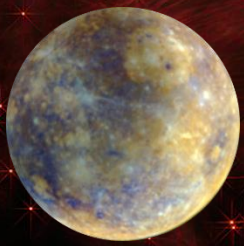
The Safety-Critical Systems Club Newsletter

Safety Systems

Vol 30 No. 3 - Oct 2022

THE SKY IS FALLING!
Assessing the risks from space weather

THERE BE DRAGONS!
Novel approaches to classifying data risks



MATRIX MANAGEMENT
Avoiding pitfalls when using risk matrices

For everyone working in Systems Safety

SCSC

thescsc.org



SCSC Publication Number: SCSC-177

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 2022 except where explicitly stated for specific articles, reports or images.

Cover image: Earth from 141585806 © Bernadett Pogácsás-Simon | Dreamstime.com
Cover image: Background 217802180 © Evgeniy Krasnikov | Dreamstime.com
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

Space Weather: Risks, Challenges and Solutions 5

Dr Jonathan Eastwood discusses the risks and challenges of space weather.

Data Risk Cygnology 13

Mike Parsons and Paul Hampton describe new concepts for describing data safety risks.

Risk Matrices and Pitfalls 21

Lucia Capogna and Stephen Bull provide advice on using risk matrices.

Safety Future Initiative 39

An SFI update from Zoe Garstang and a call for volunteers!

REPORTS

Managing Unexpected Risks 27

The Future of Coding for Safety-Critical Systems 35

DOWNTIME

How Do I Get Into Safety? 41

More insights on how safety careers started from the SCSC Steering Group.

60 Secs with ... Les Hatton 45

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

Recent Publications 47

Recent system-safety related publications and book reviews.

Safety System Crossword 50

Introducing a new prize crossword on the topic of systems safety!

GROUPS

Working Groups 52

Details of the SCSC Working Groups.

SCSC Steering Group 58

Who's who in the Steering Group.

EVENTS

Calendar 60

Events Diary 61

SCSC
FOR EVERYONE WORKING IN SYSTEM SAFETY

www.scsc.uk/sss

SSS'23

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

Safety-Critical Systems Club Annual Symposium

www.scsc.uk

THE SAFETY-CRITICAL SYSTEMS CLUB

31st Safety-Critical Systems Symposium

7-9th February 2023, in-person in York and blended online

The Safety-Critical Systems Symposium in 2023 (SSS'23) will be held in York, UK and blended online as a live-streamed event. This event comprises three days of presented papers, including keynote presentations and submitted papers. There will also be a banquet on the Wednesday evening with additional talks.

This event will be run in-person at the Principal York hotel (located next door to York station) and also online through Zoom and the Whova application.

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

It includes recent developments in the field and progress reports from the SCSC Working Groups. It takes a cross-sector approach and includes the aerospace, automotive, defence, health, marine, nuclear and rail areas.

The symposium features are:

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

And for in-person delegates in York:

- A banquet with after-dinner speaker on the Wednesday;
- Proceedings book and working group guidance books;
- Visit and demonstrations at the University of York Institute of Safe Autonomy;
- Special beer (or non-alcoholic alternative) designed and commissioned for the symposium;
- Safety Activities;
- Social events in York.

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

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

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

Editorial

Last month the nation and indeed, the world, witnessed the passing of Queen Elizabeth II, ending an extraordinary life of public service – the UK's longest-serving monarch and one of the longest ever reigns in global history.

Her life covered almost a century of national and global affairs, spanning 15 UK prime ministers, and it's remarkable to think that while she leaves us now in a society where we have the beginnings of routine space flight, quantum computing and autonomous vehicles, she was born in an era before the electronic television was invented and decades before systems safety was, in any shape, formalised.

Her husband Prince Philip also enjoyed a long life, living to 99, but this might not have been the case when, aged 37, he came perilously close to a life-threating hazard – the like of which we now try so diligently to avoid.

In 1958, he boarded an RAF Sikorsky Whirlwind helicopter travelling the short distance to RAF Patrington across the Humber Estuary. Mid-flight, the co-pilot spotted that the safety wire on the sliding cockpit window had snapped, and the window was moments away from coming off altogether and colliding with the helicopter's tail rotor, with possibly catastrophic results.

The co-pilot acted quickly by grabbing onto the window by bracing – and damaging – his knee to keep it in place as he battled against the aerodynamic forces. By now, over the Humber Estuary, and with no chance to land quickly, there was no choice but to carry on. In considerable discomfort, and with hands numb from the windchill, the co-pilot managed to keep hold as the helicopter made its way to safety.

In a sense this seems an apt metaphor for safety engineering in general. Sometimes we need to hold on doggedly to our safety assessments, designs, mitigations and indeed principles; even when this might be uncomfortable – both at an enterprise and personal level – but hold on we must; even till our hands are numb to avoid the murky waters of disaster that lie below.

In this edition of the newsletter there are three great feature articles, event reports from the "Managing Unexpected Events" and "The Future of Coding" SCSC seminars, an update from the Safety Futures Initiative and the "How do I get into Safety" series returns with insights from a few more members of the steering committee. Our 60 second interview is with Les Hatton who will be the after-dinner speaker at SSS'23.

It also gives me great pleasure to introduce some new features; we now have a "Recent Publications" section where new publications from the SCSC and other relevant sources will be listed and with thanks to Dewi Daniels we have our first ever book review!

To add in some of the fun that we enjoyed with the quiz at SSS'22, I am now including a System Safety crossword into the newsletter; so please try your hand at the questions! All correct answers received by the end of the year will be entered in the hat to win a £50 Amazon Voucher!

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



In Brief



£270k fine after fatality involving mobile elevating work platform



A Lincolnshire based manufacturing company that specialises in lifting and handling equipment has been fined after an employee died after falling with a work platform onto the M25 motorway due to a miscalibration of the vehicle.

The miscalibration occurred through incorrect data being manually manipulated and uploaded onto the machine via a laptop. *hsmsearch.com*

NHS employees warned to expect three weeks of disruption as a result of a cyberattack



A hack on Advanced, a British software and managed services provider with 25,000 customers, has severely disrupted NHS IT systems and may prevent doctors from accessing patients' records for several weeks. *emcrc.co.uk*

KLM 737 used whole runway for take-off after intersection data slip-up



Pilots of a KLM Boeing 737-800 did not amend a runway intersection designation when recalculating take-off performance data for Amsterdam Schiphol, leading the aircraft to accelerate too slowly and use almost the entire runway length before becoming airborne. Dutch investigators have attributed the incident to operational and time pressures. *flightglobal.com*

UK to Have World's Longest Drone Superhighway



The UK government has announced it has given the go-ahead for the world's largest and longest network of drone superhighways to be built in the UK.

The drone superhighway will link cities and towns throughout the midlands to the southeast of the country, with the option to expand the corridor to any other locations in the country. *uasvision.com*



AAIP launch new guidance on the safety of autonomous systems

The Lloyd's Register Foundation-funded Assuring Autonomy International Programme (AAIP) at the University of York have published their latest guidance for the design and introduction of safe autonomous systems. The new research, "Safety Assurance of autonomous systems in Complex Environments (SACE)", marks an important milestone in providing a framework for the regulation and adoption of robotics and autonomous systems across a variety of sectors. *lrfoundation.org.uk*

Space Weather: Risks, Challenges and Solutions



Dr. Jonathan Eastwood discusses the risk of space weather, the evolving challenges it poses, and what is being done to meet those challenges. He explains what is meant by space weather and describes some of its main risk pathways and potential impact on human activity and technology both in space and on the ground. He then assesses the magnitude of the problem and concludes by highlighting some future trends around ensuring that the future of space is safe, secure and sustainable.

Space weather represents a significant threat to modern critical infrastructure and is an important socio-economic risk that has become increasingly prominent in the past two decades in the UK. It is arguably uniquely challenging, because although high-impact events are known to occur, their frequency is relatively low, meaning that society has not experienced a major space weather event in the modern technological era (e.g. the last 20 years). During this time, ever more complex technologies have transformed daily life, and we rely on space-based services in ever more intricate, and surprising, ways.

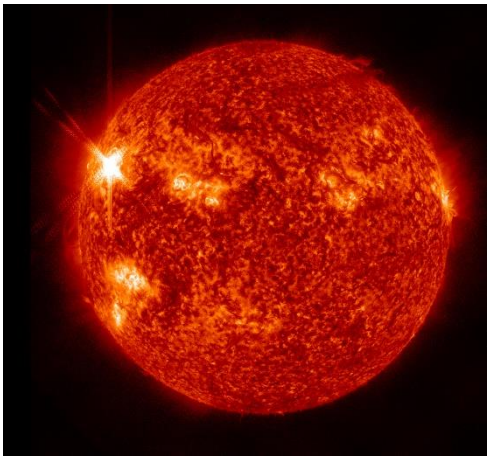
What causes space weather?

In the past 20 years, space weather has risen from being well known in the space science community to a subject that has caught the attention of the wider world to very high political levels [1]. In the UK specifically, space weather is listed on the national risk register [2], cited in the national space strategy [3] and is the subject of a dedicated policy paper on severe space weather preparedness [4].

Broadly speaking, the study of space weather is concerned with understanding how natural phenomena in space can have real and tangible impacts on human activity and technology both in space and on the ground. It is intimately related to the more general study of solar-terrestrial physics, which in itself is part of the field of heliophysics (The NASA Heliophysics Division [5] notes that it 'studies the nature of the Sun, and how it influences the very nature of space – and, in turn, the atmospheres of planets and the technology that exists there.')

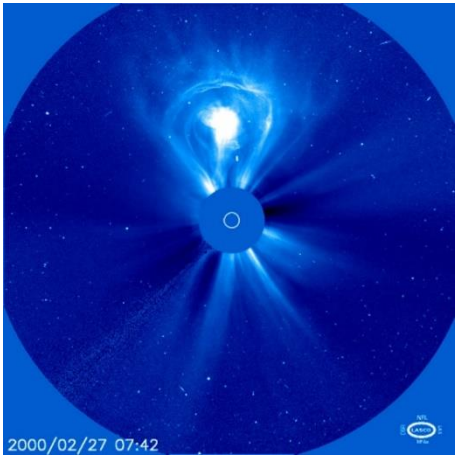
The space weather phenomenon that most people are familiar with is probably the aurora, as illustrated on the previous page by a photograph taken in Alaska. Aurora are seen near the northern and southern poles, and have intrigued and inspired observers for thousands of years.

On occasion, tremendous auroral displays can occur, with vivid and bright features filling the sky. We now understand that these are caused by the Sun. Whilst the Sun appears somewhat featureless and uninteresting when seen at sunrise or sunset, in fact it is an incredibly active and dynamic object, with two main phenomena that interest us here: *solar flares* and *coronal mass ejections* (CMEs).



A solar flare is essentially a flash of light with emission across the electromagnetic spectrum, that lasts of the order of minutes. The image on the right was taken by NASA's Solar Dynamics Observatory and is a false-colour ultraviolet image of the Sun, designed to show the lowest layers of the solar atmosphere. The brighter regions are called *active regions*, which tend to be associated with more variability and stronger magnetic fields in sunspots. The flare is visible on the left-hand side, north of the equator. *Radio blackouts* are primarily caused by solar flares increasing ionisation of the upper atmosphere and distorting/disrupting signals.

A CME is an expulsion of material from the solar atmosphere travelling out through space at speeds of the order of 1000 km/s. The image below was taken by the ESA/NASA SoHO satellite and is a white light image of the solar atmosphere (the corona). The central blue circle blocks direct light from the Sun (outlined as a white circle), allowing the structure of the corona to be seen directly.



The Sun is the source of the solar wind, which is a supersonic stream of material (plasma) that is constantly emitted from the corona at speeds of hundreds of kilometres/second and fills the solar system.

The CME is the lightbulb shaped object at the top of the image, and a time-lapse movie created from many similar images can be used to trace the motion of the CME away from the Sun as part of the solar wind.

Whereas the light travel time to Earth is 8 minutes, and so flares are seen 'immediately', CMEs can take 2-3 days depending on their speed to reach the limit of Earth's orbit. CMEs travel radially from the Sun (more-or-less), and so establishing if a CME is Earth-directed is of critical importance for understanding the space weather risk.

If a CME arrives at Earth, and directly interacts with the Earth's magnetic field in space (the magnetosphere), it can drive a *geomagnetic storm* where energy and material circulates from the CME and solar wind into the magnetosphere. Through a chain of processes best described in terms of plasma physics, energy is stored in the magnetic field and explosively released, accelerating particles into the auroral regions and the Van Allen radiation belts. This causes the bright auroral displays referred to earlier. Of crucial importance is the magnetic structure of the CME. For certain magnetic field orientations, the interaction can be very weak, and little activity arises, but for others, a very strong interaction can occur. CME magnetic field structure can only be diagnosed by in situ measurements made by satellites just upstream of the Earth such as DSCOVR and ACE [6]. Thus, ground truth about whether a CME will cause a significant impact can only be ascertained shortly before they arrive at Earth. Whilst CMEs are the major source of storms, they can also be driven by structure in the background solar wind.

