole systems view
- Need to Consider Short, Medium, Long-Term: Factor in a long-term cumulative approach; 'My one plastic straw is not a problem.'
- Aim to Improve/Restore: Include management of balance of eco-system; Consider restoration of eco-system 'opportunity management'
- Wider Scope: Aim to improve the overall environmental picture for humans so including mental health, wellbeing, etc.

Differences with Standard Safety Engineering – 4

- Complexity of Natural Systems: Need to be aware of 'tipping points' (Dragon King Events), e.g. population gets too small to be viable
- Note system may be working perfectly but still have environmental impact
- Note culture of not being blamed / not being found out is important
- Insurance can also play a part
- Net-Zero could have a longer-term impact
- Need to ascertain point at which should change to new better system with less impact (viable change)

Guidance Document Planned Contents

1. **Introduction**
   a. Mission Statement
   b. Rationale
      i. Statement of Problem
      ii. Differences with traditional system safety
   c. Applicability
   d. Definitions
   e. Intended Audience
   f. Existing Work
      I. MOD, UK, EU, ISO, etc.
2. **Risk Assessment Approaches**
   a. Preliminary Environmental Hazard/Impact Identification
   b. Evaluation Schemes
   c. Boundaries / Screening & Scoping
   d. Coverage (Impacts, Impacted groups, etc)
   e. Accumulation / Aggregation of harms
   f. Contribution to wider harms
   g. Unknowns
      I. Categories of Events: Black Swan, Perfect Storm, Dragon Kings, etc
      II. Dark Consequences, etc
      III. Non-linear Effects, Feedback Loops & Emergent Behaviours
   h. Improvements & Enhancements
   i. Priorities
3. **Analyses**
   a. Models
   b. Adaptation of existing analyses (STPA, FRAM, etc)
   c. Causality – need domain knowledge
   d. New analyses
   e. Tools / Techniques
   f. Supporting Data
   g. Proportionality (have to know when to stop)
4. **Step by Step Methodologies**
   a. New systems
      I. Lifecycles
   b. Changes to systems
      I. Lifecycles
      II. Additions
      III. Removal and Disposal
   c. Changes to Context
5. **Trade Off Approaches & Techniques**
   a. Principles and Weightings
   b. Included / Excluded
   c. Limits
   d. Business Case Inputs & Oppositions
   e. Obsolescence vs. efficiency
6. **Other Factors**
   a. Local and Cultural Sensitivities
   b. National/International Dimensions
   c. Legal & Compliance Aspects
   d. Moral and Ethical Considerations
   e. Personal Accountability & Justifications
7. **Making Justifications**
   a. Introduction
   b. Argument pattern templates
   c. Systems Approach Environmental Safety Case (SAESC)
   d. Systems Approach Environmental Safety Case Report (SAESCR)
   e. Feed through into SMS/EMS
8. **Reviewing & Auditing**
   a. Risk-based & Cover Systems Aspects
9. **Examples / Case Studies**
10. **Relationship to Other Work / Standards**
11. **Further Work**

Release Initial Issue of the Guidance

What can SCSC do better?

SSS'24

SSS'23

Topic Speakers

Grow the WG with appropriate expertise

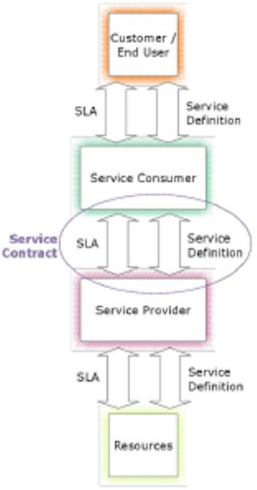
Develop Initial Issue of the Guidance



Are you passionate about the Environment?
Can you provide expertise in the planned content of the guidance?
Would you like to join the working group or attend as a guest speaker to the forum?
If so, get in touch: sarah.carrington@scsc.uk



Poster sponsored by: SQEP






Services


Interface Services


Plant Services


Safety Management Systems


Health Services


Off-Shore Services

Assurance Integration Wrappers

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

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

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

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







Service Assurance Principles

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

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

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

1 Requirements shall be defined to address the service-based solution's (SBS) contribution to both desirable and undesirable behaviours

2 Service assurance requirements shall be satisfied

3 The confidence established in addressing these principles shall be commensurate with the level of risk posed by the service-based solution

4

5

6

Service Assurance Working Group

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

Members: 34
Meetings: 47

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



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

SCSC

Safety Culture Working Group

Founded May 2020

Group Objectives

30 members - Defence, nuclear, rail, energy & health
Quarterly Zoom meetings

Safety Culture Working 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'



Focus areas

- Measuring & assessing Safety Culture
- Improving safety culture
- Safety Culture of large organisations
- Product, system & operational safety
- Safety culture across the system lifecycle - design, manufacture, commissioning, assurance & operation



What is safety culture?

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

Adapted from ACSNI Human Factors Study Group: Third report - Organising for safety HSE Books 1993

Survey of safety culture assessment & improvement (2020-21)

Aims

- Collate feedback on organisation's experience of assessing and improving Safety Culture.
- Help organisations understand how to assess and improve Safety Culture

Responses

- 122 responses from defence, nuclear, aviation, automotive, rail & other

Reasons for assessing safety culture (77% of respondents assessed culture)

Assessments are used to identify and prioritise improvements, set improvement targets and publicise safety culture within the organisation, with some also using results to report to regulators or other stakeholders. Staff questionnaires and workshops are most common methods of assessment.



75% agreed results were very or reasonably valid.

"Results are plausible and reflective of attitudes and behaviours across a broad cross-section of the organisation"

Approaches to improvement

Evidence led strategies, applying good practice to meet defined targets. Measuring progress, reviewing and iterating strategies. A common theme of engagement and two communication.





What works?

- Openness, engagement & collaborative learning.
- Passionate leadership.
- Understandable core messages & a believable vision.
- Exemplifying desired behaviours.
- Continued measurement & sharing results



See full results of the survey at https://scsc.uk/gu?page=SCWG+Survey

Webinars













April 2021:

- Patrick Hudson, Delft University of Technology and Tim Hudson, Hudson Global Consulting: **Safety Culture: What Works in Practice**
- Rob Saunders, Shell: **People Make Mistakes: Learning from Normal Work**
- Sarah Whittaker, Defence Equipment & Support: **Safety Culture: Stimulating Change**
- Michael Wright, Wright Human Factors Ltd: **Results from SCSC Safety Culture Survey**

April 2022:

- Catherine Baker: CIRAS: **Overcoming a culture of safety silence to prevent accidents**
- Tom Hughes: EDF: **Nuclear Safety Culture: From the biggest accident that never was (Davis-Besse) to the realities of building the first new nuclear plant in a generation**
- Steve Gamble - Royal Navy Flight Safety Centre: **Organisational influences on safety: RFA Argus – Wildcat Case Study**
- Michael Wright: **Just culture, psychological safety & facilitating learning from error**
- Michael Wright and Eric Griffiths: **Learning from recent major accidents**

November 2022

- Richard Folkes (OBE, FRAeS, BA Hon, EXON) Head of Aviation Safety/Accountable Manager (Military Flying): **Safety culture at Leonardo Helicopters**

Recordings of webinars are available at: https://scsc.uk/gu

A position paper for assessing & managing safety culture

Work in progress



Aims of the position paper

This position paper aims to:

- Exemplify how safety culture manifests itself in the process of specifying, designing, making and assuring complex safety critical systems;
- Provide guidance on good practice;
- Draw out key methods of particular importance to safety critical systems.

The guidance will focus on the safety of designing, making, assuring and operating complex systems.

Should organisations assess safety culture?

It is recognised good practice and is common practice amongst many safety critical organisations.

What standard of safety culture should SCSC member companies aim to achieve?

Organisations with the potential to contribute to catastrophic accidents are expected to have a proactive culture of continuous improvement, as a minimum.

What safety domains should SCSC member companies address?

Organisations should assess & manage safety culture across design, build, assurance, safety assessment & operation of safety critical systems.

If you would like to become a member of the SCWG, please contact the group leader Michael Wright at michael.wright@scsc.uk

Security Informed Safety Working Group (SISWG)

How do we manage the impact of (cyber)security on functional safety?

Stephen Bull, Nikita Johnson, Wendy Owen, Paul Hampton

contact: stephen.bull@scsc.uk

The problem ...

- **Exploitation of (cyber)security weaknesses can compromise the safety of systems with catastrophic consequences!**
- **This is a growing and complex problem as systems become more interconnected and more digital!**

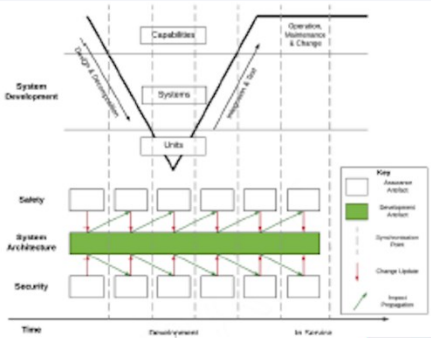
The challenges ...

Safety and security ...

