Thought for the Symposium

Tim Kelly, former Professor of High Integrity Systems at the University of York and former Managing Director of the SCSC, provides his closing remarks in the form of a "Thought for the Symposium", to conclude proceedings at the 30th Anniversary Safety-Critical Systems Club Symposium.

Firstly, I'd like to say that Mike and the team are to be congratulated at what they have been able to achieve in running this year's symposium as a blended conference – bringing together folks from near and far, on-site and online, together once more to share ideas, learn from one another and hopefully – by doing so – advance the field and practice in industry. The importance of bringing people and ideas together should never be underestimated, and it's what I'd like to focus on for the next few minutes.

I read this week some words from my new boss – Justin Welby – the Archbishop of Canterbury (not my ultimate boss, you understand!) some ideas that challenge the narrative that has (at points) emerged during the pandemic – and for this symposium it has made me reflect on some of the problems that we encounter in the field of safety engineering.

Justin Welby said that "One person put it best when they said it was as though the pandemic had caused us all to 'lose the muscle-memory of how to be together'". Covid had shown unequivocally that individualism and atomisation were both illusion and fantasy; from staying at home to bulk buying supplies, getting the vaccine, or wearing a face mask, the message was clear: "Our actions affect other people. We cannot do what we want without it having an impact somewhere else." It struck me that these ideas may have something to say to us in the world of safety engineering.

Anyone who has been on one of my Goal Structuring Notation (GSN) courses, will have heard me talk about "divide and conquer" as one of the strategies to tackle large complex problems and break them down into smaller more manageable problems. It's a natural thing for us as engineers to do. It's what we do! Some would say that it's the true sign of an engineer that perhaps even from an early age they enjoyed taking something apart into its constituent bits and then putting them all back together again!

You could say that this is even what a symposium such as this one does: it takes the complex phenomena of system safety and breaks it down into separate sessions, separate insights and papers on data safety, or autonomy, or human factors, and so on. However, when I used to teach "divide and conquer" in my GSN courses, the most alert attendees would, of course, say "But hang on … what about the interactions? What about how one sub-problem cannot be truly solved without impact another?" And of course they were right, and we'd then talk of ways to cover the interconnections and interactions, perhaps with a part of the safety argument specifically ring-fenced to address that concern.

If you're honest – you breathe a sigh of relief when a particular deviation is proposed and you realise that this particular issue is not your problem

But what does this interconnectedness of all things look like in the middle of our safety engineering activities, on a day-to-day basis. Well, perhaps you can relate to the following observations: have you ever found yourself in the middle of hazard analysis … a HAZOP or an FHA, where the list of potential concerns and problems to resolve seem to be piling up, and – if you're honest – you breathe a sigh of relief when a particular deviation is proposed and you realise that this particular issue is not your problem – it lies outside the boundary of your concern. Phew – that one, at least, is someone else's problem – or you're under no obligation to fix it given the contract you've signed up to. That would be a maintenance issue, you might say, and we're not responsible for maintenance, or that would be a human factors concern, but that's out of scope. Of course, it doesn't necessarily mean it isn't a problem, but to put in terms of the pandemic – "not my toilet roll!"

Or maybe you've found yourself drawing up the issues to be addressed by your safety or assurance case, and again if you're honest, you're relieved when some tricky claim, or some challenging part of the argument can be declared outside the scope. One project team that I was involved in that was using Modular GSN to construct what turned out to be quite a complex argument, seemed to *really enjoy* and *relish* using "Away Goals" (those claims that you've realised are a necessary part of the argument, but are addressed elsewhere) as a way of declaring something *they* didn't have to do. The metaphorical picture of a gardener throwing snails over the garden fence comes to mind, or perhaps those areas marked on ancient maritime maps which simply said, "Here be dragons" at the edge of the explored territory.

Of course, this issue of system safety being a holistic – whole – system issue isn't a new observation, but highlighting the relevance of holistic thinking I was struck by a newspaper article just this last week provocatively titled: "Covid lockdowns did more harm than good". The article reported on the results of a controversial study that had concluded that the costs to society far outweighed the benefits and called for lockdown to be questioned as a future pandemic policy.

The study reported that some lockdown measures may have increased deaths by stopping access to outdoor space, "pushing people to meet at less safe places", while isolating infected people indoors, where they could pass the virus on to family members and housemates, and of course, challenging people's mental health.

It was an interesting (if albeit since contested) study. In terms of what we have been discussing within this symposium, it served to focus attention of the dangers of ever simply

fixating on one problem, and potentially one mitigation (one solution, if you like) at the detriment of many other problems. One of the things that makes me recognise this problem most keenly at a personal level at the moment is that one of my friends – a fellow vicar – is now in a hospice, undergoing palliative care for advanced and aggressive cancer that remained unobserved, and undiagnosed for the vast majority of 2020 and 2021, in large part, because she simply could not get face-to-face access to her local GP, which was operating in a highly restrictive mode because of the lockdown measures. Her case, unfortunately, is not isolated. Cancer doctors and researchers are currently experiencing a bow wave of undiagnosed cancer cases because of the pandemic.