Finally, both solar flares and CMEs are also sources of so-called *Solar Energetic Particles* (SEPs), highly accelerated particles that represent a space weather risk in their own right, being the main source of *solar radiation storms*.

The impact of space weather

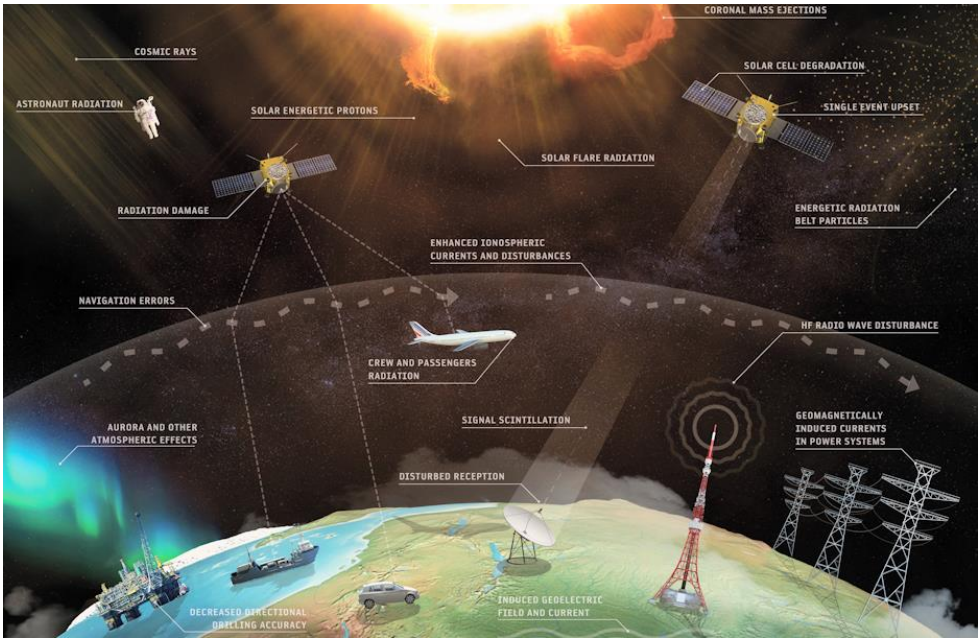
The following figure, produced by the European Space Agency, describes the wide variety of impacts that can arise as a consequence of space weather.

- **Space**: Astronaut radiation, satellite radiation damage, satellite solar cell degradation, satellite single event upset
- **Atmosphere**: Aircraft crew and passengers' radiation, HF radio wave disturbance, signal scintillation
- **Ground**: Decreased directional drilling accuracy, induced geoelectric field and current, geometrically induced currents in power systems

Of primary concern is the *loss of power*. Strong fluctuating currents in the ionosphere (essentially associated with the aurora) induce potential differences and electric fields in the Earth's surface, which can then couple into conducting infrastructure on the ground such as powerlines, pipelines and rail networks.

Of particular note here are the relatively famous events of 13 March 1989 in Quebec, where blackouts and transformer damage occurred as a result of a geomagnetic storm. The 2012 Royal Academy of Engineering report [7] suggests that 6 super grid transformers in England and Wales, and a further 7 in Scotland could be damaged and taken out of service as a consequence of severe space weather.

More recently, the Space Environment Impacts Expert Group's (SEIEG) 2022 Reasonable Worst Case Scenario [8] envisages that premature aging, and damage of transformers could occur, but also that transmission system voltage instability and voltage sag could occur, with tripping of safety systems potentially leading to cascade failure of the transmission network and/or regional outages.



Another important area of impact is in Global Navigation Satellite Systems (GNSS) and position, navigation and timing (PNT) services (eg. GPS). GNSS can be disrupted by distortion to signals as a consequence of ionospheric disturbances driven by space weather. Outages could occur unpredictably and intermittently for several days during a major event, and the impact of this is still not well understood, particularly given the ever-increasing use of PNT services for a variety of downstream services.

Satellite anomalies have been extensively observed as a result of space weather. During what is arguably the last major period of space weather in October/November 2003, 33 Earth orbiting satellite anomalies were reported. Space weather can cause surface and deep dielectric charging, surface damage and solar panel degradation, background counts in sensors, and satellite drag and changes to orbit.

Outages could occur unpredictably and intermittently for several days during a major event, and the impact of this is still not well understood

These issues are thrown into stark relief by the rise of mega-constellations. With the aim of providing high-speed internet access anywhere on Earth, companies such as Starlink, One Web, Amazon Kuiper, Telesat and others offer the potential to transform daily life for billions of people. Starlink has already launched more than 2000 satellites into orbit, and if all planned mega-constellations come to fruition, tens of thousands of satellites will orbit the Earth in the next 10-20 years. Mega-constellations have already been impacted by space weather. In February 2022, a batch of Starlink satellites re-entered after launch because of increased atmospheric drag. In this case, a small geomagnetic storm heated the upper layers of the atmosphere, causing it to expand and increasing the (small) atmospheric density at the initial satellite orbit. This increased the drag on the satellites, slowing them down, and ultimately causing them to re-enter.

Finally I note that air travel is also subject to space weather considerations. For example, polar flights have been required to divert, because HF radio communications near the poles were disrupted by space weather. ICAO regulations now require space weather advisory information to be provided to the international aviation community.

Understanding, addressing and mitigating space weather risks

Space weather is a very difficult problem to assess. Firstly, the historical record shows that very severe events can happen, but they have not really happened in the modern era. A major event, such as experienced in 1859 (the so-called Carrington event) and with a return period of approximately 100 years, is expected to have a very significant impact on a wide variety of technological systems. Smaller events happen more frequently, and power-law behaviour is a feature of probability distributions describing various space weather phenomena.

It is highly likely that system failures will interact with each other to cause cascading failure modes that are fundamentally difficult to predict, and this is an area of research that has not received a great deal of attention

Secondly, each interval of severe space weather is unique, because it is ultimately driven by solar activity and so different combinations of flares, CMEs and solar energetic particles may occur depending on the underlying solar drivers.

The Sun's rotation period means that from the point of view of the Earth, an active region will take about two weeks to transit across the solar disk, and in a severe space weather period, one may expect a two-week interval of elevated risk, during which time several different types of phenomena could occur in unknown order, severity, etc. It is highly likely that system failures will interact with each other to cause cascading failure modes that are fundamentally difficult to predict, and this is an area of research that has not received a great deal of attention, in part because of the complexity involved.

A third challenge to understanding space weather is that it is very much impact-led and driven by a desire to reduce the socio-economic footprint. Therefore, the appropriate response is a calculation that is fundamentally risk based, considering the exposure, vulnerability and hazards. This calculation is also dynamic, in the sense that as some risk is retired (for example through engineering and design choice), new risks can be introduced (such as the dramatic increase in the use of PNT services, and the wider interest in e.g. driverless cars).

This is related to the question of space weather impacts on internal organisational activity and business resilience. Many organisations are not aware of their reliance on space infrastructure, or internal exposure to space weather issues. Similarly, organisations may not be aware of how their products and services may be exposed to space weather impacts. This exposure could arise at many points and could be of particular importance where certain levels of service are guaranteed.

Here, it is typically necessary for the analysis to be client-led, where the specific organisation enlists the help of expert groups or space weather service providers to understand what

risks might be in play. It is important to recognise that space weather may well turn out not to be a major issue, but it is still necessary to investigate the possibilities as the unique nature of the space weather hazard means that surprising impacts may be identified.

The Future

At the national and international level, considerable efforts have been made to improve our ability to monitor and forecast space weather. In the UK, the Met Office is the 'owner' of the space weather risk, and operates the Met Office Space Weather Operations Centre (MOSWOC) [9] that provides 24/7 space weather forecasting. In the US, NOAA's Space Weather Prediction Center plays a similar role, and ESA's Space Safety office enables comparable space weather service provision.

Space weather forecasting relies on data and modelling, and whilst there are several satellites monitoring the Sun and the near-Earth space environment, there are plans to develop a new generation of observers, such as ESA's Vigil [10] space weather mission, that will provide new capabilities improving forecast quality and reliability. New generations of space weather models are being produced, in the UK the Space weather innovation, measurement, modelling and risk (SWIMMR) programme [11] funded by UK Research and Innovation is delivering new capabilities from the academic community into operational use at the Met Office.

Finally, space is a critical national infrastructure, and space weather is part of a wider drive to ensure the future use of space is safe, secure and sustainable. Work by the Space Lab network of excellence at Imperial College London has identified 5 key areas in this regard [12] – the terrestrial environmental impacts of space activities, space debris, planetary defence, space weather and space traffic management.

In particular, the impact of mega-constellations cannot be ignored, as they bring multiple issues about space safety, security and sustainability into sharp relief, raising many questions about policy and regulation.

Summary

Looking to the future, our use of space is transforming rapidly, and the benefits it brings has already changed many aspects of daily life. As organisations become ever more aware of how space technology is inextricably woven into the fabric of everyday life, the demand for knowledge about space weather is only likely to grow; where this touches on safety-critical systems, this may be particularly important. I hope this article will help raise awareness in the wider safety community about the risks of space weather, the challenges it poses, and what is being done to meet those challenges.

References

[1] The Economic Impact of Space Weather: Where Do We Stand? Eastwood et al., *Risk Analysis*, Volume 37, Issue 2, pg 206, 2017 https://dx.doi.org/10.1111/risa.12765

[2] UK National Risk Register 2020, https://www.gov.uk/government/publications/national-risk-register-2020, accessed Sept 2022

[3] UK National Space Strategy (Feb 2022), https://www.gov.uk/government/publications/national-space-strategy/national-space-strategy, accessed Sep 2022

[4] UK Severe Space Weather (Sep 2021) Preparedness Strategy, https://www.gov.uk/government/publications/uk-severe-space-weather-preparedness-strategy, accessed Sep 2022

[5] NASA Heliophysics Division, https://science.nasa.gov/heliophysics, accessed Sep 2022

[6] DSCOVR https://solarsystem.nasa.gov/missions/DSCOVR/in-depth and ACE https://solarsystem.nasa.gov/missions/ace/in-depth, accessed Sep 2022.

[7] Extreme space weather: impacts on engineered systems and infrastructure, https://raeng.org.uk/media/lz2fs5ql/space_weather_full_report_final.pdf, RAEng, 2013

[8] Summary of space weather worst-case environments (3rd revised edition), https://epubs.stfc.ac.uk/work/51273983, SEIEG, 2022

[9] MOSWOC, https://www.metoffice.gov.uk/weather/learn-about/space-weather/met-office-role, accessed Sep 2022

[10] Vigil, https://www.esa.int/Space_Safety/Vigil, accessed 2022

[11] Space weather innovation, measurement, modelling and risk (SWIMMR), https://www.ukri.org/what-we-offer/our-main-funds/strategic-priorities-fund/space-weather-innovation-measurement-modelling-and-risk, accessed Sep 2022

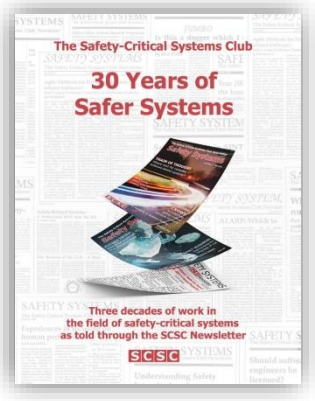
[12] Space Lab evidence-based policy reports, 2020, 2021 https://www.imperial.ac.uk/a-z-research/space-lab/research/

Image Attribution
Northern lights over the Poker Flat Research Range, Alaska USA 16/02/17 Credit: NASA/Terry Zaperach
Solar flare observed by NASA's Solar Dynamics Observatory 03/11/11 Credit: NASA
Coronal mass ejection observed by the LASCO coronagraph on ESA's SoHO Credit: SOHO ESA & NASA
ESA space weather effects graphic © ESA/Science Office CC BY-SA 3.0 IGO

Dr. Jonathan P. Eastwood, Reader in Space Physics, Imperial College London

Dr Jonathan Eastwood is a Reader in Space Physics in the Department of Physics' Space and Atmospheric Physics group at Imperial College London. His research interests include space weather, space plasma physics, and developing novel miniaturised instrumentation for space weather monitoring. He also serves as Director of the Space Lab Network of Excellence, which brings together all of Imperial's space capabilities under one network.

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



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

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

Available for purchase on Amazon
www.amazon.co.uk/Years-Safer-Systems-safety-critical-Newsletter/dp/B09KNCYKDL

SCSC
FOR EVERYONE WORKING IN SYSTEM SAFETY

The Future of Testing for Safety Critical Systems

THE SAFETY-CRITICAL SYSTEMS CLUB

The Future of Testing for Safety Critical Systems

Thursday 1 December, 2022 - London, UK and blended online

This 1-day seminar will examine how safety-critical systems are tested, some types of testing techniques and the resulting issues. It will also cover emerging technologies, including testing systems including AI and machine learning components. It will cover tools, techniques and limitations of testing methodologies. It will also cover some historical failures of testing and the lessons learnt.