- **use similar techniques but different underlying goals**
- **have different underlying concerns**
- **have different understanding on the causes of loss**
- **requirements may sometimes be in conflict**
- **have different views of the system lifecycle**
- **use differing terms for the same (or similar) concepts**

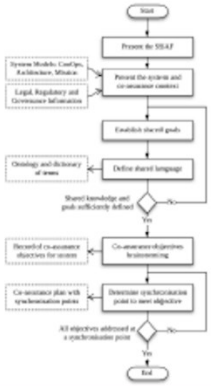


Tell us about experience in your industry!
Refine our guidance documents!
Road test our guidance!



Safety-Security assurance framework (SSAF)

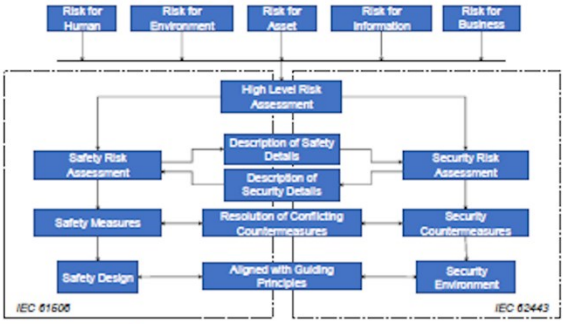
- Separate assurance processes, sharing the right information with the right people at the right time.
- Loose coupling across disciplines
- Mutual understanding to facilitate synchronised solution evolution throughout the lifecycle.



TG1: Co-assurance lifecycle

TG2: Risk assessment process

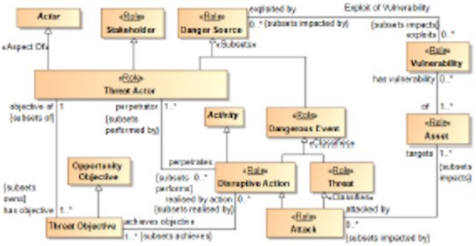
Differences in goals and approach make unified safety and security analysis difficult



TG2 material provides guidance on analysis methods to satisfy the needs of both safety and security

TG3: Common language

Differences in terminology and concepts often impede mutual understanding between safety and security disciplines.



TG3 material is intended to bridge the gap to aid understanding.

We are not trying to develop a common language to be used by all - this is just not practical.

scsc.uk/gi

Poster sponsored by Ebeni

Safety of Autonomous Systems Working Group

SASWG

SCSC

Vision

To produce clear guidance on how autonomous systems and autonomy technologies should be managed in a safety related context, throughout the lifecycle, in a way that is tightly focused on challenges unique to autonomy.

Who we are

SASWG started in 2017 to tackle the safety issues associated with achieving the positive potential of autonomous systems (AS).

The WG contains members active in multiple sectors, including avionics, automotive, defense, maritime, medical, nuclear and others. We have industrial and academic representation, and international participants, as well as members of other safety standard committees.

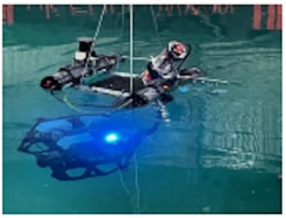
Safety Assurance Objectives for Autonomous Systems



- SASWG guidance contains 55 objectives that should be addressed to achieve demonstrably safe autonomous systems
- Considers issues at *computation/algorithm, architectural* and *platform* level
- Focus is on Machine Learning (ML) elements of AS
- Guidance available on Amazon and via SCSC website

Case study

- SASWG guidance applied to autonomous vehicle for nuclear decommissioning by D-RisQ
- Used to support safety summary to client and regulator



How it works

- Example objectives:
  - COM1-1: Data is acquired and controlled appropriately
  - ARC1-2: Operational inputs inconsistent with training inputs are tolerated
  - PLT1-1: All aspects of platform behaviour that are achieved using autonomy-enabling techniques are justified
- Evidence should be provided to support each objective, or objective justified as not relevant
- Creates context specific safety justification for ML elements

Future meetings and plans

In the next year we will:

- Continue to meet every three to four months
- Develop the guidance document to be more streamlined
- Consider the impact of autonomy and AI on traditional hazard analysis
- Promote our work and contribute to the wider AS safety community

This poster is kindly sponsored by

ATKINS Member of the SNC-Lavalin Group

HEMRAJ GLOBAL EXPERTS IN FUNCTIONAL SAFETY DESIGN FOR THE AUTOMOTIVE, AEROSPACE, & DEFENCE INDUSTRIES

D-RisQ SOFTWARE SYSTEMS

Contact us:

Webpage https://scsc.uk/ga

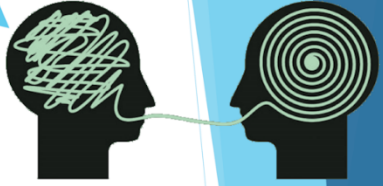
Email: philippa.ryan@york.ac.uk (Chair)

Background photo by Markus Spiske (temporausch.com). Obtained from https://www.pexels.com/

An Ontology of Risk Terminology for Safety and Security Engineering

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

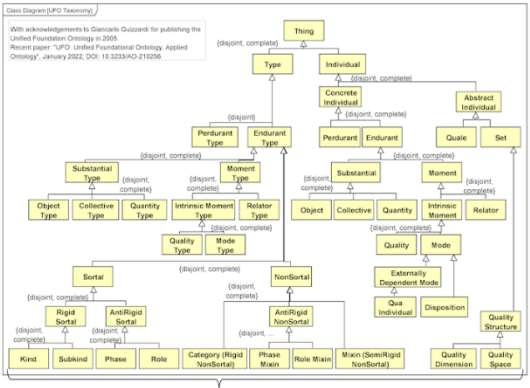




Variation in use and interpretation of language leads to misunderstanding and a lack of fully understood shared objectives; risk terminology originates from many sources including (worst of all) natural language.

Ontologies *conceptualise and formalise* the **World** by defining *concepts*, *terms*, and their *relationships*.

Examples of visual ontologies denoted as UML 2.5 class diagrams.

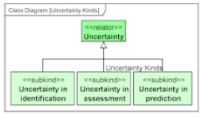


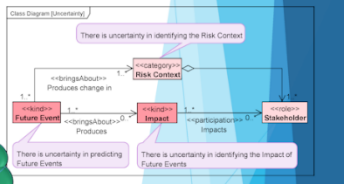
UFO Taxonomy derivative terms define the OntoUML stereotypes. Relationships infer modelling rules for the use of the stereotypes.

The Ontology Working Group

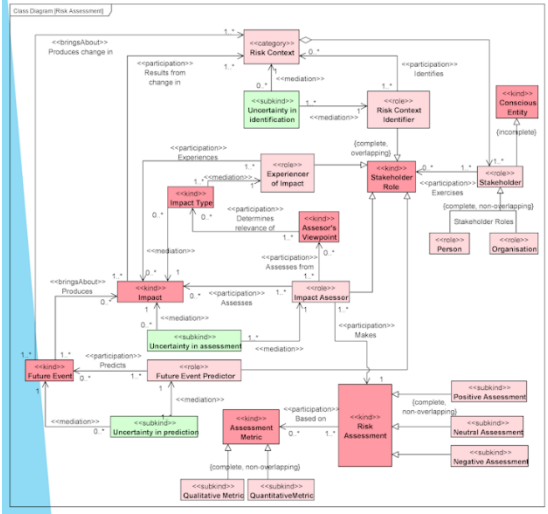
OWG 2023 Objectives:

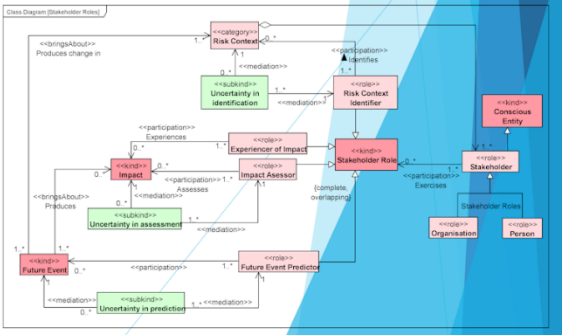
- Develop a clear, systematic, and unambiguous model of risk concepts and terminology and their relationships.
- Adoption of the Unified Foundation Ontology (UFO).
- Use of visual ontology modelling methods; UML and OntoUML profile.
- Liaison with ISO & IEC joint working group on Risk.





Example application of OntoUML for risk concepts





BlackBerry. QNX.
sponsored this poster

Assurance Case Working Group

Find out more and contact us @
ACWG Website: https://scsc.uk/gc and GSN microsite https://scsc.uk/gsn

SCSC
FOR EVERYONE WORKING IN SYSTEM SAFETY

The Assurance Cases Working Group (ACWG) was established in 2017 to provide guidance on all aspects of assurance cases including construction, review and maintenance.

It is intended that this be broader than safety, and address interaction and conflict between related topics. It addresses aspects such as Proportionality; Rationale behind the guidance; Focus on risk, confidence and conformance; Role of challenge, counter-argument and counter-evidence; and Treatment of potential bias in arguments.

The ACWG has established the GSN_SWG, working under its remit, to maintain the Goal Structuring Notation (GSN) Community standard.

