SAFETY SYSTEMS

The SCSC Newsletter

Spring 2017 Volume 26 Number 1

Guest Editorial: Twenty-Five Years of Safety - SSS'17: A Personal Perspective

by Dick Selwood

Much has happened in the safety-critical field since the first Safety-Critical SystemsSymposium (SSS) in 1992. At SSS 17 in Bristol these advances were celebrated by several of the keynote speakers, who had themselves been instrumental in the last quarter century's developments (and indeed before).

As it is impossible to compress three days of thought provoking presentations and debate into the space of a newsletter, you may want to buy the 500 plus pages of proceedings, *Developments in System Safety Engineering: Proceedings of the Twenty-fifth SSS,* on Amazon (£10.25) or download individual papers for a small charge (free to members) from the Club website, www.scsc.uk. The speakers' slides are also available from the website, and we will soon post video highlights from the Symposium there too.

Meanwhile, what one member of the audience saw as highlights (not that there were any low-lights) follows.

The historian keynoters were:
Audrey Canning, *Functional Safety: Where have we come from? Where are we going?*

Robin E Bloomfield, Kate Netkachova, Peter Bishop, *Confidence in a Connected World: Safe, Secure, Resilient and Autonomous*

Nancy G. Leveson, *My 36 Years in System Safety Engineering: Looking Backward, Looking Forward*

Dewi Daniels, *From the IBM 29 Card Punch to the Boeing 787 Dreamliner (and Beyond)*

Ron Bell, *Safety-critical Systems - A Brief History of the Development of Guidelines and Standards*.

In this Issue

Please send articles or news items for future editions to the editor, Katrina Attwood, at newsletter@scsc.org.uk

Together, these talks established the setting for the establishment of the SCSC, and followed not just with a chronicle of the activities that have taken place in the world of system safety engineering, but also an insight into the complexities of developing safety standards. One such is *IEC61508: Functional Safety of Electrical/ Electronic/Programmable Electronic Safety-Related Systems* (published 1998), the foundation stone for many more industry-specific standards, such as ISO 26262 for automotive. In some cases, herding cats may be easier than getting agreement between the differing interests and different countries involved in producing a standard. The amount of sheer hard work that has gone into these documents is astonishing. It wasn't entirely positive: several speakers held that the existing standards, while better than nothing, are a long way from perfect. One speaker said that, "most standards are unverified hypothesis", and another stated that while standards are often the consensus of a large group of experts, they are not evidence-based.

Tom Anderson, the long term Chair of SCSC, gave a wonderful talk entitled, *What can I say?* (One might argue that finding something to say is never a problem for Tom!) The talk brought together several of the most important elements of Tom's life: safety, mountains, trains and single malt whisky, to provide a very personal perspective on history.

The first, non-historical, keynote was particularly thought-provoking and provided a very high benchmark for the following three days. In *Playing Catch–Up: The Fate of Safety Engineering?*, John McDermid compared safety engineering to other engineering and scientific disciplines. Dipping into the philosophy of science, including Popper and Kuhn, he argued that other disciplines, including engineering disciplines, use experience either from experiment or in the field to challenge and modify the prevailing orthodoxy. By contrast safety engineering is always playing catch–up. While this is inevitable, as the design engineer is advancing the state of the art, it should be possible, by establishing a set of principles, and building better links with the design community, to reduce the catch–up distance drastically and so improve safety.

John McDermid mentioned Systems-of-Systems (SoS), one of the latest buzzwords. A paper by Mike Brownsword, Andy German and Ian Mitchell looked at the problems arising from SoS, which they define as the result of combining two or more independently managed elements subject to different management, investment and control policies. Driverless trains, planes/drones and autonomous and connected vehicles are already SoS, and the technology is extending into industrial, medical and other safety-critical applications. The paper discussed various approaches to understanding and identifying the safety problems that are created by SoS.

An approach to the safety of autonomous vehicles was the subject of a paper by John Birch, Mark Cousen and David Ward. The product integrity assurance argument framework for vehicle autonomy builds an MISRA's work and the ISO 26262 standard and is put forward as a starting point for more detailed work.

Related to this are the issues of Reduced Crew Operations (RCO) in the civil aviation industry. Airlines are investigating having one person (instead of two) in the cockpit, and supporting them from the ground through high speed data communications. Kevin Driscoll explored the safety issues, ranging from possible cyber-security problems with communications (there are already documented cases of individuals pretending to be air traffic controllers), through the

possible impact of latency caused by deeply secure encryption and decryption, to the problem of a pilot with a full bladder. He was uncertain that the economic benefits of RCO, once these problems were addressed, were ever actually going to be sufficient to justify the approach.