Data Risk Cygnology



Black Swans, Perfect Storms, Dragon Kings and Pudding Lanes – sound like plot elements of an elaborate fantasy novel! However, these are concepts that are relevant to system safety and describe different ways in which events can conspire and lead to catastrophic outcomes. Mike Parsons and Paul Hampton explain four of these concepts from a data perspective.

Black Swan Data

Data that is totally unexpected by those receiving it (i.e. 'out of the blue') and has huge (detrimental) impact, but in retrospect should have been anticipated



In 2013 a C-130 Hercules aircraft landed at Bar Yehuda airport near the Dead Sea [1], a saltwater lake sitting astride Israel and Jordan. The Dead Sea is the lowest place and the airfield lies -1,210 feet below sea level.

The aircraft's navigation system became unresponsive and the constellation of GPS satellites above, mysteriously winked out of existence. As it turned out, the plane's navigation electronics were not designed to operate at altitudes less than 400 feet below mean sea level. In a sense, the plane thought it was underwater!



This is what we call a "Black Swan Data" event; the stream of altitude data going to the navigation systems surprisingly turned significantly negative and could have had a catastrophic result; a situation not considered possible. Yet, with hindsight, and knowledge of earth's geography, we can rationalise this and question why the assumption of positive altitude data was ever thought to be true in the first place.

Might your system be susceptible to Black Swan Data? Presumably not something by its very nature that has been considered; but what can be done to protect against it?

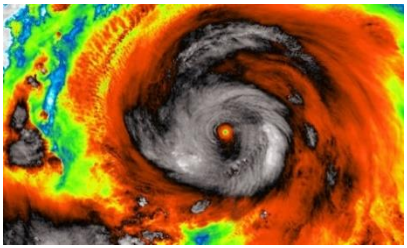
This is an area for further study, but we can offer the following suggestions:

- Be aware of changes of usage, environmental conditions or failures that may produce data that is not expected. The Ariane 501 launch disaster may be thought of in these terms, as the horizontal bias values that caused the exception leading to the complete loss of mission were not anticipated.
- Continually test the established thinking; challenge the oft quoted "that's just how we do things around here".
- What assumptions have we made about the data? Are these really valid and do they continue to be valid in a changing and dynamic world?
- What happens if different inputs (e.g. new sensors or information flows) are added to your system?
- Think outside the box; and we mean, really outside the box. It is the most wild and implausible (compared to current perceptions) ideas that will trip a Black Swan Data event – what could possibly be 'bad data' and how might we handle it?



Perfect Storm Data

Combinations, sets or occurrences of data (or absences of data) that would never have been thought possible to occur together, and when they do have a large and undesirable impact



A Perfect Storm in the risk world is when everything bad happens at the same time, and you did not anticipate that this could happen. These risks get their name from The Perfect Storm, both a 2000 American biographical disaster drama film [2] and a 1997 non-fiction book by Sebastian Junger [3].

In the data world a Perfect Storm is when the data that your system relies upon are all wrong (or missing) at the same time: it can be layers deep. A classic example might be to try and restore deleted data from a backup system, only to find that the backups had not been working properly due to a configuration problem.

So Perfect Storm Data is when multiple data faults or losses conspire to create a situation that has disproportionately catastrophic outcomes.

Another example might be from security: on 10th Dec 2021 a new critical zero-day vulnerability [4] was detected that affected Apache Log4j 2 Java library. It adversely impacted the digital domain and security systems worldwide. The vulnerability, when exploited, permitted remote code execution on the vulnerable server with system-level privileges. The exploit was a combination of both the Java code that contains different logging functions and the settings of a configuration file.

Another example might be the China Airlines A333 at Taipei on 14th June 2020 [5] when all primary computers, reversers and auto brakes failed on touchdown. During landing, flight controls reconfigured from 'normal law' to 'direct law' after all three flight control primary computers (FCPCs) became inoperative. While all aircraft primary control surfaces were still controllable, the deceleration devices including ground spoilers, thrust reversers, and autobrake were lost; the deceleration of the aircraft had to be performed by manual brake.

The following might be considered for management:

- Analyse combinations of data that are important to you: how might one data set being wrong influence another?
- Look at dependencies in your data: are seemingly different sets all derived from a common source?
- Examine as many levels of system and data as you can to establish commonalities and dependencies
- Even if no commonalities are found, consider the unlikely cases of independent data being wrong together, and follow through their consequences
-



Pudding Lane Data

Data which is unknowingly and unexpectedly critical to the whole operation and if missing or incorrect in some way has a dramatic and negative impact. After the event it may be obvious that it was critical.

"Lord! what sad sight it was by moone-light to see, the whole City almost on fire, that you might see it plain at Woolwich, as if you were by it".



With these words from Samuel Pepys diary in 1666 [6], we see the account of the Fire of London that destroyed 13,200 houses, 87 parish churches, The Royal Exchange, Guildhall and St. Paul's Cathedral, all from a single fire thought to have started in a humble baker's shop in Pudding Lane.

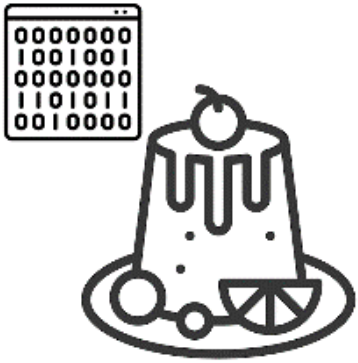
In the same way, unexpectedly critical data can also act as a catalyst to catastrophic outcomes if the dependencies are not identified and adequately mitigated. Often this data is part of an existing system and may be long forgotten about (e.g. a system configuration parameter). It may also be a hard-wired parameter in legacy source code which the maintainers of the code change because they do not understand its original purpose.



In 2015, an Airbus A400M Atlas cargo plane on a test flight crashed at La Rinconada, Spain, less than 5 kilometres from Seville Airport, killing 4 of the 6 crew [7]. Several reports suggested that as many as three of the aircraft's four engines failed during the A400M's departure from Seville.

The suspected cause of the failure was that the torque calibration parameter data had been accidentally wiped on three engines as the engine software was being installed, which would prevent the engine control software from operating properly. In this case, the seemingly innocuous calibration data had a critical role to play in the safety of the entire platform and we introduce the term "Pudding Lane Data" to encompass this form of data. We suggest the following considerations for this type of data:

- Understand and know all your data. The high profile data streams will of course be first and foremost, but do you have an inventory of all the data that the system depends upon and the implications if there is loss of their data properties?
- Configuration and tailoring data may seem static and uninteresting but what are the dependencies on this data? If loss of properties of this data can have catastrophic outcomes, then what processes and mitigations will you put in place to assure those properties are maintained?
- Consider the reporting and monitoring data: if this is incorrect will poor decisions be taken?



Dragon King Data

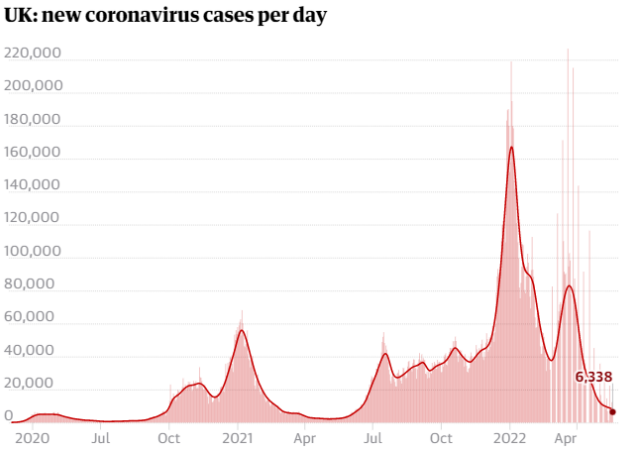


Data whose effect might have been foreseen, but leads to an unexpected and explosive escalation with major impact ('things get rapidly out of control').

In risk management a Dragon King is defined as an event that is both extremely large in size or impact (a "king") and born of unique origins (a "dragon") relative to other events in the system.

Dragon King events are generated by, or correspond to, mechanisms such as positive feedback, tipping points, bifurcations, and phase transitions that tend to occur in non-linear and complex systems, and serve to amplify events to extreme levels. In the data domain we introduce "Dragon King Data", to represent incorrect or missing data whose consequences unexpectedly escalate into an unpredicted and often catastrophic system event.

An example might be the loss of data relating to Covid-19 test results in the UK due to a row limit in Microsoft Excel. This led to Public Health England losing 15,841 positive test results which in turn meant that 50,000 potentially infectious people were missed by contact tracers and not told to self-isolate [8]. Because of the exponential way that viruses spread, this may have led to many more infections and deaths.



Another, older, example could be the infamous comment given by the weather forecaster Michael Fish about the Great Storm of 1987 [9]:

> *"Earlier on today, apparently, a woman rang the BBC and said she heard there was a hurricane on the way. Well, if you're watching, don't worry, there isn't!"*



These few words may well have led to precautions not being taken across the whole of Southern England, affecting millions of people. In fact the storm was the worst to hit South East England for three centuries, causing record damage and killing 19 people.

Some ways this can be managed are:

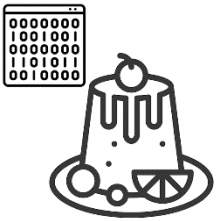
- Identify all the receiving systems or users of your data: what are the consequences of errors or losses in the data to those receiving it?
- Analyse the effects of data impact: are any effects subject to non-linear effects? Try to establish the consequence chains and knock-on effects
- Do any of your data potentially impact systems that have large fan-out or spread?
- Create models (or even Digital Twins) of the system in a way that different combinations of data can be tested and simulated to reveal extreme non-linear behaviours



Conclusions

Looking at Data Risks this way can help to tease out some unlikely but severe failures of systems involving data. It is possible that sometimes these risks are already considered in system Hazard and operability study (HAZOP) sessions but discounted as too unlikely to happen. We suggest this approach is a useful and visual 'Tool in the Box' when trying to identify extreme data-related risks of systems. Due to their serious impact we argue that they should be included, assessed and managed alongside more 'normal' risks.

Summary Table

Type	Brief Explanation	Icon
Black Swan Data	Data that is totally unexpected by those receiving it (i.e. 'out of the blue') and has huge (detrimental) impact, but in retrospect should have been anticipated.	
Perfect Storm Data	Combinations, sets or occurrences of data (or sets of absences of data) that would never have been thought possible to occur together, and when they do have a large and undesirable impact.	
Pudding Lane Data	Data that is unknowingly and unexpectedly critical to the whole operation and if missing or incorrect in some way, has a dramatic and negative impact. After the event it may be obvious that it was critical.	
Dragon King Data	Data that might have been foreseen, but leads to an unexpected and explosive escalation with major impact ('things get rapidly out of control').	

References

[1] C-130 Crew Gets a Rude Shock When They Fly Their Plane Below Sea Level, https://www.popularmechanics.com/military/aviation/a26598/c-130-sea-level-dead-sea, accessed August 2022

[2] The Perfect Storm, https://www.imdb.com/title/tt0177971, accessed August 2022

[3] The Perfect Storm: A True Story Of Man Against The Sea, Sebastian Junger, https://www.amazon.co.uk/Perfect-Storm-True-Story-Against/dp/0007230060, accessed August 2022

[4] NCSC Alert: Apache Log4j vulnerabilities, https://www.ncsc.gov.uk/news/apache-log4j-vulnerability, accessed August 2022

[5] A China Airlines Airbus A330 Lost Primary Computers After Landing, https://simpleflying.com/china-airlines-a330-lost-computers, accessed August 2022

[6] The Diary of Samuel Pepys, https://www.pepysdiary.com/diary/1666/09, accessed August 2022

[7] 2015 Seville Airbus A400M crash, https://en.wikipedia.org/wiki/2015_Seville_Airbus_A400M_crash, accessed August 2022

[8] PHE statement on delayed reporting of COVID-19 cases, https://www.gov.uk/government/news/phe-statement-on-delayed-reporting-of-covid-19-cases, accessed August 2022

[9] Quotes of famous people, https://quotepark.com/quotes/1829009-michael-fish-earlier-on-today-apparently-a-woman-rung-the-bbc, accessed August 2022

Image attributions
Top image © Jpldesigns | Dreamstime.com
C-130: © Mr Paul Hanley | Dreamstime.com
A400M © Abhishek Singh | Dreamstime.com
Storm © Zenobillis | Dreamstime.com
Fire © Eric Flamant | Dreamstime.com
Swan © Jerome Whittingham | Dreamstime.com
swan icon: © Skalapendra | Dreamstime.com
Michael Fish from Wikipedia published under the fair use license
Covid chart: data.gov.uk published under the Government OGL license v3.0
storm icon: © Андрей Морозюк | Dreamstime.com
pudding icon: © Amonrat Rungreangfangsai | Dreamstime.com
dragon icon: © Kuzzie | Dreamstime.com
binary code: © Webtechops Llc | Dreamstime.com
Log4J logo © Apache Software Foundation,licensed under: https://www.apache.org/licenses/LICENSE-2.0

Mike Parsons, SCSC DSIWG Chair

Mike is the SCSC Director and Events Coordinator. He also leads the SCSC Service Assurance, Data Safety Initiative and the new Systems Approach to Safety of the Environment Working Groups. He is currently a researcher at the University of York working on the Assuring Autonomy International Programme (AAIP). He has been in the business of safety since 1989.

