The Future of Safety Engineering and Assurance



The SCSC has come a long way since its inception 30 years ago, and has achieved a great deal throughout that time, undoubtedly contributing to making systems safer. Over those three decades, the club has needed to adapt to a changing world: the use of technology in society has expanded rapidly, and systems have become more powerful, complex and distributed with many new disruptive technologies (such as AI) making safety assurance ever more difficult. So what will the world be like in another 30 years? What will the concerns of the club's members be in 2052, and what achievements will the club be celebrating?

Jeremy Messersmith, in his ukulele song "Everybody Gets A Kitten" [1], offers his particular optimistic vision of the future:

"Gotta say the future's awesome, everything is a-okay!
All the work is done by robots, every day is Saturday.
Future people all have jet-packs, fly around in flying cars…"

And, as hinted by the title, he goes on to predict that:

"Everybody gets a kitten, a new one every single day …
You can name if you want, or you can give it away!"

Jet packs and flying cars? Probably – we have prototypes of those now; but, as we've seen, the logistics of distributing vaccines to 50+ million citizens in the UK alone has been immense; imagine the distribution infrastructure, processes and personnel required to ensure everyone had a kitten delivered *every day*… well, perhaps not.

To get a, hopefully, better informed and sagacious answer to these questions, members of the SCSC Steering Group were canvassed for their opinions on how they see the future of safety engineering. The following summarises some of their predictions in response to four specific questions.

The pressing concerns of the day might be best illustrated through the title of the key note speakers' talks at SSS'52, but what might these be?

The continued progression of autonomous systems featured in a number of suggested titles:

- Why my iPartner isn't always pleased to see me
- Training Adaptive Systems of Systems in a Secure and Ethical Way
- Why Manually-Driven Vehicles are a Danger and Should be Banned
- The Importance of Non-human Factors in Safety Assurance
- Can AIs Argue Their Own Assurance?

There are also views that system safety will be an increasing concern for systems operating off-world in space and on other planets:

- Fatal Mars Rover Collision in 2050: Final Accident Report and Analysis
- A review of safety standards for commercial space transport vehicles



Other titles suggest that safety assurance challenges will emerge from novel technologies:

- How Weather Control Failed in the Storms of '51
- Regulating System Safety in the Metaverse [2]

The expansion of safety consideration from primarily focussing on harm to individuals and the associated technical mitigations to include the wider societal and environment impacts, and encompassing the trade-off between harms and benefits, is expected to bring more expansive concerns:

- Safety, Ethics and Sustainability of Domestic Space Flights
- Safety Assurance of Earth's Digital Twin

As with our existing standards – some being in use for several decades – standards are expected to continue to feature in the future:

- The key differences between IEC 61508 Editions 9 and 10

Autonomous Systems and Artificial Intelligence (AI) are some of the current bêtes noires for Safety Engineers, but what sort of technologies will be the most challenging for safety engineers in 2052?

The challenges of AI are still expected to be present well into the future, with new developments confounding the assurance progress that might have been made in the meantime:

- Explainable systems that make up false explanations for their decisions, i.e. create lies
- The automation of safety certification using AI based on 2040's practices and how to get new techniques accepted
- Evolutionary systems that breed new behaviours
- Personal robotic assistants



As with the key note speaker title, space travel is also seen as a future challenge as the capability becomes more accessible and available to a domestic market. However, this is just one example where technological expansion will need the safety community to take a wider view, such as: what are the impacts on global resources, climate change and risk distribution from such activities?

Challenges in the Healthcare domain and medical science also features as presenting future challenges, both technically and morally. Some Covid anti-vaxxers already believe the technology exists to inject microchips into people. When such technology is available, how will we deal with the safety implications and need to weigh the risks of not introducing (life-saving) technology? Specific examples are:



- Healthcare Nanobots
- The embedded man-machine interface – cyborgs
- Robotic surgery

Other suggested areas that will present challenges are related to the challenges we face now:

- Highly adaptable, configurable systems – just what are they doing today?
- Systems of Systems; Systems of Services – everything interconnected and inter-dependent

And of course, we will still have the same issues that we've not been able to solve in the last three decades, such as the metrics used to measure software.

Interestingly, there were not many responses in terms of the integration of safety and security disciplines; only some concerns around Ubiquitous Communications and Computing, but perhaps this reflects an optimism that safety/security integration will be eventually 'solved'…

What new tools, techniques and methodologies will be available to safety engineers in 2052?

New tools and techniques are certainly anticipated, but there is also an expectation that the tried and tested techniques will also still be with us. Firstly, new suggestions:



- Better visualisations
- Simulation/animation models
- Virtual environments
- Quantum Risk Assessment
- AI-prediction in Safety analysis - now we don't have to guess 'What if?

And evolutions of the more familiar standards and techniques that we have now:

- DO-178K
- STOMP: The Systems-Theoretic Outcomes Model and Processes (c.f. STAMP [3])
- Safety V (c.f. Safety I and II [4])
- Dependable software reliability techniques

There is also an acknowledgement that existing tools have limitations (eg. They tend to focus upon single failures) and will find it difficult to cope with more complex systems. It's therefore expected that new tools/techniques will be required to enable safety analysis of increasingly complex systems without incurring disproportionate time or cost.

And finally, what club achievements will we be celebrating over the previous 30 years?

On a fundamental level, one basic achievement will be for the club to still be going strong in another 30 years' time and still fulfilling its community objectives. The Covid pandemic has been a challenge to the club financially, and has demonstrated how much it depends on its members and in the knowledge-sharing environments where it thrives.

As well as having much increased membership from all around the world, a demographic of much younger members is anticipated, with the range of safety concerns also expanding in a more intersectional way, to include areas such as environment, sustainability, ethics and inclusion.

By expanding the scope of safety to include ethics, sustainability and the wider societal benefits and impacts, the club will have played a more influential role in government policy making and contributed to tackling the world's bigger issues, such as global warming and inequitable risk distribution.



Embracing new media formats is also expected; the enforced move to online events in recent times has shown that multi-media events can work, and this will only get more interactive with the Metaverse, Virtual Environments and Augmented Reality.



And to conclude, might we be having our first ever successful meeting held in space or even on a different planet?

References

[1] "Everybody Gets A Kitten", Jeremy Messersmith, from the album "11 Obscenely Optimistic Songs For Ukulele: A Micro Folk Record For the 21st Century and Beyond", 2017

[2] Metaverse, https://en.wikipedia.org/wiki/Metaverse, accessed January 2022.

[3] An Introduction to STAMP, https://functionalsafetyengineer.com/introduction-to-stamp/, accessed January 2022.

[4] The Safety-II approach: Learning from what goes well, https://www.patientsafety.com/en/blog/safety-2-versus-safety-1, Jens Hooiveld, accessed January 2022.

Article by Paul Hampton SCSC Newsletter Editor with thanks to our Steering Group contributors: Mike Parsons, Brian Jepson, John Spriggs, Graham Joliffe and Tim Kelly.

Image attribution:
flying car: 86370063 © Pavel Chagochkin | Dreamstime.com
mars rover: 69574941 © Sergey Drozdov | Dreamstime.com
robot on train: 113031130 © Pavel Chagochkin | Dreamstime.com
nanobot 208880224 © anolkil | Dreamstime.com
virtual meeting: 206600489 © Sofiia Shunkina | Dreamstime.com
second life virtual environment: license by CC BY
meeting in space: 63942984 © 純一 島崎 | Dreamstime.com