WG Membership:

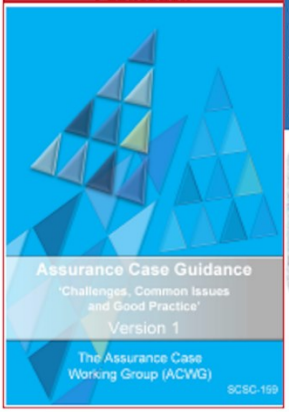
- *Active: 42*
- *Observers: 13*
- *Industries represented:*
  Academia, Aerospace, ATM, Automotive, Consultancy, Healthcare, Maritime, Nuclear, PetroChemical, Rail
- *Countries represented:*
  Australia, Belgium, Canada, Germany, Japan, Norway, Poland, UK, US

Current Activities:

The ACWG is working on guidance material for **Proportionality** and **Assurance Case through the Supply Chain.**

The ACWG is also forming plans to take the next steps for the AC guidance and GSN Standard. These plans are embryonic, and contributions are welcome.

Publication



Guidance has been created to support the production and maintenance of assurance cases that are complete, coherent and proportionate to the confidence required. It is aimed at those who create, review, approve and use assurance cases and is not sector specific.
The guidance takes the form of a framework that provides a general introduction to the scope and context of assurance cases supported by papers that each address a specific guidance topic. Supporting terminology and references are provided.



WG output:

- *Assurance Case Guidance:*
  - *Published: Aug 2021*
  - *Downloads: 2986 (7 Dec 22)*
  - *Amazon Sales: 16 (16 Nov 22)*
  - *WIP: Planning stage for V2*
- *GSN Standard*
  - *Published: May 2021*
  - *Downloads: 4149 (7 Dec 22)*
  - *Amazon Sales: 12 (16 Nov 22)*
  - *WIP: Planning stage for V4*
- *Published documents are made available:*
  - *Under Creative Commons 4 license*
  - *In soft copy (A4-pdf) for free via SCSC website*
  - *In hardcopy (8.5"x11") via Amazon (search SCSC in books)*
- Online Resource (GSN microsite)

Guidance topics in the current publication:

- **Avoiding Bias in Assurance Cases:** identifies a number of common biases to be aware of (and thus avoid) when constructing, reviewing and using an assurance case.
- **Risk versus Benefit:** outlines the need to balance risk against benefit and how to tell when such an argument may be required.
- **Modular Assurance:** deals with the structure and presentation of large and complex assurance arguments to support reader comprehension and managing the impact of change.
- **The Risk-Confidence-Conformance Approach:** introduces the concept for clear presentation of arguments structured around three central themes.
- **Dialectic Arguments in Assurance Cases:** introduces the concept of dialectic arguments to add confidence to an assurance argument while it is being authored or during review/evaluation.

Goal Structuring Notation (GSN) Standard

GSN is a graphical argument notation that can be used to document explicitly the individual elements of any argument (claims, evidence and contextual information) and the relationships that exist between these elements and the context that is defined for the argument.

The GSN Standard includes:

- Introduction And Concepts;
- Definition Of The Goal Structuring Notation;
- Guidance On The Development And
- Evaluation Of Goal Structures.

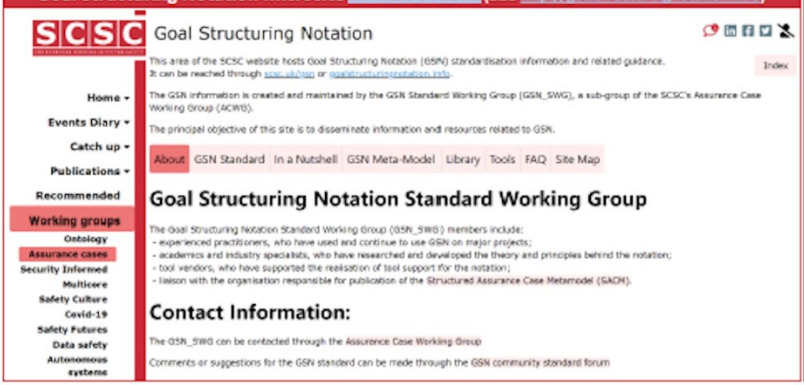
A complementary web-based repository of GSN resources (GSN microsite) has been created.

A meta-model of GSN has been developed, showing the relationship to Object Management Group's (OMG) Structured Assurance Case Metamodel (SACM).



Printing sponsored by:
Engineer for Safety ...and... Limited
The Furious Engineer
Independent System Safety Consultancy and Training

Goal Structuring Notation Microsite https://scsc.uk/gsn (also http://goalstructuringnotation.info)


SCSC

Goal Structuring Notation

This area of the SCSC website hosts Goal Structuring Notation (GSN) standardisation information and related guidance.
It can be reached through scsc.uk/gsn or goalstructuringnotation.info

Index

Home
Events Diary
Catch up
Publications
Recommended
Working groups
Ontology
Assurance cases
Security Informed
Multicore
Safety Culture
Covid-19
Safety Futures
Data safety
Autonomous systems

The GSN information is created and maintained by the GSN Standard Working Group (GSN_SWG), a sub-group of the SCSC's Assurance Case Working Group (ACWG).

The principal objective of this site is to disseminate information and resources related to GSN.

About | GSN Standard | In a Nutshell | GSN Meta-Model | Library | Tools | FAQ | Site Map

Goal Structuring Notation Standard Working Group

The Goal Structuring Notation Standard Working Group (GSN_SWG) members include:
- experienced practitioners, who have used and continue to use GSN on major projects;
- academics and industry specialists, who have researched and developed the theory and principles behind the notation;
- tool vendors, who have supported the realisation of tool support for the notation;
- liaison with the organisation responsible for publication of the Structured Assurance Case Metamodel (SACM).

Contact Information:

The GSN_SWG can be contacted through the Assurance Case Working Group

Comments or suggestions for the GSN standard can be made through the GSN community standard forum

Publication



The Innovative Hydraulics and Automation Lab



Marea de Koning discusses the safety assurance challenges of highly automated heavy-duty mobile machinery, often operating in harsh environments, such as construction and mining sites. She introduces her research aimed at addressing these issues through safe logic-driven decision making and describes the role the Innovative Hydraulics and Automation Laboratory plays in supporting those objectives.

The fourth industrial revolution is characterised by the emergence of smart cyber-physical systems (CPSs) that integrate various levels of automation, such as heavy-duty mobile machinery (HDMM), robotic systems, and automotive vehicles. These CPSs require behaviours with higher levels of automation, perception, and cognition not only to execute their functions but also to ensure the safety of their intended behaviour. This necessitates the integration of numerous sensors, actuators, deterministic, probabilistic, and data-driven elements to interrelate with each other, resulting in complex architectures where hidden flaws can lead to death or serious injuries to humans, severe damage to the machine, or environmental harm, i.e., safety-critical situations.

In light of technological advances facilitated by the integration of autonomous capabilities in HDMM, safety is of a growing concern. With operators being phased out from full control of the machines, it is necessary to determine a method that harnesses the advantages of automation while ensuring adequate levels of safe and logic-driven decision making by the machine.



Tampere University and the Innovative Hydraulics and Automation Laboratory

Tampere University (Tampereen yliopisto) was established on 1st January 2019 through a merger between Tampere University and Tampere University of Technology. Along with TAMK – Tampere University of Applied Sciences, this constitutes the higher education community of the Tampere area [1]. Within the Department of Automation Technology and Mechanical Engineering (ATME), the Laboratory of Innovative Hydraulics and Automation (IHA) conducts interdisciplinary research in the field of fluid power and automation, bridging theory and practice in close collaboration with industry.

IHA provides excellent facilities for practical research, including the campus area testing ground. This area has several instrumented HDMMs enclosed within a 4,000m^2 working area for excavating, with different surfaces ranging from gravel to asphalt and a hill with three slopes ranging up to about 18 degrees [2]. Within IHA, the Autonomous Mobile Machines Research group, led by Prof. Reza Ghabcheloo, the Zonal Hydraulics and Hybrid Technology Research group, led by Prof. Tatiana Minav, and the Heavy-Duty Robotics Research group, led by Prof. Jouni Mattila, conduct practical and relevant research based on solid theoretical grounding in the application areas of HDMM and heavy-duty robotics. Our research focus is determined to face emerging challenges with the goal of developing innovative solutions, methods, tools, and processes to build energy-efficient autonomous behaviours in a short time and at lower costs that are generic, modular, and transferable.

Safety Limitations in varying levels of HDMM automation

The increase in levels of automation integrated in machinery exceeds the scope of available safety assurance guidelines, limiting the market placement of highly automated HDMM within the European Economic Area (EEA), as compliance with regulatory requirements cannot be guaranteed. For example, the existing legislation on safety in HDMM does not consider limited or no operator control for safety assurance purposes, revealing limitations for manufacturers in justifying sufficient integration of adequate risk reduction efforts.

Increasing the automated capabilities of a HDMM to a level where it becomes responsible for the correct execution of its tasks, it consequently assumes the responsibility of safety. When a machine becomes responsible for safety it must become aware of the environment it operates in, this requires a significant and reliable level of perception and safe logic-driven decision making. Additionally, HDMM operates in harsh environments, such as construction sites or mining sites, providing unique challenges for system architecture and interoperability of safety functions.

The integration of complex systems supplied by multiple vendors can make interoperability and safety across components difficult. Ensuring that all of the different subsystems work together effectively and reliably requires thoughtful design, integration, validation and testing.

"Existing legislation on safety in heavy-duty mobile machinery does not consider limited or no operator control for safety assurance purposes."