Paul Hampton, SCSC Newsletter Editor

Paul is a Chartered Engineer with over 30 years' experience in IT. He has spent 15 of those designing and developing enterprise systems in many diverse sectors and the remainder involved in system safety in a variety of capacities including: safety engineering, safety management, independent auditing and corporate governance and assurance.

Risk Matrices and Pitfalls



Risk is a concept we implicitly understand as human beings, and we discuss and evaluate it in many situations on a day-by-day basis. But what is the actual definition of risk? And what is considered an acceptable/tolerable risk? Does this concept change depending on the context, or has it an absolute meaning? How do we represent the risk? Lucia Capogna and Stephen Bull explore these questions and provide advice on some of the pitfalls that may be encountered when categorising and treating risk.

Risk definition – a reminder



In this article we will try to answer the questions around risk and present one of the possible representations and method for risk ranking: the risk matrix. Examples, types of matrices, their calibration and the main pitfalls are also discussed.

The International Electrotechnical Vocabulary (IEV) defines risk as "combination of the probability of occurrence of harm and the severity of that harm".

This definition has been adopted by many standards, including EN 61508-4:2010 and ISO 26262-1:2018.

A slightly deviation from this definition of risk is documented in the EN50126-1:2017, where "risk, <for railway RAMS>," is defined as "combination of expected frequency of loss and the expected degree of severity of that loss".

Thus, "risk" can be seen as a two-dimensional concept, where the two dimensions are the probability or frequency of occurrence of an event and the severity of the consequence of that event.

What is a risk matrix?

A Risk Matrix is a common method used for risk ranking or categorisation.



A Risk matrix is defined by Cox (2008) [1] as "a table that has several categories of "probability," "likelihood," or "frequency" for its rows (or columns) and several categories of "severity," "impact," or "consequences" for its columns (or rows, respectively)".

There are three types of risk matrices:

- qualitative risk matrix: the items on the axes of the matrix are defined with qualitative or descriptive terms (not numerical)
- quantitative risk matrix: the items on the axes of the matrix are defined in quantitative or measurable terms (numerical)
- semi-quantitative matrix: it is a combination of the qualitative and quantitative matrices. One of the axes can be defined qualitatively and the other one is expressed quantitatively (or one or both axes could be defined both qualitatively and quantitatively).

This is an example of a qualitative risk matrix (although it could be made quantitative by defining ranges for the descriptive frequency and severity labels).

Frequency of occurrence of an accident (caused by a hazard)	Risk Acceptance Categories			
Frequent	Undesirable	Intolerable	Intolerable	Intolerable
Probable	Tolerable	Undesirable	Intolerable	Intolerable
Occasional	Tolerable	Undesirable	Undesirable	Intolerable
Rare	Negligible	Tolerable	Undesirable	Undesirable
Improbable	Negligible	Negligible	Tolerable	Undesirable
Highly improbable	Negligible	Negligible	Negligible	Tolerable
	Insignificant	Marginal	Critical	Catastrophic
	Severity of an accident (caused by a hazard)			

For reference, CENELEC, EN 50126-1:2017 Annex C [5] gives an explanation of risk matrices (although no guidance on their calibration).

Where are risk matrices used?

Risk matrices, independently from the type, are commonly used to rank/categorise risks in a hazard log to prioritise effort and/or to single out high risks for further attention.

Later in the lifecycle they are used to accept risks in a hazard log.

Risk matrices are also used in many other fields than safety to determine the acceptability of other types of risks, e.g. they are also used for determining the acceptability of the operational, security, reputation and environment risks.

Example risk matrices

Examples of risk matrices can be found in many standards or codes of practice applicable to different industries or sectors, but also in guidance created for specific projects (usually where the project is complex or high profile).

With regards to the railway industry, an example risk matrix can be found in the EN 50126-1:2017 standard. This has been also reproduced in the Network Rail (NR) guidance on CSM-RA. Project-specific examples include the recently opened Crossrail in London; many other examples or guidelines can be found.

Other examples can be found in the Defence Industry:

- the Regulatory Article 1210 (RA 1210) issued by the Military Aviation Authority and specific for the ownership and management of operating risks, and
- the MIL-STD-882E issued by the US Department of Defence. This standard identifies the Department of Defence (DoD) approach for identifying hazards and assessing and mitigating associated risks encountered in the development, test, production, use, and disposal of defence systems.

Pitfalls in the definition and the use of risk matrices



When looking into the definition of risk matrices, we should consider that there are multiple exposed populations in different roles (e.g. workers and passengers) and the (perceived) risk appetite may be different for each. Thus, the risk matrices specific for each population are likely to be different. (For example, the UK HSE document Reducing Risks, Protecting People (R2P2) [3] assigns different targets for workers and members of the public.)

The judgement around the frequency, the severity or the risk appetite is often subjective and dependent on the experience of the people involved in their definition/calibration, in hazard workshops and in hazard review meetings.

In addition, the risk matrices definition should not be a standalone exercise but should consider the big picture (including applicable law or regulations and possible contradictions), otherwise across the same project/programme or domain the adopted risk matrices may be inconsistent. This does not mean that risk matrices for different operational aspects should be identical, but that it is very important they are compatible.

This should be also considered when different organisations are involved in the same programme. A supplier/subcontractor may have their own risk matrix which is not (necessarily) aligned to the programme / operator's matrix. The specific project scope (or portion of the project scope) should be considered in the risk matrix definition, as the overall risk matrix may be not adequate for the scope of the analysis or the sub-system. This adds additional burden to the entity in charge of the integration and responsible to "import" the contribution from a different matrix with possible transformation consequence.

This practice attracted criticism from the Haddon-Cave report into the Nimrod XV230 crash [2], which said "There are a myriad of different Hazard Risk Matrices used to determine risk categorisations. This is confusing, potentially dangerous, and makes it more difficult to compare risks across platforms", and we share that view that multiple risk matrices can cause confusion. However, for the reasons presented in this paper it is essential to calibrate matrices to the individual application. It is also essential that the reasons for different matrices are clearly justified and that care is taken to ensure that matrices used within the same project or programme reach consistent conclusions on the level of risk.

When using a risk matrix, it is also fundamental to consider the level of detail at which individual events are assessed. If the risk matrix is calibrated (see below) to consider hazards at the boundary of a system then separate assessment of the individual causes of the hazard (each representing a smaller portion of the overall risk) may lead to the false conclusion that the risk is acceptable. This needs to be taken into account:

- when deriving a risk matrix for a particular programme/project and
- when applying the risk matrix to individual hazards.

When using the risk matrices to rank risks, there are a few other areas that can lead to misuse or misinterpretation of the risk matrices too. For example, the link between tolerable and ALARP. There is the misconception that a tolerable risk is automatically ALARP. However, they are two different concepts: it is still necessary (and legally required in the UK) to demonstrate that all practicable measures have been taken to reduce the risk (ALARP). Hence, a risk matrix cannot be used on its own to declare that a risk is ALARP!

"There are a myriad of different Hazard Risk Matrices used to determine risk categorisations. This is confusing, potentially dangerous, and makes it more difficult to compare risks across platforms." (Haddon-Cave)

Another important pitfall in the use of risk matrices is the understanding and interpretation of the risk matrix axes.

The frequency of occurrence can be understood as "frequency of the Event (often the hazard) that might lead to the consequence" or the "estimated frequency of the Consequence". Many people do not understand the difference and mix them up in the same analysis. Instead, the consequence may be understood as the "worst case consequence" or the "most likely reasonably foreseeable consequence". It is very important to not mix up these concepts in the same analysis and understand the difference in their interpretation.

Sometimes standards and codes of practice may help in solving this. For example, in the railway sector a clear definition of the axes is documented in the EN 50126-1:2017, that states that the axes should be interpreted as the frequency and consequence of the accident arising from the hazard.

Another aspect to consider is the "additionality": if the scope of the programme is increased during its execution, then an amount of extra risk is likely to be added: depending on the nature of this risk, the risk matrix may need recalibrating and existing risks may need re-evaluating.

For further information, RSSB, Taking Safe Decisions, 2019 [4] provides useful principles on how to evaluate safety of a system.

Calibration

It is possible to calibrate a risk matrix from "first principles", taking into account that there are lots of issues and shortcomings. Often this calibration is necessary to ensure that the matrix is appropriate for the project.

When the risk is derived from a generic (overall) target, the calibration of the risk matrix must consider the scope of the analysis and how much of the overall risk can reasonably be assigned to the system under consideration.

The calibration should also consider the level of the risk assessment, i.e. if the scope is the assessment of individual hazards, then only a proportion of the risk budget (i.e. the tolerable level of risk for the overall system) is available per hazard and the risk matrix needs to be scaled accordingly.

For further reading on calibration, GE/GN8642 Issue 2 (withdrawn, but available from RSSB) (Appendix C) provides some guidance on calibrating a risk matrix [6].

Conclusions

The use of the risk matrices is considered an "easy" approach and for this reason they are very often overused or abused.

In reality, they are not really so easy to use, as they require to be calibrated to their particular application and there are many possible pitfalls in their use or definition.

Risk matrices can be a useful tool to quickly assess risks if properly customised / calibrated, however there are contexts where the use of risk matrices is not appropriate and alternative techniques are available.

Any use of a risk matrix should be accompanied by expert judgement as to the suitability and relevance of the outputs; it must also consider the context and the possible misuses and misinterpretations. Perhaps any risk matrices should come with a comprehensive set of assumptions and warnings!

References

[1] Cox Jr., "What's Wrong with Risk Matrices? Risk Analysis 28", L.A. 2008

[2] Charles Haddon-Cave QC, "The Nimrod Review - An independent review into the broader issues surrounding the loss of the RAF Nimrod MR2 aircraft XV230 in Afghanistan in 2006", Oct. 2009

[3] HSE, Reducing Risks, Protecting People (R2P2), 2001: HSE's general approach to risk management, including the "carrot diagram" and overall targets for acceptable risk

[4] RSSB, Taking Safe Decisions, 2019: gives principles about how to evaluate safety of a system

[5] CENELEC, EN 50126-1:2017 Annex C: gives an explanation of risk matrices (no guidance on their calibration)

[6] GE/GN8642 Issue 2 (withdrawn, but available from RSSB) (Appendix C) provides some guidance on calibrating a risk matrix

Image attribution
top image 99257674 © Alphaspirit | Dreamstime.com
risk 114395146 © Anyaberkut | Dreamstime.com
risk matrix 175934678 © Elnur | Dreamstime.com
pitfall 48702118 © Alexmillos | Dreamstime.com

Lucia Capogna, Principal Engineer, Ebeni Limited

Lucia has over 15 years' experience in software, safety and cyber security with background in multiple industries including Railway, Defence, Oil & Gas and Renewable Energy. Lucia also represents the UK in several CENELEC and IEC standardisation groups for software, cyber security and safety standards.

Stephen Bull, Principal Safety Engineer, Ebeni Limited

Stephen has over 25 years' experience in the development and assurance of safety critical systems in a variety of industries, including rail, defence and air traffic control. He is a Chartered Engineer and a Fellow of the Safety and Reliability Society.

Managing Unexpected Risks Event Report

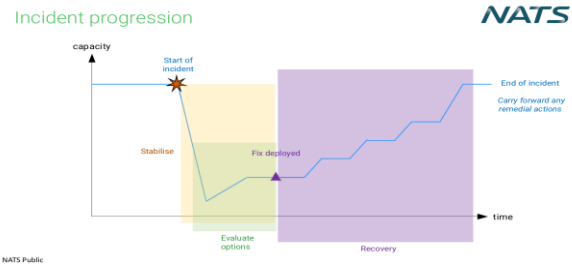


The Seminar "Managing Unexpected Risks: Handling Rare and Severe Events Now and in the Future", took place in person at the BCS offices in London and online on 26th May 2022. Paul Hampton and Martin Atkins provide the highlights of the event.

The event opened with Mike Parsons, SCSC Managing Director, introducing the concepts of 'Black Swans'. He said that increasingly complex systems and new technologies like autonomous vehicles are presenting new opportunities for the occurrence of Black Swan events.

Managing Novel Incidents

The first presentation was by John Holmes from NATS, the UK air traffic service provider, on the topic of Managing Novel Incidents. John talked about an incident associated with a well-established system.



Traffic was low due to an overnight storm and there was an intermittent fault with a radar display system in the morning resulting in delays. Intermittent low-level packet loss was being experienced on a network switch, but it was decided not to replace it, because of the storm. However, a

switch on the redundant network then also failed, resulting in track data blocks – data associated with the trails displayed on Air Traffic Control (ATC) displays – being intermittently lost.

To deal with the situation, NATS implemented traffic control methods, by reducing the number of aircraft taking off. The fault was diagnosed and a fix was completed in around 4 hours.