System safety engineering can sometimes seem like a game of "whack-a-mole"

During the pandemic we experienced at first hand the emphasis on one set of statistics, one set of indices and charts – of "flattening the curve" – in the daily number 10 briefings. We are perhaps only now starting to see the impact of the many 'curves' that weren't flattened, or of the other indices that were rising. A reminder, if ever we needed one, of the danger of focusing on single set of metrics.

And talking of "flattening the curve", it brings to mind how the activity of system safety engineering can sometimes seem like a game of "whack-a-mole". I'm sure you've seen this fairground game, where you're given a big hammer with which you are to bash on the head of a mole as soon as it appears … only as soon as you knock one mole down another pops up to be knocked down … and then another and so on.

One of the earliest group hazard analysis exercises we used to teach at the University of York on the Safety Critical Systems Engineering MSc was called the "Aircraft Configuration Check". In that system, the maintenance engineer had to write down a part number for a faulty unit, walk it over to the stores, retrieve the replacement part and then enter the details of the new part back into the configuration management unit. Lots of potential for error – that was the idea! However, I was always struck how some – in definite "fix it" mode – would simply suggest that if the whole process could be managed by computer and networked connections, then the problem would be solved.

I would then point out that this was a problem *changed*, rather than solved. As soon as one problem was eliminated, another potential problem would be created. Whack-a-mole, see? It doesn't mean that we wouldn't make the change, but we should never be so naive as to think that apparent progress doesn't bring with it its own set of contingent problems.

So what are the takeaways for us today? My observations over the recent years of the symposium are that, firstly, given the complexity of systems we are increasingly proposing and integrating into everyday life, we will never run out of challenges and problems to address in this field!

I hope you've all had a chance to read the article that Paul Hampton has put together for the 30th Anniversary Edition of the SCSC Newsletter entitled, "The Future of System Safety". To collate ideas for the article, Paul asked contributors to imagine it was SSS'52 and we were celebrating the 60th anniversary of the club. He asked us to imagine possible titles for the keynotes and the challenges that we would be facing: For my part, my contribution was a keynote on "Regulating Safety in the Metaverse" and a session on "The Safety of Healthcare Nano-bots". I invite you to take a look at the rest of the article!

However, my other observation is that we don't even need to look into the future to see that the sub-disciplines and aspects of safety engineering are getting more and more interconnected and entangled (and rightly so). Even reviewing the papers and programme of this year's symposium, highlights how, in many regards, it's increasingly difficult to "break off a chunk" of a problem without it impacting on other aspects – whether that be the interaction of safety and consumerism that we heard of from John McDermid on day one, or the necessity of consideration of ethics that we heard from Paula, or the need to manage dependencies in Human Factors in Rachel's talks yesterday, or Gary's talk today of how the march of progress in multi-core processors provides challenges for safety. One person's progress is another person's headache. One person's cost-efficient solution ("we don't need LIDAR for autonomous vehicles", I hear Elon Musk say), is at the expense of another person's software complexity, and yet another's assurance claims to be addressed.

John Donne once famously wrote in his poem, "No Man is an Island"

> *No man is an island entire of itself; every man is a piece of the continent, a part of the main; if a clod be washed away by the sea, Europe is the less, as well as if a promontory were, as well as any manner of thy friends or of thine own were; any man's death diminishes me, because I am involved in mankind. And therefore never send to know for whom the bell tolls; it tolls for thee.*

(Apologies for the non-inclusive 17th Century language). As we survey the rich panoply of safety engineering and its many disciplines, as a symposium such as this allows, we might well, from whatever vantage point we take (whether that be data safety, or processor safety, or organisational safety, or any other), heed John Donne's words that challenge isolationism.

Rather than gazing from afar and perhaps thinking "phew, I'm glad that's not my problem", we should remember "ask not for whom the bell tolls, it tolls for thee!" The discipline is increasingly interconnected and interdependent. If anything, as those reports on the pandemic and the effects of lockdown have shown, the need for thinking more holistically about our safety problems will only increase in time and heighten in importance.

As well as John Donne, I'd like to end by suggesting that the words of Jesus may give us a particular perspective on the problem. The Bible records that a rich man once asked him what the most important commandments were to follow. After telling him that the most important commandment was to love God, Jesus told him that the second most important commandment was similar, but was to "love others as you love yourself" … a commandment that highlights the interconnectedness that exists amongst us all. So, if there's a final thought for me to end the symposium with it would perhaps be this, "to love other safety engineers as much as you love yourself", and alongside this "to care for other's safety problems and challenges as much as you care for your own."

Thank you.

Tim Kelly

Tim Kelly worked for over 25 years in the domain of high-integrity and safety-critical systems engineering and was Managing Director of the SCSC from 2016 to 2019. Over the years he has published many seminal papers in the field of systems safety and developed the Goal Structuring Notation (GSN). In 2019 he took a 'leap of faith' and gave up being a full-time Professor in High Integrity Systems at the University of York to become a vicar in the Church of England at Beverley Minster.