Compliant Safety Assurance for Automated HDMM

As a result of these concerns, my research aims to find a balance between higher levels of automation in HDMM while simultaneously ensuring adequate risk reduction of safety-critical situations. The ability of a highly automated HDMM to adequately avoid harm through timely reactions of the safety-related control systems requires the integration of high levels of safe logic-driven decision making. The cognitive awareness of a HDMM influencing its decision-making capacity necessitates a significant number of sensors, conventional deterministic software logic, and probabilistic modules such as machine learning and data-driven methods. Furthermore, ensuring the risk reduction efforts are sufficient in relation to the level of automation and operator engagement requires an understanding of EU machine safety legislation.

Ensuring safety compliance of a HDMM becomes challenging when it is capable of executing functionalities based on its own discernment, assuming all task conditions are met. The HDMM's ability to discern the safety of the actions it plans to execute heavily depends on its perception of the environment it operates in. However, the inherent complexity of the HDMM's operating environment significantly increases the risk of known hazardous situations and also opens up the possibility of previously unforeseen hazardous situations emerging. Thereby exceeding the scope of the minimum health and safety requirements as established in EU directive 2006/42/EC.

Through analysis of Directive 2006/42/EC and harmonized machine safety standards it can be concluded that limitations with the machine safety argument emerge throughout the machine safety development lifecycle and can be summarised in six concrete limitations [3]:

- run-time failures
- algorithmic failures
- convoluted architectural design patterns
- data-driven intended behaviour
- quality integration
- formal verification limitations

In addressing the limitation of convoluted architectural design patterns, the current trend is to integrate safety through a separate monitoring layer encompassing intricate fault-handling modules, thereby increasing the overall fault tolerance of the HDMM.

Currently, there are no tangible guidelines available for the safety architectural design patterns of higher complexity. Therefore, my current objective is to determine these design objectives and integrate them into a highly automated HDMM available within IHA.

By providing a physical realisation of safety assurances for highly automated HDMM, I aim to derive a method for future realisations of appropriate risk reduction techniques in highly automated HDMM.

References

[1] Tampere University, "Tampere University Home." https://www.tuni.fi/en Accessed May 2023.

[2] IHA, "Innovative Hydraulics and Automation". https://research.tuni.fi/iha/research/autonomous-off-road-machines/ Accessed May 2023.

[3] AMR de Koning. and Reza Ghabcheloo, "Machine safety conformance limitations for highly automated and autonomous heavy-duty mobile machinery" published in "The Future of Safe Systems: Proceedings of the Thirty First Safety-Critical Systems Symposium". https://scsc.uk/scsc-179 SCSC, York, UK, 2023.

Image Attribution
Images are the copyright of the Innovative Hydraulics and Automation unit of Tampere University, Finland.

Marea de Koning, Doctoral researcher, Tampere University, Finland.

Marea de Koning is a newcomer to the field of safety engineering. She is a doctoral researcher from Tampere University in Finland within the field of safety for autonomous heavy-duty mobile machinery. Her background comes from a bachelor's degree in embedded software development and a master's degree in industrial engineering received from the Netherlands and Germany respectively. Her aim is to contribute to the advancement of autonomous technologies, by ensuring that these systems can be deployed safely.

The author retains copyright of this article.

The Future of Testing for Safety Critical Systems



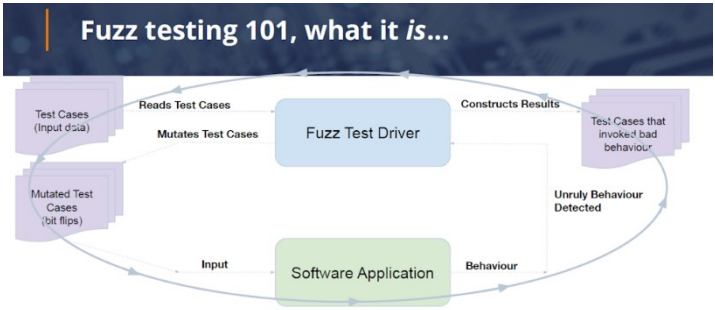
The "Future of Testing for Safety-Critical Systems" seminar was held on the 1st December 2022 at Hard Rock Hotel, London and virtually online. The seminar examined how safety-critical systems are tested. It covered tools, techniques and limitations of testing methodologies and also explored some historical failures of testing and the lessons learnt.

Mike Parsons introduced the seminar and the seminar speakers and said testing was a topic close to his own heart but the topic was vast and applicable at many different levels and there are many techniques and ways of testing. Automation is also a hot topic and there are particular challenges with Artificial Intelligence/Machine Learning (AI/ML).

Fuzzing for High Integrity Software

Paul Butcher from AdaCore, discussed work he was doing in Fuzz Testing under the High Class research initiative – a UK joint venture between industry and the government focussing on cybersecurity in civil avionics. Paul introduced the concept of Fuzz Testing as the injection of random data into a process, which has its origins in the 50's.

Now very popular in Automotive, less so in Defence and Aerospace, but this is changing now due to legislative changes that are helping drive the concept through advisory circulars and guidelines coping with unauthorised electronic access. Advances in hardware allow higher volumes and complexity of data to be injected into the system.



Paul introduced the open source American Fuzzy Lop (AFL) (now AFL++) tool that has a mutational approach, and AdaCore is a maintainer of this source.

Paul described what Fuzzy testing is and said it is more focussed on system behaviour (is in operating in a known state, not crashing etc) rather than checking detailed outputs. The Fuzzer takes an initial input and mutates these at a binary level (without knowledge of structure). One question is how long fuzz testing should be run for, that is, the stopping criteria, and Paul referred to the Security Refutation Objectives in "Airworthiness Security Methods and Considerations" (EUROCAE ED-203A/RTCA DO-356A).

Primary objectives are to automate test case generation, execution and anomaly detection (segmentation faults, hung processes and other language runtime constraint checks: eg. overflow violations). Other more advanced aspects can be techniques such as differential-fuzzing where outputs can be checked by using a reference model and algorithmically generating expected outputs.

Mutation Strategies are generally better than pure random selection and involve making small changes to an initial set and there are different approaches: deterministic, random, splice, dictionary (help to ensure mutations don't get thrown away) and custom.

Fuzzing testing can borrow from genetic algorithms or "smart-grey-box" fuzzing. The natural selection element is 'did my test make progress', for example, by improving the test coverage.

Paul discussed some state-of-the-art approaches:

- Input-to-State Correspondence (also known as "Red Queen" or "CmpLog") helps solve problems with getting into simplistic "tight branches" where entry into the branch is hard, purely by selecting random parameters
- Symbolic Execution using tools like KLEE, is a more heavy-weight approach for the same problem but where there is no clear input to state correlation. Symbolic execution tries to execute multiple code paths simultaneously by working out what the inputs should be to arrive at a leaf node in the execution tree. This does suffer from path explosion and memory issues.
- Concolic using tools like QSym/SymCC is a combination of concrete (traditional unit testing) and Symbolic (especially when coupled with fuzzing)
- Differential Fuzzing is where outputs resulting from fuzzed inputs are compared with a reference model with outputs being compared.

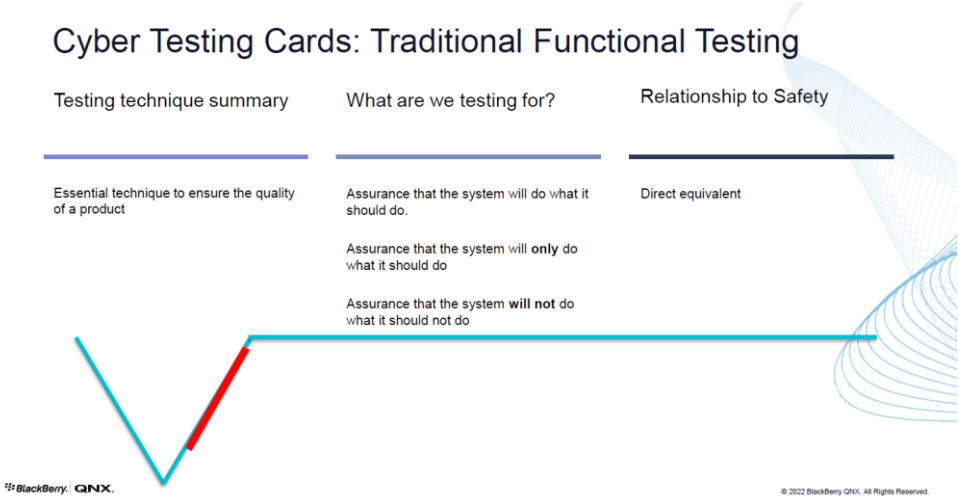
Cyber Security Testing Techniques

Bob Oates from Blackberry QNX – a security company with a focus on automotive and medical device operating systems but with a pedigree in both safety and security.