There is a mature hierarchical incident management system at NATS and incidents are escalated based on the level of impact. This is well-exercised through training. However, analysis of the event found that:

- There was loss of a single point of truth between ATC and Engineering
- Focus was on the controller positions but less on other affected systems connected to the same network
- There was inconsistent use of language and communication between different stakeholders
- There was insufficient recording of the decision-making process to provide evidence that the correct actions had been taken

Although the team arrived at what proved to be the correct course of action, these good decisions were not an inevitable product of the process.

Following an investigation, NATS developed a more prescriptive process for evaluating options for risks, benefit and trade-offs and a set structure for recording decision rationale. This was based around a structured series of questions, but was not adopted in the end, as it was felt to be cumbersome and risked stifling the flexible and reactive nature of the more informal problem solving approach.

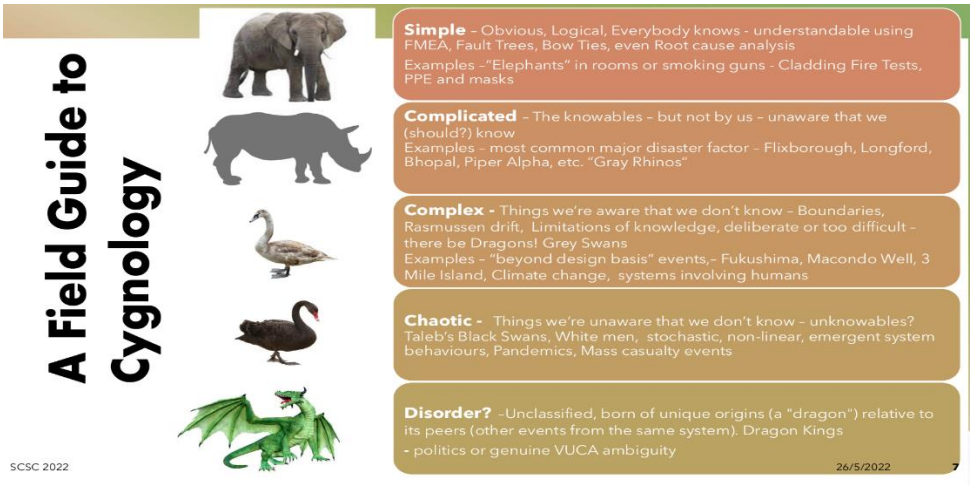
It was acknowledged that there is heavy reliance on highly trained, skilled, adaptable and empowered people and NATS decided to create a better training programme for staff to ensure there is a clear framework for necessary discussions, retaining flexibility and pace.

Black Swans - Decisions under Uncertainty

David Slater from Cardiff University presented on the importance of instinct, experience, and time for thinking in emergencies.

"Normal" emergencies are usually well-handled as the system is well understood but 'black swans' are different as we are dealing with the 'Unknown Unknowns' as famously expressed by Donald Rumsfold.

David introduced a range of complexity categorisations from Obvious or Simple (the known), Complicated (the knowable), Complex (the unknowable), Chaotic (incoherent), Disorder (not determined). He introduced a 'Cygnology' for these systems and gave examples: for Complicated emergencies, he gave examples of Bhopal and Piper Alpha and for Chaotic emergencies, he gave Black Swan events, such as Pandemics.



The Cynefin framework helps the decision-making process but David noted that there can be drift between quadrants (Rasmussen Drift).

David gave further examples of Simple, Complicated and Complex accidents and gave examples of real Black Swans in the Chaotic category such as 9/11, Covid-19 and the shelling of Ukrainian Nuclear Power stations.

David then went on to discuss what we can do about managing these types of events. There is acceptance that Chaos does happen, we live in a complex environment, but we have evolved to survive in these environments. Planning and training are seen as important but is 'robotic' Plan Do Check Act (PDCA) methodologies sufficient? David discussed other models such as John Boyd's OODA loop (Observe, Orient, Decide and Act). Klein also had a model called Recognition Primed Response. But the real question is whether there is time to think logically or read the manual during a crisis.

David also referred to Kahneman's thinking 'fast and slow' with system 1 being automatic and little or no effort and no sense of voluntary control. System 2 allocates attention to the effortful mental activity.

He referred to Libet's experiment and the complexity of the brain.

David noted how people respond differently to emergency situations and referred to the Fukushima Daini (No 2) plant which survived a similar set of problems to the Daiichi (No 1) plant that experienced the well-publicised meltdown. The No 2 plant was saved due to innovative human ingenuity to help route power after the flooding by the tsunami. David thought that AI systems can help in the simple or more complicated systems, but their inflexibility could limit their utility in more complex situations.

David concluded that the instinct, experience and time for thinking in emergencies is critical. It's important to have more than just classroom-based training, there should be empowerment of those responsible, leadership not micromanagement, team leading and building resilience.

The Buncefield Explosion

Martin Atkins from MCA Ltd discussed the events surrounding the Buncefield Explosion. He defined a Black Swan as an event that is a surprise, has a major impact and in hindsight, is rationalised as predictable.

He stressed however, that Black Swans are very much 'in the eye of the beholder' and relative to role an affected party plays in an incident.

The Fuji Building



Martin discussed the Buncefield Site in 2005, an Oil Storage Terminal near Hemel Hempstead, the 5th largest oil storage depot in the UK with a capacity of 60,000,000 gallons and filling ~400 tankers a day.

Each tank had 3 indicators if it was full: a gauge, another (which was not operating at the time) and a backup full/empty switch that was intended to be an independent safety mechanism.

For tank number 912, only the backup was operational and the gauge was known to stick occasionally. A lever selected whether the backup was looking for full or empty and was supposed to be locked in the full position. However, the padlock to protect this was never fitted and there is some doubt of which mode was selected.

There were also design and construction issues: the tank construction caused overflowing fuel to "bounce" and increase evaporation, and the walls ("bunds") between tanks could not contain a spill due to gaps and bad gaskets.

Early in the Sunday morning of the incident, the tank was being remotely filled and started to overflow, with about 250,000l of fuel making a pool 2m deep. There were then several explosions with the largest one being a "fuel-air" explosion, which was felt 28 miles away. This led to a fire that burned for 3 days.

This in itself was not a Black Swan event, being a conventional failure of safety mechanisms. However, when considered from the perspective of organisations situated in buildings adjacent to the site, this was clearly a Black Swan event. One building in particular, the Northgate building, contained a datacentre which contained the Schengen Information System, the Police National Computer's hot stand-by backup system and the Addenbrookes Hospital Admission and Discharge system. Further afield, other consequences included the closure of a motorway, fuel rationing of flights at Heathrow, closures of schools and public buildings, and pollution from the fire and the fire-fighting chemicals.

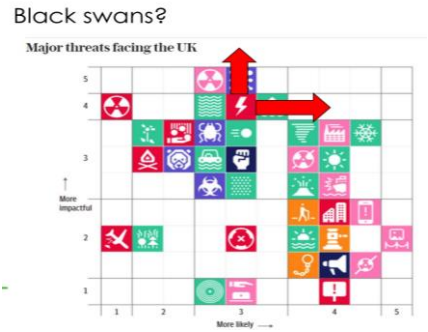
Martin then discussed an issue in January 2021 where data was accidentally deleted from the Police National Computer; it took ~15 weeks to recover the records, which could not have been helped by the hot stand-by backup system, destroyed during Buncefield event, never having been replaced. Martin argued that although the event itself was a normal predicted event, it became a Black Swan event for many people outside, such as businesses, a hospital, the Police, the environment etc.

Martin concluded that there will always be Black Swan events, but whether it counts as a Black Swan depends on who you are.

Martin suggested that to protect against these events requires approaches that are not dependent on the nature of the disaster, such as Disaster Recovery planning and "general" resilience. Organisations need to take a wider view, not just within themselves, but also including their suppliers, the physical surroundings and how failures in external organisations may affect them.

Hunting Black Swans in Power Grids Related to EV Charging and Satellite Navigation Timing Signals

Andrew Larkins from Sygensys Ltd discussed Black Swans in the context of Power grids.



Failures of power grids typically arise from severe weather, failures and supply imbalance and these can have significant impact as there is an extreme societal dependency on power. For example, outages in 2021 in Texas led to many businesses being left without power for several days and there were hundreds of fatalities associated with the event.

The dependency on power is reflected in the National Risk Register with impact at the high end and medium likelihood.

Andrew said that the introduction of electric vehicles (EV) will increase the load on the grid and represents a rapid change that will present a significant challenge to grid operators – by 2035 charging is predicted to be over 40% of the total load at certain times of the day.

A key question is whether the system will still work when faced with these external challenges, and so, this might be a good hunting ground for Black Swans. Andrew found that there were no detailed investigations about the impact of the short-term stability of EV charging after a fault, to prevent a "domino" effect occurring.

Andrew said to help hunt potential Black Swans you need time, skill and freedom to think around the issues.

EVs, by their nature, are high demand and users will want to charge on low tariffs in a smart optimised way, and there is the potential to manage this using IOT technologies. This means that the operator can shift from varying the supply to match the demand, to controlling the demand itself, but this introduces new failure modes.

Andrew suggested some of types of teams and techniques required to explore Black Swans, such as cross-functional teams, mix of generalist and specialists and trying to get people to think in different ways.

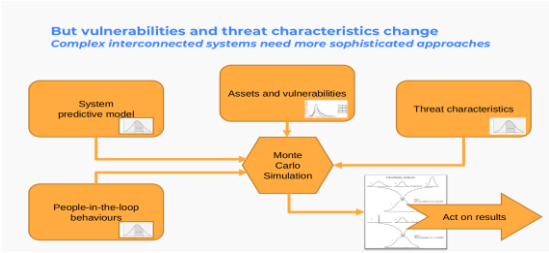
The results of a number of workshops in this area resulted in 6 ways in which EV chargers can present a risk to grid security. For example:

- Step: Too many chargers switching on or off at the same moment
- Ramp: Too many chargers switching on or off within a few minutes
- Oscillations: a group of chargers switching on and off repeatedly
- Degraded stability: increases risk of post-fault collapse
- Demand control: deficiencies are eroded
- Restoration: Erratic behaviour after restart hindering process of restoration.

Andrew asked whether it can be classed as Black Swan if it is predicted before it happened. His focus is on how to fix these future issues but noted there is, for various reasons, resistance from industry to focus on this area at the moment.

Andrew concluded with a discussion on Satellite navigation signals, which are subject to Jamming and Spoofing despite the high dependency that modern society has on them, and so are potential future sources of Black Swan incidents.

Grey Swans



Bill Blackburn from Process Renewal Group concluded the afternoon session with a discussion on Grey Swans. Bill noted that things do happen, such as financial collapses and security breaches that affect large volumes of people.

Bill noted that there are a large number of regulators but noted that it is impossible to regulate away risk and regulators are quite fragmented. Often companies align their organisations around the regulator requirements, compliance is more 'tick box' and regulators struggle to keep abreast of change.

Bill then showed the national risk register and noted that there are several risks that are clearly safety-critical but others that might be classed as safety-related such as Cyber attacks, serious and organised crime and animal diseases.

Bill discussed what items were not in the national risk register such as the Stephen Hawking warning around AI being the 'best or worst thing' for humanity, which then brought in the question around ethics.

Other areas are Quantum computing, which might bring benefits, such as improving the accuracy of inertial GPS systems (eg. using quantum accelerometers and gyroscopes), but might have downsides, such as undermining current encryption techniques. Bill asked how best to gain this foresight and noted that some government organisations like the Department for Business, Energy & Industrial Strategy (BEIS) are doing horizon scanning and commissioning others like the Royal Society to glimpse into future technologies, such as computer/neural interfaces.

Bill said that Quantum Computing, AI and Ethics are hot topics for lawyers who are exploring these areas as potential future areas of litigation.

Bill said the UK Financial Conduct Authority (FCA) are building resilience into financial services after various crashes and discussed some of the challenges the FCA see, such as, technical innovation (AI, blockchain, crypto assets), changing behaviour, keeping pace, challenging environments and system complexity.

Assessing threats in the real world is expensive and can be dangerous and Bill noted some commonly used approaches – techniques (such as those in SCSC Guidance documents), system modelling, crisis-management and simulations.

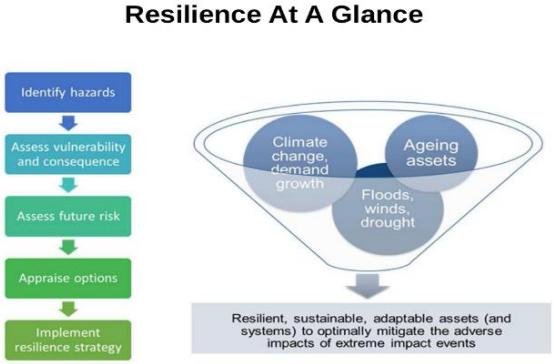
Vulnerabilities also evolve, for example, behaviourally with people moving to higher risk areas, the demand for greater mobility and overuse of drug/antibiotics. New business models and technology adoption and supply chains can often mask vulnerabilities and can have exposure to cyber threats.

Bill concluded that the Royal United Services Institute's (RUSI) viewpoint of the National Risk Register is that half of the risks are missing. Having an entry on the register does not mean that we have methods to manage the risk.

