SSS'21 Event Report



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

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

Thought for the Symposium



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

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

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

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

The Pivotal Pandemic

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

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

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



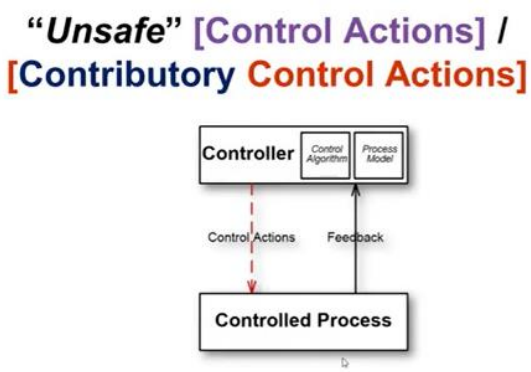
Learning from the UK pandemic response using STAMP

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

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

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

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



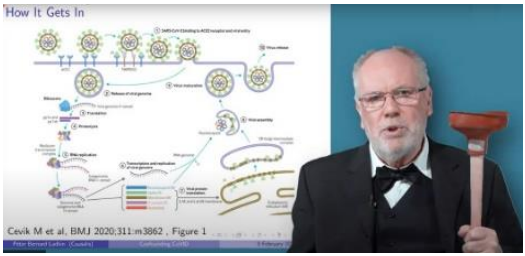
Simon showed how this model can be applied in the context of the Covid-19 pandemic. For example, processes under control could be Population Behaviour and Virus Transmission with lockdowns being typical control actions. Feedback would represent the daily statistics of infections and deaths used to inform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

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

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

Confounding Covid

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



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

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

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

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



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

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

Assurance 2.0: A Manifesto

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

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

Robin presented the key points of the manifesto:

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

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

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

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

Evening Session (After-Dinner)

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

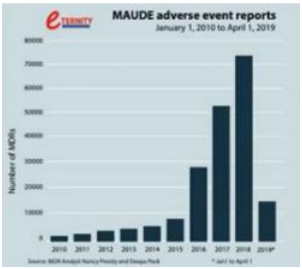
PETER – A Pan-European Training, Research and Education network

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

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

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

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



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

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

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

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

Virtual Networking and Exhibitions

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



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

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

Success!

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

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

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

Report by Paul Hampton, SCSC Newsletter Editor