Bob started with the key security test challenges:

- Quality: (you can't do safety/security without an underpinning of quality. Also test-driven development; breaking the architecture up so it is easier to test
- Technology trends: hyperconnectivity with lots of systems of systems (eg. software-defined vehicle) lots of integrated subsystems. Challenge of security and test coverage especially in autonomous vehicles.
- Threat Trends: increase in attacks of critical national infrastructure and in general state sponsored cyber warfare
- Security Role: safety/security no longer can be siloed
- Resource Constraints: working in a constrained environment and so test worthiness is important

Bob then discussed a number of Cyber Testing Cards:



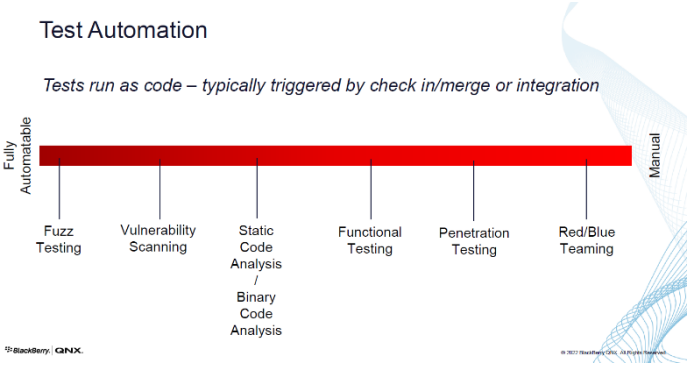
These cards covered:

- **Traditional Functional Testing**: testing against well-define requirements that the system will behave only as specified (classic right-hand side of the "V Model")
- **Fuzz Testing:** scalable approach providing mutated inputs and recording behaviour – highly automatable to test for unexpected behaviour
- **Static Code Analysis:** classic cyber security testing technique, checking code against pre-defined rules such as those in MISRA C and MISRA C++
- **Binary Code Analysis**: decompile binary code using tools like Jarvis and look for 3rd party library usage, static strings and software bill of materials to do license compliance and check against product vulnerability libraries

- **Active Vulnerability Scanning**: scan systems for open ports and library use and mis-configuration. Dangerous to run on live operational system as tests can be harmful!
- **Penetration Testing**: Simulating an attacker with a predefined anchor into the system (such as giving the attacker a user's logon credentials). Need well-defined rules of engagement to ensure the testing is not interacting with safety-critical systems
- **Red v Blue Team Testing**: a more modern technique with a blue team also being part of the test acting in an operational capability to detect and respond to the attacker (red team). Bob emphasised that the blue team can be just as dangerous as the red team if they take an inappropriate action.

Bob then discussed Test Automation and said that it needs a well-defined environment (eg. through use of tools like Docker to automatically provision environments) and well-defined pass/fail criteria.

The level of automation varies depending on the technique and Bob proposed the scale given in the figure opposite.



Bob also said the security of the IT environment, such as the development environment tools, is equally important.

Bob concluded by saying:

- Security is going to be a huge part of the future of safety testing
- We need to understand when and how to perform security tests
- Automation is going to be key to achieving "Test worthiness"

Testing in the real world: hard lessons learnt

Ian McDonald of Island Systems Ltd and John Dixon of Platinum QA Systems started their talk with a description of the costs of failure of software projects that have led to deaths, huge economic impact, costly repairs and recalls and brand damage. Despite this, Ian said it is often a battle to ensure people take a responsible and ethical approach to ensuring systems are sufficiently well-tested.

Ian provided some real-world examples of their experiences, for example, a case where software development was subcontracted without the contract defining the success of code coverage. Requirements were also long with many embedded sub-requirements so difficult to assess test success. This resulted in defect fixes leading to even more defects and the delivery falling behind schedule.

It is key to understand why a customer wants something, their expectations, the timescales, the level of required quality of product and also the stakeholder's perception of risk.

In some cases, an element of evangelism is required to promote the benefits of properly documenting and accurate capture of metrics such as root cause analysis. Blame culture can also be detrimental to a project development as is incentivising the absence of defects as this can lead to lack of reporting and gaming of the test systems.

Hardware testing also needs to be considered – there is a general focus on software testing but issues with the hardware can be just as serious.

Lack of formalised QA and test approaches lead to poor estimation and hence delayed projects that are over budget and bug ridden. John said that testing does not start at the end of a development but at the beginning by ensuring that the requirements make sense, are atomic and are testable.

John and Ian also said to be wary of standard metrics for estimating the amount of testing on a project (eg. 40% of total effort) as large projects require much more effort due to the larger number of interactions.

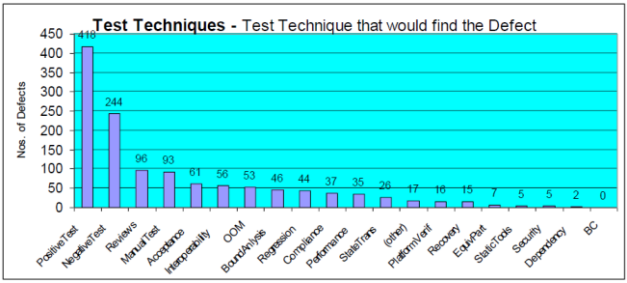
There are techniques to allow you to develop the least number of tests for the maximum impact called boundary value analysis focussing on tests of values around the minimum and maximum values that a variable can hold.

Test strategies are often too reliant on things happening perfectly. A good test manager will be thinking about alternative paths if the unexpected occurs.

Care should also be taken when making assumptions about relying on testing undertaken when reusing software in a different context and gave an example of the Ariane 5 launch failure.

Automation is not a magic bullet; it can help to speed repeatability of testing but there is a cost for updating automated tests and this can take longer than writing the code. Automation doesn't replace good test design. Poor automation may fail to provide sufficient coverage and maintenance costs can mount.

Code standards and implementing code review standards is seen as important. Reviewing code is cheap but it is important that reviews are frequent and have the right people in the review.



Ian concluded by asking how problems are fixed. Two key techniques were discussed: Root Cause Analysis (RCA) and Test Escape Analysis (TEA). Ian said that RCA feedback is often provided late and is therefore not that effective. TEA looks at why defects escaped early detection. This involves a periodic review between the test and development leads to classify defects with the aim to feed this information back into test planning. The figure shows an example chart of defect counts using this method.

Bad Behaviour: Automating system-level safety testing

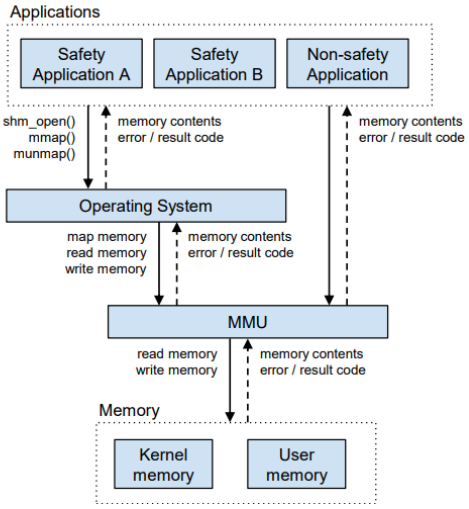
Paul Albertella from Codethink, opened his talk with a discussion of his background in using open source in automating development and testing of systems. Paul said that software testing plays many essential roles in safety. Different types of test have different purposes, context and scope, for example, not just verifying the correct implementation but also other aspects such as detecting issues with integrating software, validating safety mechanisms, testing systems under stress and under adverse environmental conditions.

Paul said that system-level testing is important as safety, being an emergent system property, can only be understood by considering how all the system components work in concert together in a particular context – especially timing aspects.

There are a number of challenges with testing for safety:

- identifying "bad behaviour" rather than just the "happy paths"
- understanding the requirements tests are intended to verify
- ensuring test completeness – coverage does not mean that all conditions have been tested
- making sure tests are consistent and reproducible, not just in test inputs but in replicating the test environment

Paul has been looking at System Theoretic Process Analysis (STPA) as a way of modelling systems to provide a basis for deriving safety test cases. Not only describing how the system behaves but also a way of thinking about the negative outcomes (eg. unsafe control actions) that need to be avoided. it is also often not possible to prevent negative outcomes so ways of mitigating those outcomes need to be considered.



Once the control structure is established, consideration is then given to the impact if those actions are not provided, provided, provided too late/too early and provided too much/too little.

This can then be used to derive and refine safety tests but the process needs to be iterative, even through into live operation, as new issues emerge and to cope with changes to the system requirements.

Ensuring that stakeholders speak a common language is also important as they have different areas of expertise. Using a restricted-form natural language (RNL) can help give stakeholders a clear understanding of tests and their purpose and allows the derivation of logical tests.

Automating system-level tests has a number of considerations:

- What is being tested, how was it built, what else is part of the system and what context is it tested in?
- What actions does the test involve? What observations need to be made and what criteria need to be satisfied?
- How are result collected and published?

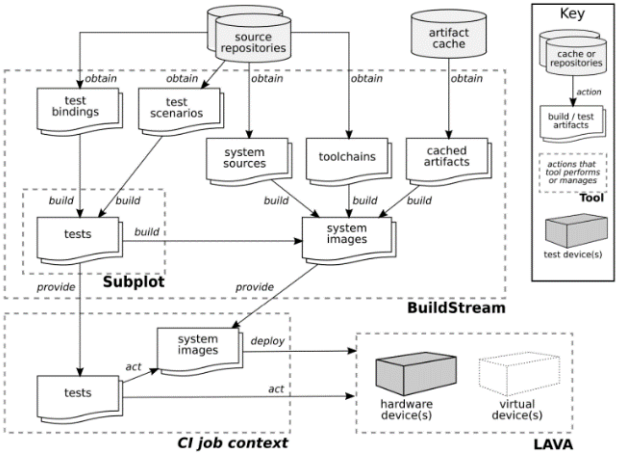
Paul introduced an example of an automation tool called **Subplot** that provides a tool for documenting and executing tests. Scenarios are written in a mark-up language that match syntactical elements (nouns, verbs etc.) to test implementations. Tests can in theory be implemented in any language with current implementations supporting Rust and Python.