Safety and Resilience of Designs of the Future

Wendy Owen from Bangor University discussed resilience and the work she has been involved in with the Institute of Asset Management (IAM) working group producing SSG-32 Contingency Planning & Resilience Analysis.

Wendy started by explaining the terminology around resilience, resilience analysis and contingency planning. She discussed the resilience analysis process and some points around resilient organisations being typically forward thinking.



She gave examples of the typical processes where resilience analysis is undertaken and contingency planning activities are developed.

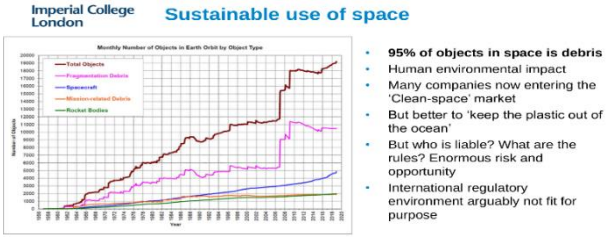
- Prevention: technique used to prevent the issue from occurring
- Response: what is done to respond to an issue once it has occurred
- Recovery: how to return the business back to normal operations and importantly want to learn lessons and prevent reoccurrences

Wendy provided several case studies that were in SSG-32 such as the Pacific Gas & Electric San Bruno (2010) rebuilding after a gas explosion.

In this study, after the incident, rather than abandoning the site, they rearchitected the site with automation, replacement of pipeline, testing and enhanced telemetry and set their goal to be the safest and most reliable company in the industry.

Wendy also noted that there are standards for Business Continuity Management (BCM) such as those used by Network Rail. Some BCMs can use questionnaires to help structure assessments.

Space Weather Risks



The final presentation was pre-recorded by David Southwood and Jonathan Eastwood from Imperial College and introduced in the meeting by Bill Blackburn. David introduced Jonathan as an expert in Space and Atmospheric Physics at Imperial College London.

Jonathan explained what Space Weather meant and he noted it was on the national risk register. He said auroras are the most recognisable visible part of a much larger system resulting from solar activity. Solar flares are common but there are also Coronal Mass Ejections (CME) from time to time that take about 1 or 2 days to reach the Earth but can have significant interaction with the Earth's Magnetosphere.

Jonathan then discussed the worst that could happen from a severe space weather event, typically those that might occur every 100 years. There is real concern that it can disrupt the supply of electricity. Other impacts would be PNT (Position Navigation and Timing) signals from GPS. In space, it can affect the services provided by satellites, and the satellites themselves.

Jonathan gave an example, of a weather event in 1989 that affected supplies in Quebec, North America. However, this was not as severe as that thought to have occurred in 1859, known as the 'Carrington' event.

In another example, in February 2022 SpaceX launched 40 Starlink satellites, but lost most of these because of a small geomagnetic storm.

Space weather is hard to assess as many extreme events have not occurred in the modern technological era. Each event is unique and could last for a period in the order of two weeks. Jonathan asked for feedback from this community about this topic.

Jonathan made some observations:

- The economic impact could be huge based on studies
- Many organisations are not aware of their reliance on space infrastructure and how their products may be exposed to space weather
- There is much more predicted use of satellites in space, such as ubiquitous internet access, and this will bring new challenges, such as managing the 95% of objects now in space, which are debris

Jonathan concluded by asking what a reasonable response is to space weather risk?

The Future of Coding for Safety-Critical Systems



The Future of Coding for Safety-Critical Systems Seminar aimed to provide insights into the future of coding for safety systems: what languages, techniques and methodologies are likely to be used, what coding standards and guidelines may be applicable and how verification and analysis might be integrated with the process of developing code. Dewi Daniels provides the highlights from this fascinating event.

The SCSC held a seminar on "The Future of Coding for Safety-Critical Systems" on Thursday, 9th June 2022. This was a blended event, held in-person at the Wellcome Collection, Euston Road, London and online via Zoom. This was the second SCSC seminar to be held at the Wellcome Collection, which was a lovely venue that was a very short walk from Euston Square underground station.

The C Language… You Wouldn't Start from Here!



The first talk was by Andrew Banks from the Motor Industry Software Reliability Association (MISRA) on "the C language… you wouldn't start from here!" Andrew said he was sorry that Rod Chapman hadn't been able to attend, since he and Rod like to taunt each other about the relative merits of C and Ada!

Andrew started with a brief history of C, followed by the history of MISRA C. He described MISRA C and showed how MISRA C checking would have found Apple's SSL bug [1].

Safety For Software-Intensive Systems

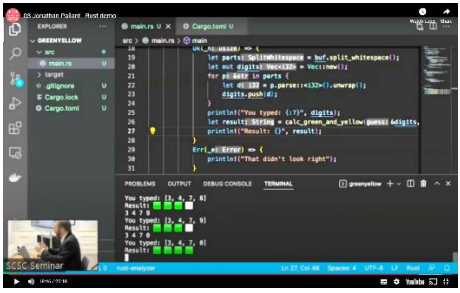


The second talk was by Paul Sherwood from CodeThink on "safety for software-intensive systems". Paul started by describing the history of CodeThink and their safety journey in automotive, including Artificial Intelligence (AI) and infotainment.

Paul presented a proposal as to how to define trustable software. He said that most software is not certified, or even certifiable, and he was sceptical of partitioning claims. He cited an example where an untrusted JavaScript client could crash the hardware.

He presented a solution using Nancy Leveson's Systems Theoretic Process Analysis (STPA) to model the functionality required to support safety applications and examine what could go wrong. His use of STPA is supplemented by fault injection testing to show that the mitigation is effective.

What About Rust for Critical Systems?



The third talk was by Jonathan Pallant from Ferrous Systems on "what about Rust for critical systems?" The talk was originally to be presented by Rod Chapman of Protean Code, but Rod was feeling unwell. Rod is well-known for his work on the SPARK programming language, and he has been using and studying Embedded Rust for about 4 months.

Jonathan felt it would be useful to present a third-party (i.e., Rod's) view on the Rust programming language. John is very well-qualified to speak about Rust, having written two chapters of the Embedded Rust Book [2]. Jonathan gave an introduction to the Rust language, including an interactive demonstration where he wrote a Rust program to implement a number-guessing game, and shared Rod's thoughts on the language, which were that Rust is a huge leap forward compared to C but that, compared to SPARK, there are some rather obvious omissions.

Auto Code and Auto Verify – Is That All?



The fourth talk was by Nick Tudor from D-RisQ on "auto code and auto verify – is that all?" Nick said there had been a great reaction to his paper in the inaugural SCSC Journal [3].

Nick said that people like to write code, but they're not so interested in software verification. A lot of software projects go over-budget. We can't just test and say that's good enough.

Nick advocated removing the opportunity for error introduction by using suitable languages and tools, and using mathematical techniques to replace testing, while hiding the mathematics from the user. He described a set of tools developed by D-RisQ, including Kapture: a requirements management tool, Modelworks: a design verification tool, CLawZ: a source code verification tool and FEVER: an executable object code verification tool.

Coding With Meaningless Symbols



The final talk was by Les Hatton, emeritus professor of Forensic Software Engineering at Kingston University, on "coding with meaningless symbols". Les no longer works in safety-critical software – he says he can't stand it! He now works as a geneticist.

Les said there is good software out there, but we don't have the knowledge to build software as a scientific discipline. We can recognise good and bad code, but we can't explain why. While there are systems out there that are obviously very good, we need to spend more effort on finding out what makes them good.

Les showed that there are emergent and apparently inevitable properties of all discrete systems, from the length of words in books, the distribution of wealth, the length of proteins and the length of subprograms in software programs. Whatever programming language you choose and whatever your program does, your system as a whole is overwhelmingly likely to share the same emergent properties, safety-critical or not.

Since his talk, Les has published an excellent book [5] on this topic, which is available as a paperback or for the Kindle. I have read the book and highly recommend it.

Where To Find Out More

More details of the event, including videos of the presentations and copies of the presentation slides, can be found on the SCSC website at Seminar: The Future of Coding for Safety-Critical Systems (scsc.uk) [4]

References

[1] Apple's SSL/TLS bug (22 Feb 2014), https://www.imperialviolet.org/2014/02/22/applebug.html, retrieved 28 July 2022.

[2] The Embedded Rust book https://docs.rust-embedded.org/book/, retrieved 28 July 2022.

[3] Daniels & Tudor, Software Reliability and the Misuse of Statistics, SCSS Journal, Vol. 1, No. 1, Software Reliability and the Misuse of Statistics (scsc.uk), retrieved 28 June 2022.

[4] Seminar: The Future of Coding for Safety Critical Systems https://scsc.uk/e912

[5] Exposing Nature's Bias: The Hidden Clockwork Behind Society, Life and the Universe, Les Hatton and Greg Warr, Bluespear Publishing, 10 June 2022, ISBN 978-1908422040

Dewi Daniels, Software Safety Limited

Dewi is a highly experienced software engineer specialising in the development and verification of safety-critical and other kinds of high-integrity software. He has worked on programmes ranging from civil airliners such as Airbus A380 and Boeing 787 to personal air vehicles, air taxis and unmanned air systems.

Safety Futures Initiative Update



Zoe Garstang, lead for the Safety Futures Initiative (SFI), provides an update on the progress made by the SFI including details of future events, and she asks for volunteers for the SFI's new mentoring scheme.

Progress Update

Work is underway to provide SFI members with a series of events and activities. This includes a mentoring scheme and regular events, such as further Get To Know You sessions and an upcoming lecture competition (Spring 2023).

The lecture competition will see individuals deliver a short presentation on a safety-related topic of their choice, followed by a short Q&A. Keep an eye on the SFI website (www.scsc.uk/gf) for updates and to find out when entries open.

Mentoring Scheme – Volunteers Needed!



We are establishing a mentoring scheme for SFI members and members of the SCSC community to build on knowledge sharing and career development. The scheme will be one-to-one mentoring, which is flexible to suit the requirements and schedules of those involved. The focus of the mentoring sessions can be anything from technical areas through to career development.

If you would like to register your interest as a mentor or mentee please contact Zoe Garstang (zoe.garstang@scsc.uk).

Upon registering your interest, you will be provided with a short questionnaire in order to match you with the best possible mentor/mentee that aligns with your experience and aspirations.

"We are establishing a mentoring scheme … to build on knowledge sharing and career development."

Membership

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

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

Further Information

If you would like further information about any aspect of the SFI, please do get in touch with Zoe Garstang (zoe.garstang@scsc.uk).

Zoe Garstang, Airworthiness Engineer and SFI Lead

Zoe is an Airworthiness Engineer at BAE Systems. She previously undertook an Advanced Engineering Apprenticeship with the company before joining the Airworthiness & Product Integrity Team.



How Do I Get Into Safety?



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

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

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

With this situation in mind, we continue our series of articles where members of the SCSC Steering Group share their experiences of 'getting into safety'. Some of the routes taken are definitely not linear!

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

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

Roger Rivett



I worked for 10 years developing software for engine management systems. In 1990, the department head, on reading an article about applying BS 9000 to software development, decided that the department should work within a software quality management system (QMS). Of his staff at the time, he considered me to be best person to make this happen. Despite my initial reservations, I accepted the new role of software quality manager with the brief to introduce a software quality management system with external certification.

In the same time frame, the MISRA group was formed under the DTI SafeIT programme with the brief to produce an automotive response to the recently issued draft of what became IEC 61508. This led to the publication in 1994 of the Development Guidelines for Vehicle Based Software. I was my company's representative in the MISRA group, this gave me the opportunity to explore the subject in more detail and I found the topic both intellectually stimulating and of great importance to the wellbeing of my company's customers. Consequently, I started incorporating the functional safety recommendations from the MISRA guidelines into the requirements of the software QMS.

When the software QMS was considered to be firmly established, after successfully completing its 3-yearly recertification, I handed over day to day responsibility for it to a member of my staff and focussed on functional safety, as by now this had become my main area of interest. This involved performing hazard analysis and risk assessment on all the electronic control units fitted to the vehicle at that time and developing associated procedures for inclusion in the QMS. Further knowledge and understanding came from regular attendance at conferences, especially the yearly Safety Systems Symposium run by the SCSC, involvement in further DTI and European projects and continuing involvement with MISRA. The latter resulting in the publication in 2007 of the Guidelines for safety analysis of vehicle based programmable systems. During this time, I became the company's Technical Specialist for functional safety and in 2005 I became a founder member of the ISO working group that developed ISO 26262, first published in 2011.

Jane Fenn



Whilst working as a Systems Engineer for BAE Systems, it was noted that I also had a flare for Project Management, so when a safety-critical system displayed some worrying behaviour during rig testing, they asked me to put together a multi-disciplinary team to undertake a full safety assessment and agree a modification programme with the supplier.

During that time, I met people who became mentors and friends, who drew me further and further into the dark arts of Safety Engineering. I became entirely and shamelessly hooked. When a replacement system was planned, I was determined that we would engineer 'in' safety from the outset. Defence Standard 00-55 issue 2 had only recently been issued and we followed that closely, bringing a level of rigour that was unusual at that time. I started to undertake modules of the Safety Critical Systems Engineering MSc course at the University of York, to ensure I was applying latest and best practice.

