Tim Kelly's SSS'20 After-dinner Speech



First of all, I must say how delighted I was to be invited back to do the after-dinner speech at this year's symposium. I've always enjoyed this event, my first being 26 years ago.

It's now approaching eight months since leaving my friends and colleagues at the University of York, becoming ordained as a Church of England minister – a Reverend! (some people have mistakenly suggested that I just like collecting titles) and upping sticks with my wife and family to the East Riding of Yorkshire to become part of the clergy team at Beverley Minster. So, it's lovely to have this reason to be here and to catch up with old friends.

Despite speaking at the symposium many times, I've never before given the *after-dinner speech*. So this remains for me a new and daunting prospect. However, this may be one area where advice from my new vocation could readily apply. George Burns, the American comedian once said that:

> *The secret of a good sermon is to have a good beginning and a good ending; and to have the two as close together as possible.*

I think this advice probably applies quite well to a good after-dinner speech too, so don't worry, I won't be keeping you all too long from the bar.

One of my most recent talks (last week) in my role as curate at Beverley Minster has been to primary school aged children. People have asked me which is the most challenging crowd. Is it delivering a keynote at a conference or speaking to 6 and 7 year olds? Perhaps you can already guess the answer! All I will say is that 6 and 7 year olds ask some *really* good questions if you like being put on the spot! And they often have a refreshing perspective on longstanding and challenging problems. Such as the story of the teacher who was walking around observing her classroom of children while they were drawing pictures. As she got to one girl who was working diligently, she asked what the drawing was.

> *The girl replied, "I'm drawing God."*
>
> *The teacher paused and said, "But no one knows what God looks like."*
>
> *Without looking up from her drawing, the girl replied, "Well they will in a minute!"*

You might wonder, having made the leap from the world of safety critical systems engineering to the world of the Church of England, what could possibly read-across from my former career to my new vocation (and vice-versa). Well I'm going to take you on a journey of a few thoughts that I've had that connect these, perhaps at first glance, extremely diverse domains. Firstly, where better to start than a discussion of *risk*. Now, as I'm sure this audience appreciates well, risk is everywhere, risk unites us all.

As humans we are physically born, we live (variously) and then we die.

In a way, I feel much more aware of this now that part of my job involves the very beginning of life – baptism – and the very end of our earthly life – funerals. Risk is a function of living. We can't escape it. In my new role I've certainly discovered a fair few new occupational hazards: Clergy Robes (Cassocks and Surpluses – the white frilly bit with the long sleeves) mixed with candles, many candles, is definitely a hazard. And then there's the hazard of a large 12th century font, baby in one hand, with a towel and an order of service in the other and making sure that if you're going to drop one thing it's not the baby. I've also been grateful for the hazard mitigation advice of funeral directors of where and exactly how far back I am to stand to avoid falling in when conducting a grave side funeral. But back to the fundamental question of *risk aversion*. I'm going to question for a moment; should we ever really want to totally escape risk when it comes to our own experience?

I can remember a discussion with John Knight when talking about a concept that he was trying out with his PhD student at the time (Patrick Graydon), which they had called *Assurance Based Development*. The basic premise of the idea was that they wanted to have the development of a safety critical system being totally driven by the incremental development of an assurance case (or safety case to most of us). However, there was a problem. When they tried out the idea on the development of an artificial heart device, *it simply didn't work.* The problem was that the development of the safety case has as its goal (and rightly so) the continuous minimisation of risk – how could we reduce risk. And, of course, that can never work as the sole, or primary driver. It has a tendency to promote *nothing* … doing nothing … risk nothing. If in doubt, say no! Some of you may have heard me say before that whenever a company says "Safety is our top priority" or "Safety is our number one goal", they are clearly, in my opinion, *lying*. How can it be? If safety was genuinely the number one priority, in many cases the answer as to what do is simple – do nothing! Safety always has to be addressed in juxtaposition to other competing objectives. We manage the risks of high speed train travel in relation to our goal of wanting to move large numbers of people from city to city in as short a time as possible, or the risks associated with space travel in order that we can explore the wonders of the universe. Putting it this way, it can perhaps start to be seen as important that we shouldn't let safety win. We shouldn't want safety always to dominate. Safety needs to be put in its place, and perhaps we still don't have the tools to manage this. The ALARP framework focuses on risk versus cost and is not adept at managing multi-attribute tradeoffs – something once explored by my PhD student George Despotou.