Other tools discussed were:

BuildStream allows systems and tests to be built deterministically.

LAVA: manages devices (hardware and virtual) used in system tests, maintaining pools of devices with defined characteristics.

Paul concluded by saying these products can be combined in an ecosystem to automate the end-to-end process as shown in the figure.



Bootstrapping Safety Assurance

Phil Koopman from Carnegie Mellon University concluded the seminar on "bootstrapping" safety assurance using examples drawn from the area of the assurance of autonomous vehicles.

Phil said the autonomous vehicle industry started out by "testing with miles", or simply operating vehicles in the field to gather data and learn from emergent issues. This method however is expensive and there is a risk of high-profile crashes occurring. Nevertheless, several car manufacturers are using the safety of autonomous vehicles as a selling point.

Phil asked how safe is "safe" and noted that the current US fatality rate is ~100M miles per fatal mishap and noted that this includes those with alcohol impairment (28%), speed related (26%) and distracted drivers (9%). The target comparison should therefore be a fully functional driver (unimpaired, undistracted) with a modern vehicle (ie. with modern safety features).

Phil said the target safety rate for autonomy is a difficult question (entire books have been written on it) but suggested a ballpark figure of 200M miles per critical mishap. It is however, impracticable to test using this "brute force" method as it would require 2 billion miles of testing (50 round trips on every road in the world) to be statistically meaningful.

Simulation to supplement road tests is seen as a more feasible and cost alternative; it is scalable and cheaper and capital equipment outlay is much less. However, models are not perfect and there will still be a need for real-world testing to validate the simulations.

Phil introduced the Bootstrapping approach to road testing assurance, which follows the incremental steps as follows:

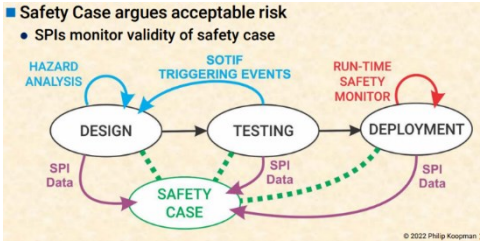
- Observe safety drivers are not intervening
- Remove the safety driver
- Crash-free history predicts crash unlikely for small window
- Drive for small window with no crash
- Repeat last two steps with growing window size

He then, through the use of an example of a successful 10-mile US truck demonstration, argued that because a one-off test did not result in any safety incidents, it does not mean the system is safe. However, the bootstrap argument being used is that every low-risk incremental test without incident contributes to the overall confidence that the system is safe.

Phil then said that if there is a crash during testing, then the bootstrapping argument means you need to test for longer and the maths is not in the tester's favour as it quickly becomes impractical, even if there are only a few crashes. Phil said companies are finding ways to discount crashes, eg. it was the other driver's fault or it was a freak/black swan that's now been fixed.

Phil argued that there is no such thing as "uncrewed AV safety testing" and is really just deployment of unproven technology.

Slow-rolling and pilot deployments also do not help as it is just a manifestation of the Bootstrap argument. They reduce the risk of multiple concurrent early mishaps but this does not mean that systems are any safer.



Phil suggested a potential approach for the issues raised, which is speculative based on Safety Performance Indicators (SPIs). An SPI is a metric supported by evidence that uses a threshold comparison to condition a safety case claim. The metrics are measurements of performance, design quality, process quality, operational procedure conformance etc. Importantly, a violation of an SPI shows that part of a safety case has been falsified rather than a failure of the vehicle. This allows SPIs to be based on aspects that don't involve crashes. A sketch of an argument would be:

- Industry safety standards and strong safety culture
- Known hazards have been mitigated
- Arrival rate of unknowns is low
- Safety has good SPI coverage
- SPI usually detect unknowns without an actual crash

This can then be used to bootstrap on surprise arrival rates and SPI improvements.

Report by Paul Hampton SCSC Newsletter Editor

Image Attribution: lead car: 130733406 / Safety Testing © Andreistanescu dreamstime.com. Other images copyright original authors.

STEAM GWR Museum Tech Trip Report

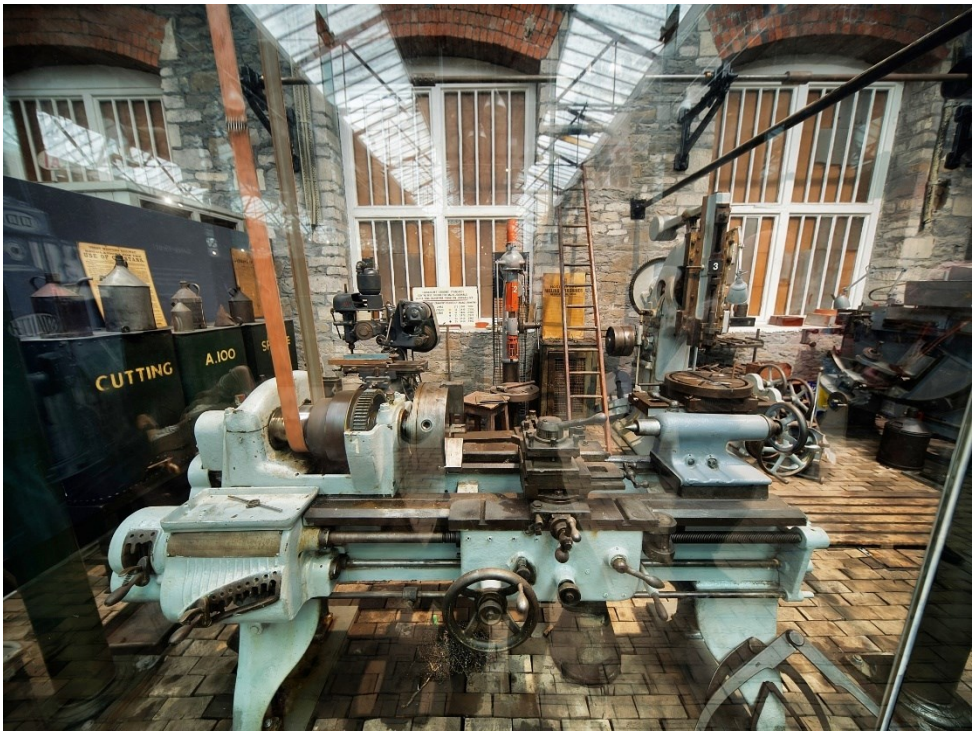


The SCSC's recent Tech Trip was to the STEAM museum of the Great Western Railway on 22nd April 2023. The trip, which was open to everyone, included a highlights guided tour of the museum's collection given by a very enthusiastic and knowledgeable guide. Mike Parsons provides a report of the trip.

Our guide had spent his early working life as an apprentice and worker on the railways. He recounted some fascinating stories about 'life on the footplate' of steam locomotives. The tour was only meant to be an hour but turned into nearly two! The difference a knowledgeable guide brings to appreciating the museum exhibits is amazing; a guide is highly recommended.

The museum is located close to Swindon mainline station, among the vast historic Swindon railways' works buildings. Some of the museum is devoted to the works themselves. In these days of contracting and outsourcing, it is hard to believe that virtually all component manufacture and assembly was done on-site.

Our tour covered the history of the Swindon works itself, the manufacturing process, the people involved, and of course plenty of steam-era locomotives and rolling stock.



Our guide explained that although the workers were paid a good wage, and the site had very good recreational facilities (for the time), total commitment was expected and any absences or deviations were dealt with harshly. Accidents in the works were commonplace but with a site hospital, these could be dealt with quickly.



The museum is spread over several connected halls and features different eras. I found it fascinating to be able to walk underneath a steam locomotive and see the many oiling points that were far underneath and presumably became very dirty.

These apparently had to be serviced before any journey and young apprentices were used to do the job.

There are locomotives, railway buildings and many other artefacts of industrial history (for instance cast-iron moldings – I still don't quite understand how these are used to make things with holes in like pipes!) There are some speed record-breaking locomotives, and plenty of information on Brunel, who was of course, the architect of the railway going west.

There is history of Brunel's broad gauge, which by all accounts was superior to standard gauge in most ways, but was dropped to conform with the rest of the country.

The conversion of the tracks from broad to standard gauge was done amazingly quickly in some cases, and of course, completely manually.



Our guide lined us up for a team photo in front of a fabulous locomotive, Caerphilly Castle:



The museum is spacious and set in an historic industrial context. The picture of the Swindon Works at its height found in the gift shop really put it in context: it was once a vast industrial complex producing two steam locomotives a week.

For some reason I liked this vintage 'bar' coach:



It was a good visit and one that is highly recommended to anyone interested in railways or industrial history.

Special mention must go to our guide who took us on the footplate of one locomotive and recounted many first-hand stories of railway lore. He said there was a 'railway family' and still very much felt he belonged!

The museum's website is: https://www.steam-museum.org.uk it has extensive information about the exhibits too.