Needless to say, once that programme was finished, I jumped at the chance when I was offered the opportunity to manage BAE Systems' research centre, the 'Dependable Computing Systems Centre' at York, and in conjunction with Newcastle University; it was my dream job! That allowed me to be involved with and influence leading edge Safety Engineering research.

Subsequent roles included managing industrial research teams, across defence industry, developing modular safety cases, and later, software architectures, as well as managing the MOD-funded pan-defence industry Software Systems Engineering Initiative. My current role is 'Lead Consultant Engineer – Engineering Safety' where I define the Safety Engineering policy, competency and training requirements as well as some of the processes used by safety practitioners within BAE Systems Air Sector.

I dabble in the occasional safety consultancy activity with other Business Units of BAE Systems and support several of the SCSC Working Groups: Assurance Case, Safety Culture, Security-Informed Safety and Safety of Autonomous Systems. And those people who led me astray all those years ago.... some of them are on the SCSC Steering Group today....

Dewi Daniels



I graduated with a degree in Computing Science from Imperial College, London in 1981. My first job after graduation was with Logica. I spent the 1980s developing software that was not safety-critical but was mission-critical. For example, I designed a software product that allowed applications running on VAX minicomputers to interface to airline reservations networks. I was privileged to demonstrate the product to Ken Olsen (founder of DEC) at DECworld '87. I also worked on a secure trading system for the Bank of England.

I first got involved with safety-critical software when I went to work for Program Validation Limited (PVL) in 1989. There, I was one of the developers of the SPARK Examiner. SPARK is still widely used, though the software we wrote has long since been replaced by open-source software developed by AdaCore. I also did program proof for several Rolls-Royce jet engines, including the RB211-535. This was one of the first industrial applications of program proof, as far as I know, and was very labour-intensive, though also very enjoyable (interactive program proof felt a lot like playing Tetris).

In the mid-1990s, I worked for Lloyds Register. I spent 6 months in Atlanta working on the software safety case for the then-new Lockheed C-130J (which is to be retired from RAF service next year!). I also spent 6 months in Paris writing the outline safety case for the European Geostationary Navigation Overlay Service (EGNOS), a precursor to Galileo. In the late 1990s, I worked for Praxis Critical Systems. It wasn't a very happy time for me; Praxis wanted me to do system safety engineering, whereas I was much more interested in software development.

In 2004, I went to work for Silver Software, which was a great company and a great bunch of people. A turning point for my career was when I joined the committee that was writing DO-178C. I greatly enjoyed the experience and made many friends. In 2010, I was headhunted to form Verocel Limited, the UK subsidiary of a US company. I grew Verocel Limited from a one-man start-up to a company with a turnover of over £2 million. I recruited a

great team of software engineers. I also started a company called Aeronautique Associates in 2012 to offer DO-178C training. When I left Verocel in 2015, I decided to do some consulting while I decided what to do next. I've found that I really enjoy being an independent consultant. I particularly enjoy the variety of work. I've worked on some very interesting projects. I led a team that developed an innovative flight control system for an optionally manned rotorcraft. I helped to develop an unmanned air system (UAS) autopilot. I've audited several companies against DO-178C and DO-254. I've always been interested in software processes, so I enjoy seeing how different teams approach software and hardware development. I'm currently helping Vertical Aerospace build an air taxi. My consultancy work has enabled me to do unpaid work that I also enjoy. I'm currently a member of the RTCA/EUROCAE Forum on Aeronautical Software and of EUROCAE WG-117. I'm one of the UK representatives on the IEC 61508 committee. I'm a member of the SCSC Steering Group.

SCSC is my main means of interacting with, and learning from, like-minded professionals. What I particularly value about the SCSC is the mix of industrial and academic members.

Sean White



I have only ever worked as a Safety Engineer so know nothing else – hang-on a minute, as a Safety Engineer you need to know a lot about a lot of things – that's what's kept me enthralled, challenged and motivated over a number of decades.

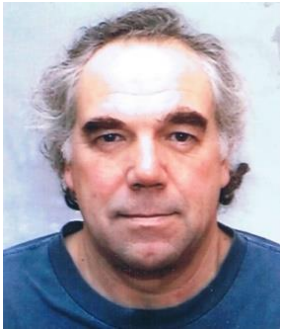
I started in the role, although I didn't know it at the time, as a fresh faced electronics Graduate, working in the Advanced Engineering Department at Westland Helicopters. Days when integrated modular avionics, fly by wire and active control technologies were in their infancy and safety standards were at best interim drafts. The standards matured and so did my understanding and skills and I still get a buzz seeing a Merlin hovering in the sky.

A move to BAe and fast jets gave me the opportunity to work on Hawk, Tornado, Typhon and best of all Harrier – it must be the hovering thing. A short secondment to Boeing to develop a safety case for the Harrier flap controller and a longer one to Flight Test to support Hawk AJT development were highlights.

I then jumped ship or is that plane to join the NHS, working within a team to establish a safety management system for health technologies. Challenging, frustrating but also very rewarding. I'm now writing national & international standards and training clinicians and technologists in the principles of safety management. Still actively involved in research, investigating how to assure AI technologies for health and medical purposes.

Image attribution: top image 54463913 © Somsak Dalad | Dreamstime.com

60 Seconds with … Les Hatton



Les Hatton Ph.D. is a mathematician notable for his work on failures and vulnerabilities in software-controlled systems. Originally an award-winning geophysicist, he switched careers in the early 1990s to study software and systems failure.

He has published widely and his theoretical and experimental work on software systems failure can be found in "Nature", "IEEE Transactions on Software Engineering", and numerous other journals. His 1995 book "Safer C" helped promote the use of safer language subsets in commercial embedded control systems.

In 2012, he took early retirement to try to understand recurring patterns he was observing in the many millions of lines of code he had then studied. In 2014 he proved that all software systems asymptote to the same length and alphabet distribution. In 2015, with the biochemist Greg Warr, he extended this to the distribution of known proteins and has since demonstrated similar behaviour in software, biology, music, literature and many other systems. Their findings have been recently published in the 2022 book: "Exposing Nature's Bias: the hidden clockwork behind society, life and the universe".

He is an emeritus Professor of Forensic Software Engineering at Kingston University, London and spends his spare time doing computational biology in his shed!

What first attracted you to working in the field of software reliability?

I was an earth scientist for the first 20 years of my career. In meteorology and later in seismology I found glaring examples of software failures frequently derailing the science. In 1992, I changed careers to study software reliability to try and find answers.

What aspect of your career are you most proud of?

I don't look back so taking early retirement in 2012 to work full-time on a problem in information theory with an old college friend, a biochemist, which eventually led to the discovery of a new Law of Nature – the Fundamental Law of Inequality. This has been hidden in plain sight for 5,000 years, but manifests itself in literature, language, wealth distribution, software and notably, genomics. The book just came out after some 15 years of work. Curiously, although unintentional, this mostly resolved my original questions about software reliability, but its implications for evolutionary biology are particularly exciting.

What advice would you give to yourself age 12?

Practice the guitar more.

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

The primacy of engineering professionalism and judgement over management, media and indeed politics.

What's your most favourite quote or motto?

Albert Einstein. When he heard that a book titled 100 Authors against Einstein was published in Germany, he said:

"If I were wrong, then one would have been enough."

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

Fly.

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

None of them really. Fictional characters are defined by somebody else. I'm far happier with my own path. If I could play any fictional character, it would probably be "the man with no name", although I'm not very good with horses.

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

In spite of his unfailing belief in the opportunities of education, my dad's career advice was:

"It's not what you know, it's who you know".

The younger idealistic me disagreed, but boy was I wrong.

"Taking early retirement in 2012 to work full-time on a problem in information theory with an old college friend … eventually led to the discovery of a new Law of Nature – the Fundamental Law of Inequality"

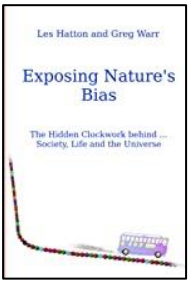
Which work of art or fiction best sums up your experiences with Covid-19?

It would have to be a work of fiction – the government's Covid-19 figures. I volunteered to work in a Covid modelling group through the pandemic and the data quality was truly awful – some of the worst I've ever had to work with.

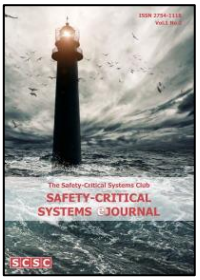
Recent Publications



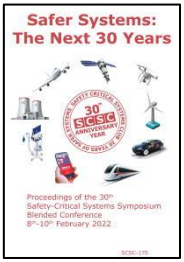
Guidance on the Safety Assurance of autonomous systems in Complex Environments.
http://www.york.ac.uk/assuring-autonomy/guidance/sace/



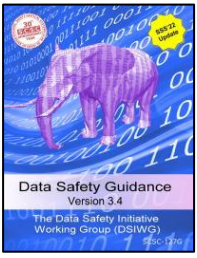
Revealing a newly discovered fundamental law of inequality.
http://www.amazon.co.uk/Exposing-Natures-Bias-Clockwork-Universe/dp/1908422041



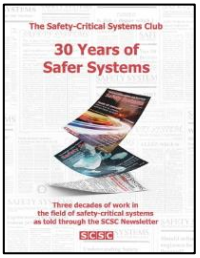
Safety-Critical Systems eJournal vol.1 no.2
Summer Issue 2022
scsc.uk/scsc-176



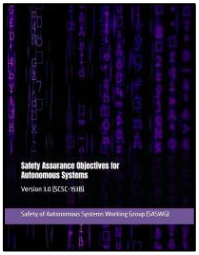
Proceedings of the 30th Safety-Critical Systems Symposium.
scsc.uk/scsc-170



Guidance on the management of data safety risks.
scsc.uk/scsc-127G



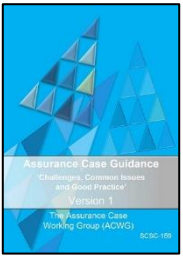
Three decades of work in the field of safety-critical systems as told through the SCSC Newsletter.
scsc.uk/scsc-169



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

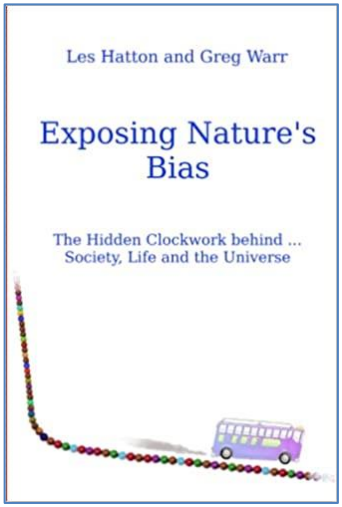


Guidance on assuring safety-related service.
scsc.uk/scsc-156B



Assurance Case Guidance covering Challenges, Common Issues and Good Practice.
scsc.uk/scsc-159

Book Review



Dewi Daniels reviews the new book, "Exposing Nature's Bias: The Hidden Clockwork behind Society, Life and the Universe", by Les Hatton and Greg Warr.

Les Hatton, who is well-known to members of the SCSC, has co-authored a new book [1] that presents a ground-breaking new theory on the emergent behaviour of all discrete systems.

Les presented some of the early research that led to this discovery at the 25th Safety-Critical Systems Symposium [2]. More recently, Les gave a very interesting presentation on the topic at an SCSC seminar [3]. Les will be giving the after-dinner speech at SSS'23.

Benoit Mandelbrot claimed that power law distributions are ubiquitous. Les and Greg have been able to explain why, for the first time. They've called their discovery the Fundamental Law of Inequality.

They show how inequality is the overwhelmingly most likely outcome of all discrete systems. Their theory is corroborated by analysis of large amounts of data, which has only been made possible in the last few years by the availability of powerful personal computers and the publication of open databases.

We think of evolution as an inexorable advance towards organisms of increasing complexity and that humans are the pinnacle of evolution. The Fundamental Law of Inequality shows that nearly all evolution occurs within simple organisms. An alien observer could quite reasonably conclude that bacteria are the dominant form of life on Earth.

The book also shows that inequality of wealth has always been with us and is likely to always remain with us. The Scandinavian countries have low levels of wealth inequality and are among the happiest in the world. Have the Scandinavians found the secret of happiness, or are they simply the countries that happen to be in the long tail of the distribution?

This is one of the most thought-provoking books I've read in the past few years.