Cyber security problems in a hospital were the subject of Harold Thimbelby's paper. A hospital has seen nurses successfully prosecuted for falsifying data. A key plank of the prosecution was the evidence of records in a database. In a further trial, Thimbelby successfully discredited the evidence derived from the database, because of basic flaws in the recording process, poor management of the database and even editing between the records being created and the police downloading the data. It was disconcerting to the entire audience that, under English Law, a computer producing an evidential record is presumed to be working correctly.

Accuracy of medical data was the subject of a paper by Tom Adams, Paul Hampton and Mike Parsons. Data has previously been virtually ignored as a factor in safety. By drawing on case studies and personal perspectives, the paper identified data problems and suggested mitigating techniques, leaving the impression that there is still a great deal of work to do. The SCSC has a working group on data safety and its latest report *Data Safety Guidance (Version 2.0)* is available for free download from the Club website.

As well as poor data, another area that has not been well studied is the threat posed by the insider. As Ryan Meeks and Robert Dickie discussed, there are a number of potential threats, ranging from mistakes through espionage, fraud, theft (particularly of IP), to sabotage. They used cases such as Chernobyl, Edward Snowden and the German Wings flight 9525 to make a strong case for always considering the insider as a safety issue.

A new problem that faces safety engineers is the increase in what Rob Ashmore and Elizabeth Lennon call "non-traditional software". Current standards assume that software is created from a set of requirements, which include safety requirements, against which the software can be verified. However machine learning, using techniques such as neural networks to change code, or even create entirely new code, is moving out of the lab and into real applications. Here the link between the initial high level requirements and the executing code is not so easily determined and such systems are not amenable to many existing safety techniques. They see hope in the Four Plus One principles (set out in 2013 by Hawkins et al) and, in analysing how these can be applied to machine learning, came up with an additional principle. So they put forward Four Plus Two as the basis for developing safety engineering for machine learning.

So far, we have been looking at emerging problems and possible ways of solving them, but as is usual at the SSS there were a number of papers reporting work that has analysed existing problems and have either solved them or are actively implementing solutions. These included: human factors in helicopter operations; certifying a multi-core processor architecture; software handling of hardware errors; electromagnetic disturbances; formally verified optimising compiler, time-triggered software architectures; formal proof in DO-833; and sneak path analysis.

The final keynote was by Les Hatton. He didn't look at history, but instead addressed the issue of raging feature-itis - adding more features to a product - one contributor to the 20% per annum growth in system source code size. This is, in part, because there is no data for the system engineer that matches the structural

engineer's ability to say, "A beam that long will break." Instead, all that can be said is "My experience leads me to think that adding that new feature will cause severe unintended consequences." Les has been working on trying to bring measurement to software quality evaluation, but has concluded (not without a great deal of time and effort) that we are more likely to improve the safety and reliability of systems containing software by pursuing the traditional engineering virtues of redundancy and designing for failure than by pursuing studies of the fabric of software.

This is a very brief summary and doesn't include the stimulating after-dinner talk by Air Marshal Julian Young, the panel session nor the to-and-fro around the exhibitors' displays, across the coffee cups and the lunch plates, and during the beer tasting.

Dick Selwood is a freelance writer with a strong interest in safety and related matters.

SCSC would like to thank all speakers, session chairs and organisers for a wonderful 25th Anniversary Symposium. We look forward to seeing you all again next year at the Principal Hotel, York, 6th - 8th February 2018.

Working Group Report: Safety of Autonomous Systems

by Rob Alexander and Philippa Ryan

Building on the success of the long-established Data Safety Initiative Working Group, SCSC has recently established new Working Groups, to address various pressing issues in system safety engineering. To date, three further groups have been established: the Safety of Autonomous Systems Working Group, the Assurance Cases Working Group and the Service Assurance Working Group. *Safety Systems* will be reporting on developments within the Working Groups. In this issue, the focus is on the Safety of Autonomous Systems Working Group (SASWG).

The SASWG has been formed 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 first meeting was held at Conekt in Solihull on 17th January. The discussion was interesting and wide-ranging, and considered, among other things, domains and applications of interest and terms of reference. The group agreed to produce an outline – content list and candidate structure – of a cross-sector guidance document by the end of the year. We plan to hold meetings roughly once a month for the foreseeable future.

The second meeting was held on 9th March at the Transport Systems Catapult in Milton Keynes. A number of domain-specific examples were presented, from automotive, medical, civil aerospace, defence, rail, maritime and space. These were used to establish the zone of interest for the guidance, in terms on internal and contextual complexity.

The third meeting will be held in early May. Location to be confirmed. For further details, please contact Rob Alexander: rob.alexander@york.ac.uk.

See the *Events Guide* on page 36 for details of other forthcoming Working Group meetings and other Club events.