Photographs copyright of Mike Parsons.

60 Seconds with ... Jane Fenn



Jane is a Chartered Engineer and Fellow of both the Institute of Engineering and Technology, (IET), and the Safety and Reliability Society, (SaRS). Jane has worked for BAE Systems for 33 years, as a Safety Engineer and an Engineering Manager, focussing predominantly on collaborative research programmes that developed new approaches and processes for safety engineering.

Jane was awarded an MSc in Safety Critical Systems Engineering from University of York in 2004 and has published a number of papers around safety engineering and software architectures.

Jane is an Engineering Fellow within BAE Systems, providing internal safety consultancy and is responsible for the processes, competency and Safety Engineering training within the company. As a Technologist for Safety Engineering for Robotics and Autonomy, Jane advises the company whilst also pursuing a PhD on 'Linking the design and in-service Safety Case for Autonomous Systems' as part of the Assuring Autonomy International Programme (AAIP) at the University of York.

Jane is an active member of the SCSC Working Groups on Assurance Cases and the Safety of Autonomous Systems. She is also a Diversity and Inclusion Champion.

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

I was asked to manage a programme to correct a fault which had been detected during rig testing of a particular variant of a system, where earlier variants were already deployed with seven different international customers. The bug was observed to have potentially safety critical impact, under certain circumstances, which were temporarily controlled by operating limitations, until I could get the fix rolled out across all users. Being at the 'sharp end', considering the scale of the potential risk, the investigation into the root cause and the work to recover the situation as well as putting the lessons learned into the development of a replacement system all whetted my appetite to understand how not to be there again!

What aspect of your career are you most proud of?

I hope and I believe that inspiring others is the most profound legacy one can have. What I can achieve on my own is necessarily limited, but by inspiring others, our collective effects are magnified.

Tell us one interesting unusual fact about yourself!

I'm as passionate about Diversity and Inclusion as I am about Safety! I co-developed and co-present a training course on 'Gender Identity Awareness' for BAE Systems which we've collectively delivered to almost 1000 people, from 1st year apprentices through to company directors.

What advice would you give to yourself age 12?

Recognise earlier that being 'different' is a strength. Don't torture yourself with doubt over whether you are 'good enough' or by trying to please everybody. Decide to ride a motorcycle earlier!

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

Enough with the obsession with failure rates – they give false comfort when it comes to complex systems! Compliance is necessary but not sufficient. It is possible to give safety advice as soon as an idea can be sketched 'on the back of a fag packet'/'on a table napkin' (choose your own generational context), so why wait until design is chilled/frozen/the end of the programme to engage meaningfully with designers, by which time it's far too late to influence design?

"Why wait until design is chilled/frozen/the end of the programme to engage meaningfully with designers, by which time it's far too late to influence design?"

What's your most favourite quote or motto?

"Safety isn't expensive, it's priceless"

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

Be tidier.....

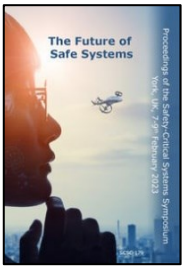
If you could be any fictional character, who would you choose?

I have to choose just one???? Jack Reacher/Robert Hunter/Jack West Jnr/Cotton Mallone/Jonathan Payne/Painter Crowe..... flip a coin!

Tell us about the parrot!

My 'other half' is an Eclectus parrot called Henry. He's 33 this year and he's owned me for about 25 of those years. I also have 3 smaller rescued parrots and they all keep me very busy indeed! They loved me working from home during lockdown and are very unhappy with the amount of time I'm spending away from home again now!

Recent Safety Publications



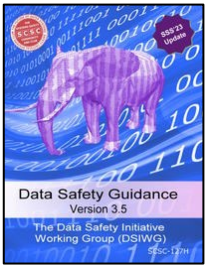
Proceedings of the 31st Safety-Critical Systems Symposium.
scsc.uk/scsc-179



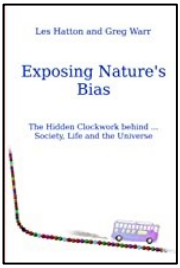
Catastrophe and Systemic Change. Learning from the Grenfell Tower Fire and Other Disasters.
https://www.amazon.co.uk/Catastrophe-Systemic-Change-Disasters-Perspectives/dp/1913019292



Guidance on the Safety Assurance of autonomous systems in Complex Environments.
http://www.york.ac.uk/assuring-autonomy/guidance/sace/



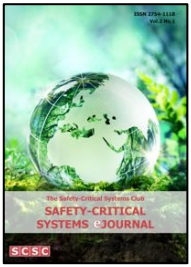
Guidance on the management of data safety risks (V3.5)
scsc.uk/scsc-127H



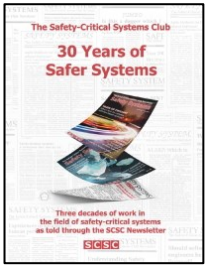
Revealing a newly discovered fundamental law of inequality.
http://www.amazon.co.uk/Exposing-Natures-Bias-Clockwork-Universe/dp/1908422041



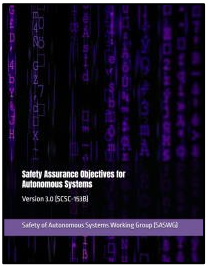
Guidance on assuring safety-related service (V3.1)
scsc.uk/scsc-156C



Safety-Critical Systems eJournal vol.2 no.1 Winter Issue 2022
scsc.uk/scsc-183



Three decades of work in the field of safety-critical systems as told through the SCSC Newsletter.
scsc.uk/scsc-169



Guidance on assuring autonomous systems.
scsc.uk/scsc-153B

Seminar: Safety Cases: Past, Present and Future

Event description | Programme | Booking form

THE SAFETY-CRITICAL SYSTEMS CLUB, Seminar:

Safety Cases: Past, Present and Future

Thursday 29 June, 2023 - London Marriott Hotel, Marble Arch

This seminar will look at the origins of safety and assurance cases, where they are today and where they are heading. There will be a range of speakers covering different aspects, approaches and sectors.

Safety cases have evolved over the years: from their origins in historical accidents, through the development of better structuring and argument notations such as GSN, to where we are today where assurance cases often integrate other key system attributes such as security. The future promises more powerful notations, dynamic updating and approaches for large-scale and complex systems.

This event will be relevant to anyone who has to produce, review or approve safety or assurance cases.

Speakers include:

Robin Bloomfield, Adelard

Richard Hawkins, University of York

Nikita Johnson, Rolls-Royce and Sheffield University

Adrian Stavert-Dobson, Safehand Consulting

Thor Myklebust, SINTEF - *"Future challenges and opportunities when using a safety case approach. Includes results from interviews and coverage of: XAI, compliance, relevant standards for Autonomous Systems and maintenance of safety cases"*

Further details TBA.

This event will be held in-person in at the London Marriott Hotel Marble Arch, 134 George St, London, W1H 5DN.

Seminar: How to Write Compelling Safety Arguments

THE SAFETY-CRITICAL SYSTEMS CLUB, Seminar:

How to Write Compelling Safety Arguments

Thursday 28 September, 2023 - London, TBA

This event will consider what makes a compelling safety argument, and how to use narrative techniques to improve the flow and 'story' of the argument. Talks include one from a professional writer who will explain how to write prose so as to engage and grip the reader.

There will be discussion on the use of metaphor and imagery in arguments and a workshop in the afternoon.

This event will be held in-person in London.

Further details TBA.

Speakers include:

TBA, Ebeni

Catherine Menon, University of Hertfordshire

Connect

The Newsletter and eJournal

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

The SCSC Website

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

Facebook

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

www.facebook.com/SafetyClubUK

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 1,000 of individuals involved in Systems Safety and so is the perfect medium for engaging with the community. For prices and further details, please get in touch with the Newsletter Editor.

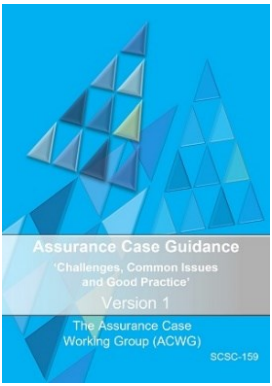
SCSC Working Groups

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

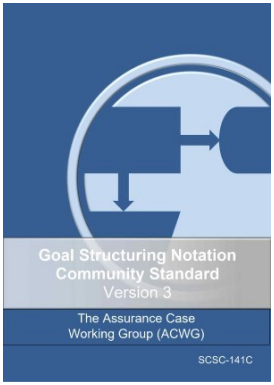
Assurance Cases

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

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



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



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

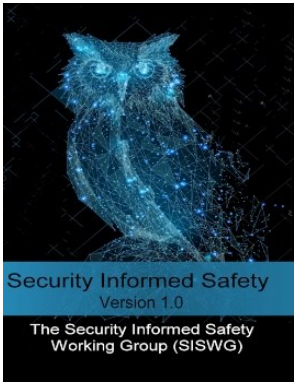
See scsc.uk/gsn for further details.