References

[1] Exposing Nature's Bias: The Hidden Clockwork behind Society, Life and the Universe, Les Hatton and Greg Warr, Bluespear Publishing, 10 June 2022, ISBN 978-1908422040 https://www.amazon.co.uk/Exposing-Natures-Bias-Clockwork-Universe/dp/1908422041

[2] Balancing safety with rampant software feature-itis, Les Hatton, Twenty-fifth Safety-Critical Systems Symposium, 9 February 2017, Bristol UK, https://scsc.uk/r135/24:1

[3] Coding with meaningless symbols, Les Hatton, SCSC Seminar on the Future of Coding for Safety-Critical Systems, London, 9 June 2022, Seminar: The Future of Coding for Safety-Critical Systems https://scsc.uk/e912prog

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

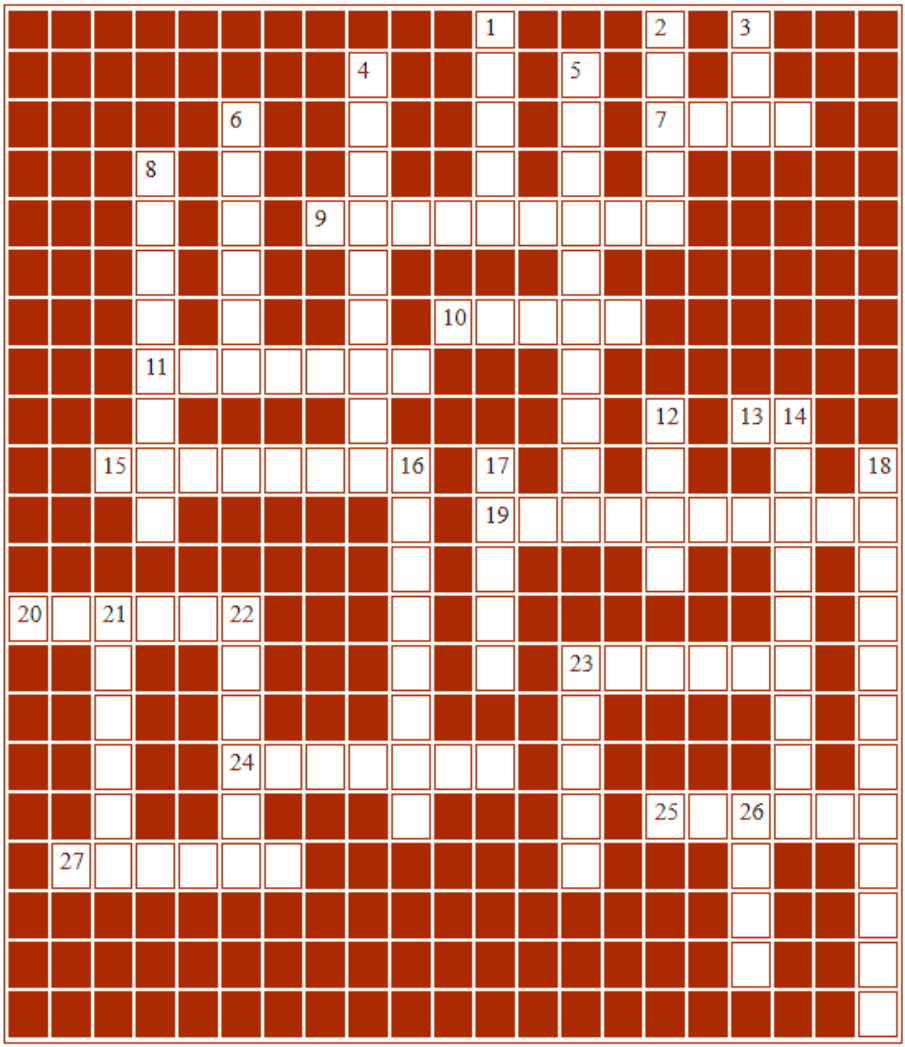
Advertising

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

Safety Systems Crossword

Welcome to the first Safety Systems Crossword prize competition where you can test your knowledge of the world of System Safety!

Send you completed grids to crossword@scsc.uk by 31st Dec 2022. The first correct answer drawn from a hat at SSS'23 will win a £50 Amazon Voucher!



Across

7. Abbreviation for a system designed to prevent aircraft collision (4)
9. A device for keeping an aircraft on a set course without the intervention of the pilot (9)
10. Type of attack that targets computer information systems, computer networks, infrastructures, or personal computer devices (5)
11. Type of process automation that mimics back-office tasks of human workers (7)
13. Abbreviation for a technology with applications such as natural language processing (2)
15. Type of network for representing knowledge about an uncertain domain (8)
19. Name given to the event associated with the most intense geomagnetic storm in recorded history (10)
20. Farmer from Kansas who founded an aircraft manufacturing company (6)
23. A visual display device used in the railway industry to convey information to drivers (6)
24. Author of a report that led to the development of a national police intelligence system (7)
25. Type of stochastic process conditional only on the present state of the system (6)
27. Actual colour of a flight data recorder (6)

Down

1. Abbreviation for a system-theoretic model of accidents (5)
2. A type of tube for measuring fluid flow velocity (5)
3. Abbreviation for a type of top-to-bottom failure analysis technique (3)
4. Location of a significant nuclear accident precipitated by a powerful earthquake (9)
5. Name of the vehicle where cold weather contributed to its loss (10)
6. Low Earth Orbit satellite constellation company that survived Chapter 11 bankruptcy (6)
8. Site of a nuclear power station deriving its name from "fort on the mound" (8)
12. Adjust the aerodynamic forces on the control surfaces so that an aircraft maintains the set attitude without any control input (4)
14. A feature that makes the state of two mechanisms or functions mutually dependent (9)
16. A type of chart that has a graphic representation of a sea area and adjacent coastal regions (8)
17. Shutdown a nuclear reactor in an emergency (5)
18. Type of machine learning algorithm that learns patterns from untagged data (12)
21. A device which detects or measures a physical property and records, indicates, or otherwise responds to it (6)
22. Vehicle safety feature that reduces the severity rather than likelihood of an accident (6)
23. Nickname of the pilot involved in a famous emergency water landing (5)
26. Abbreviation for a type of graphite-moderated nuclear power reactor (4)

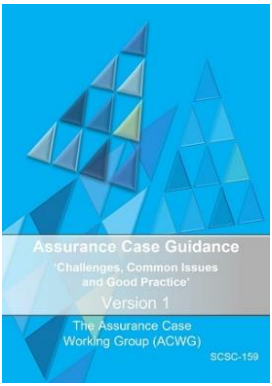
SCSC Working Groups

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

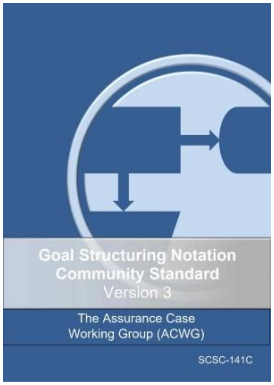
Assurance Cases

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

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



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



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

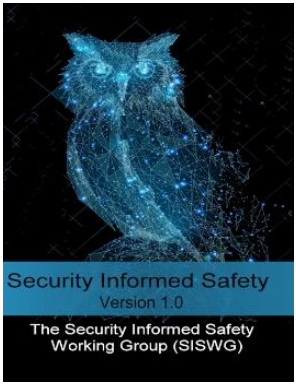
See scsc.uk/gsn for further details.

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

Lead Phil Williams phil.williams@scsc.uk

SCSC Working Groups

Security Informed Safety



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

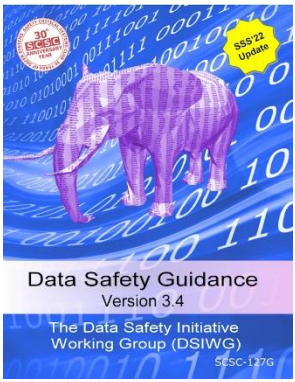
The working group aims to produce clear and current guidance on methods to design and protect safety-related and safety-critical systems in a way that reflects prevailing and emerging best practice.

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

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

Data Safety Initiative

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



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

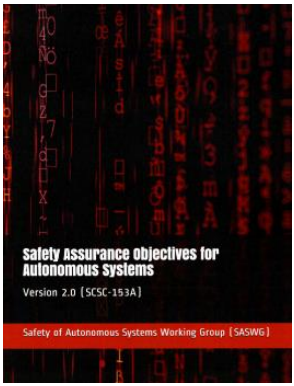
The Data Safety Initiative Working Group (DSIWG) aims to have clear guidance on how data (as distinct from the software and hardware) should be managed in a safety-related context, which will reflect emerging best practice.

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

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

SCSC Working Groups

Safety of Autonomous Systems



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

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

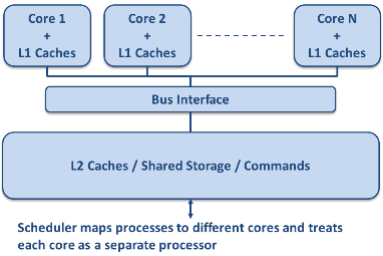
The Safety of Autonomous Systems Working Group (SASWG) aims to produce clear guidance on how autonomous systems and autonomy technologies should be managed in a safety-related context, in a way that reflects emerging best practice.

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

Lead 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.



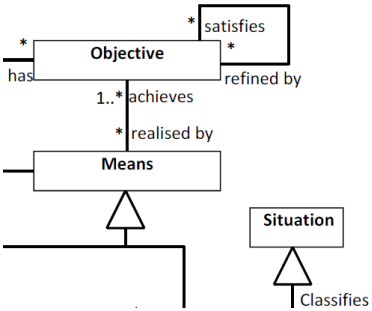
Parallel processes need to access the same shared resources, including memory, cache and external interfaces, so they may contend for the same resources. Resource contention is a source of interference which can prevent or disrupt completion of the processes, meaning it is difficult to know with a defined 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

Covid-19



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

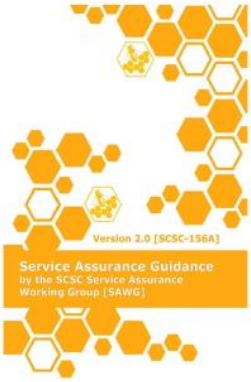
The group has compiled an extensive range of Covid-19 related material and made this available on the working group's website pages along with ongoing developments in the thoughts and ideas of the group.

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

Lead Peter Ladkin ladkin@causalis.com

SCSC Working Groups

Service Assurance



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

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

Lead Mike Parsons mike.parsons@scsc.uk

SCSC Safety Culture

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

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

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.

The group held its inaugural meeting on 17th June 2022 with its 3rd meeting planned for 19th October 2022. Please get in touch with the working group lead if you would like to join, or find out more about this group.

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: £125
- 2 year Membership: 20% discount: £200
- 3 year Membership: 33% discount: £250 (3 years for the price of 2)
- 1 year SFI Membership: FREE for first year, £35 for years 2 & 3
- 1 year Membership, retired member rate: £35
- For Corporate Membership discounts contact Alex King.

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

Zoe Garstang 2019-

Nikita Johnson 2019-2021

Calendar

October '22

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

November '22

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

December '22

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

January '23

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

February '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					

March '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		

April '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

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
31						

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	

Events Diary



11 Oct 2022
Conference

High Integrity Software (HIS)

Marriott Hotel City Centre, Bristol

www.his-conference.co.uk

12-14 Oct 2022
Conference

RISK/SAFE 2022: 13th Conference on Risk Analysis, Hazard Mitigation and Safety and Security Engineering

Rome, Italy

www.wessex.ac.uk/conferences/2022/risk-safe-2022

18 Oct 2022
SCSC Working Group

Assurance Case Working Group (ACWG) #17

Online

scsc.uk/e958

19 Oct 2022
SCSC Working Group

Systems Approach to Safety of the Environment (SASEWG) #3

Zoom, 16:00-17:30

scsc.uk/e964

20 Oct 2022
SCSC Working Group

ACWG: Assurance Case Paper TG

Online

scsc.uk/e960

3 Nov 2022
SCSC Working Group

ACWG: GSN SWG

Online

scsc.uk/e959

22-23 Nov 2022
Conference

10th Scandinavian Conference on System and Software Safety

Gothenberg, Sweden

safety.addalot.se/2022

28 Nov 2022
SCSC Working Group

SCWG: SCSC Safety Culture Working Group (SCWG) Meeting

Location – TBA

scsc.uk/e922

1 Dec 2022
SCSC Seminar

The Future of Testing for Safety Critical Systems

London, UK and blended online

scsc.uk/e966

7-9 Feb 2023
SCSC Symposium

Safety Critical Systems Symposium SSS'23

York, UK and online

scsc.uk/e898

6 Apr 2023
SCSC Seminar

Safety of Autonomy in Complex Environments

London, UK and blended online

scsc.uk/e890

Partner Event



The High Integrity Software conference is back! #HISConf2022

www.his-conference.co.uk

After two years of virtual events, HIS 2022 will be making its physical comeback on Tuesday 11th October 2022 at a new venue: the Bristol Marriott Hotel City Centre for what promises to be a great event.

Modern-day national infrastructure programs are often comprised of critical software-intensive systems. A key differentiator with these projects is the scale of the engineering endeavour coupled with the need to remain operational for the long term – often over several decades.

This year, the High Integrity Software conference will consider this issue from a technical perspective. More specifically, the aim is to understand how early decisions around cyber-physical system architectures and adopting effective software development lifecycles and verification techniques will later impact defect rates and maintainability. However, the challenge for such large-scale and long-term systems is multi-faceted. Therefore, the conference will also consider broader issues within the software development ecosystem, such as sustainable supply chains and talent streams.

To see the full programme and book your place - https://www.his-conference.co.uk/

All delegate tickets are £220.00 (excl VAT) per person

If you have any questions about the conference, the exhibitor package or further sponsorship opportunities, contact info@his-conference.co.uk.