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

Lead Phil Williams phil.williams@scsc.uk

SCSC Working Groups

Security Informed Safety



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

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

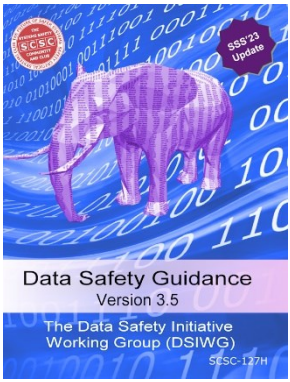
The guidance will allow safety, security and other stakeholders to navigate the different security standards, understand their applicability and their integration with safety principles, and ultimately aid the design and protection of secure safety-related and safety-critical systems.

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

Data Safety Initiative

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

It is acknowledged that data has been a contributing factor in several incidents and accidents to date, including events related to the handling of Covid-19 data. There are clear business and societal benefits, in terms of reduced harm, reduced commercial liabilities and improved business efficiencies, in investigating and addressing outstanding challenges related to safety of data.



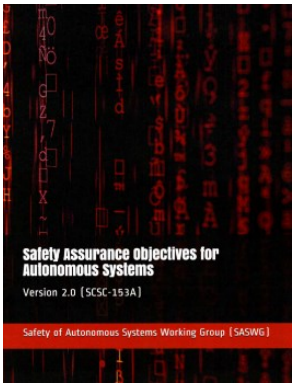
The Data Safety Initiative Working Group (DSIWG) aims to have clear guidance on how data (as distinct from the software and hardware) should be managed in a safety-related context, which will reflect emerging best practice.

An update to the guidance (v3.5) was published in Jan 2023: scsc.uk/scsc-127H

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

SCSC Working Groups

Safety of Autonomous Systems



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

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

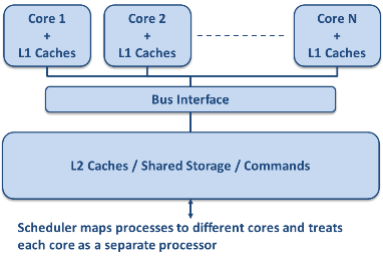
The Safety of Autonomous Systems Working Group (SASWG) aims to produce clear guidance on how autonomous systems and autonomy technologies should be managed in a safety-related context, in a way that reflects emerging best practice.

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

Lead Philippa Ryan pmrc@adelard.com

Multi- and Manycore Safety

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



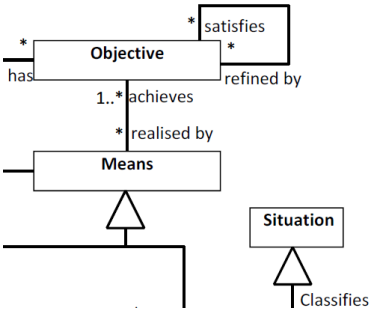
Parallel processes need to access the same shared resources, including memory, cache and external interfaces, so they may contend for the same resources. Resource contention is a source of interference which can prevent or disrupt completion of the processes, meaning it is difficult to know with a defined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

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

Lead Lee Jacques Lee.Jacques@leonardocompany.com

SCSC Working Groups

Ontology



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

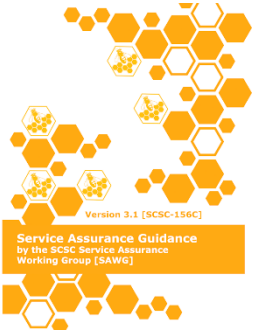
The OWG is currently working on the definition of an ontology of risk for application in guidance for risk-based decision making – notably safety and security – and for which ISO 31000 Risk Management principles are to be applied.

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

Lead Dave Banham ontology@scsc.uk

Service Assurance

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

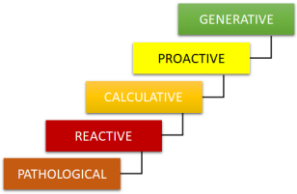


The group published v3.1 of the guidance in Jan 2023: scsc.uk/scsc-156C

Lead Mike Parsons mike.parsons@scsc.uk

SCSC Working Groups

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

Systems Approach to Safety of the Environment



The Systems Approach to Safety of the Environment Working Group (SASEWG) is a new group intending to apply Systems Safety practices to systems that are embedded within the natural environment, while focussing on that environment.

The group aims to produce clear guidance on how engineered systems should be developed and managed throughout their entire lifecycle so as to preserve, protect and enhance the environment.

Since holding its inaugural meeting on 17th June 2022 the group is now well underway with its last meeting held on 21st April 2023 and a further one planned for 24th May 2023. Please get in touch with the working group lead if you would like to join or find out more about this group.

Lead **Sarah Carrington** sarah.carrington@scsc.uk

Safer Complex Systems



The Safer Complex Systems Working Group (SCSWG) builds on the IET/RAE work already done in this area. It is recognised that the RAE work is ongoing and collaboration is encouraged. The group's mission is to produce practical guidance on developing, managing and assuring complex systems throughout their lifecycle (so as to achieve and justify their safety).

The second meeting of the SCSC Safer Complex Systems Working Group will take place on Thursday 25th May 2023. Contact the group lead if you would like to attend or find out more about the working group.

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

SCSC Membership

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

Individual Membership

To become an individual member of the SCSC please register on the SCSC website using the 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: £140
- 2 year Membership: 11% discount: £250
- 3 year Membership: 17% discount: £350 (3 years for the price of 2)
- 1 year SFI Membership: FREE for first year, £35 for years 2 & 3
- 1 year Membership, retired member rate: £35
- For Corporate Membership discounts contact Alex King.

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



Dai Davis
Honorary member



Zoe Garstang
zoe.garstang@scsc.uk



Louise Harney
louise.harney@scsc.uk



Brian Jepson
brian.jepson@scsc.uk



Graham Jolliffe
Honorary member



Alex King
alex.king@scsc.uk



Wendy Owen
wendy.owen@scsc.uk



Felix Redmill
Honorary member



John Spriggs
john.spriggs@scsc.uk



Phil Williams
phil.williams@scsc.uk



Robin Bloomfield
Honorary member



Dewi Daniels
dewi.daniels@scsc.uk



Jane Fenn
jane.fenn@scsc.uk



Paul Hampton
paul.hampton@scsc.uk



James Inge
james.inge@scsc.uk



Nikita Johnson
nikita.johnson@scsc.uk



Tim Kelly
Honorary member



Mark Nicholson
mark.nicholson@scsc.uk



Mike Parsons
mike.parsons@scsc.uk



Roger Rivett
roger.rivett@scsc.uk



Emma Taylor
Honorary member



Sean White
sean.white@scsc.uk

Club Positions

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

Managing Director

Mike Parsons 2019-

Tim Kelly 2016-2019

Tom Anderson 1991-2016

Steering Group Chair

Roger Rivett 2019-

Graham Jolliffe 2014-2019

Brian Jepson 2007-2014

Bob Malcolm 1991-2007

Programme & Events Coordinator

Mike Parsons 2014-

Chris Dale 2008-2014

Felix Redmill 1991-2008

Manager

Alex King 2019-

Honorary Solicitor

Dai Davis 2022-

Newsletter Editor

Paul Hampton 2019-

Katrina Attwood 2016-2019

Felix Redmill 1991-2016

University of York Coordinator

Mark Nicholson 2019-

eJournal Editor

John Spriggs 2021-

Administrator

Alex King 2016-

Joan Atkinson 1991-2016

Website Editor

Brian Jepson 2004-

Safety Futures Initiative Leads

Zoe Garstang 2019-
Nikita Johnson 2023-

Nikita Johnson 2019-2021

Calendar

May '23

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

June '23

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

July '23

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

August '23

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

September '23

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

October '23

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

November '23

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

December '23

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

January '24

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 '24

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			

March '24

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 '24

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



25 May 2023
SCSC Working Group

SCSC Safer Complex Systems Working Group meeting

Online, Zoom

scsc.uk/e1033

6-8 June 2023
Course

An Introduction to System Safety Engineering and Management

University of York, UK

www.cs.york.ac.uk/professional/intro-system-safety-engineering-management

12-16 June 2023
Course

Assured Software Engineering and Proof

University of York, UK

www.cs.york.ac.uk/professional/assured-software-engineering-proof

13-14 June 2023
Course

Safety Cases: Safety Arguments for GSN

University of York, UK

www.cs.york.ac.uk/professional/safety-cases-safety-arguments

24 June 2023
SCSC Tech Trip

Visit to the National Space Centre

Leicester, UK

scsc.uk/e1035

29 June 2023
SCSC Seminar

Seminar: Safety Cases: Past, Present and Future

London, UK

scsc.uk/e1032

3-8 Sep 2023
Conference

ESREL 2023: European Conference on Safety and Reliability (ESREL)

University of Southampton, UK

esrel2023.com

28 September 2023
SCSC Seminar

How to Write Compelling Safety Arguments

London, UK

scsc.uk/e982

10-12 Oct 2023
Conference

RSSRail 2023: International conference on reliability, safety and security of railway systems

Berlin, Germany

rssr2023.ebuef.de

17 Oct 2023
Conference

HISC 2023: High Integrity Software Conference

Bristol, UK

www.his-conference.co.uk

1-2 November 2023
Conference

IET SCS: Safety Critical Systems training course: Managing systems, hardware and software safely

Online

safetysystems.theiet.org

13-15 Feb 2024
SCSC Symposium

Safety Critical Systems Symposium SSS'24

Bristol, UK

scsc.uk/e1007

Charisse's view of the Symposium (age 7)