This balancing of risk and reward is something that I can recognise in my move from safety to church and clergy life. I understand when some even described my move itself as an excessively risky thing to do. Why would I want to leave my secure job and career to receive less pay for potentially more hours? Why would I risk uprooting my family – new house, new schools for my boys – what could possibly be worth it? If my sole interest was the minimisation of risk, this was clearly an unnecessary move. However, the risk needed to be balanced with other competing forces – and in my case, I felt one pretty large competing force. This was something that I felt I was being clearly prompted and nudged to do. The risk of doing nothing, although the apparently safe option, was now having to be weighed against the lost opportunity of doing something that I was meant to do. Thinking about the end of that bathtub curve again, the end of life, was I going to reach the end and look back and see there was so much more to be done? Safety critical systems engineering, safety cases, and dare I say it even GSN, are not the be all and end all!

And of course, having made the move, there's the question of the appetite for risk in the life of a Christian. Jesus himself wasn't averse to a little risk. He challenged injustice and oppression where he saw it, didn't insulate himself in fancy temples and palaces but instead lived lightly on the road, and of course, he wasn't afraid to upset the authorities and the established order of things. Someone could pipe up at this point and rightly say, "and you can see where that landed him", and you'd be right to point that out. Risk was balanced against reward – just not necessarily the kind of rewards everybody associated with success – money, military and political power. You could say that a life of love, a life driven by love, looks very different to a life driven by safety and risk management. Love isn't safe – it drives us to do things that sometimes look *far* from safe.

Last autumn I was delighted to be asked to be involved in the marriage ceremony of a friend and safety engineering colleague from BAE Systems, and I was determined to see if I could get a mention of some safety and security terms into his wedding sermon. In the end it wasn't that difficult at all. You see there's perhaps few greater examples than a wedding of trust and of course, it's flip side of risk. Where the instinct of the world is so often to try to stay as safe and secure as possible, where we try to reduce risks ALARP, and to not trust anyone unless you absolutely have to, when two people get married together love and trust clearly wins over risk.

So where does this discussion of risk leave me now professionally? Well, I think the church is having to challenge itself on this very topic of risk. How should the church move forwards? Play it safe or live dangerously? Well you might guess where my thoughts start to land. To play it safe would be to change nothing, risk nothing, maintain the status quo and avoid trying or exposing ourselves to anything new – better not, it might backfire. Surely, we should minimise the risk surface not extend it? But you see the Christian church is called to a life of love, and some might say, as a consequence, called to life set with risk. It was never meant to be about power, influence, or wealth (as some might suggest from the outside). It was meant to be about love, including sometimes wilful sacrifice. (Now, don't get me started on what can be considered a reasonable risk!) I'm not about to suggest to the Church of England, following the fashion of John Knight, a new process called "Love Based Development" – but it wouldn't necessarily be a bad place to start!

And where does this discussion of risk leave the world of safety engineering? I think it shows we have to be careful about sometimes playing the safety hand too strongly, and to the detriment of other reasonable societal goals. The field is still open for the development of a new multi-attribute ALARP framework!

Now I want to move on to discussing a man that, I suspect, many of you may not have heard of before – Richard Hooker. He was a priest and influential theologian in the life of the Church of England and lived between 1554 and 1600.

Amongst other things, he was famed for, what is now known as, his *three-legged stool*. Not an actual stool, but theological framework that said *scripture*, *reason* and *tradition* all had a role in determining the thought and practice of the life of the Anglican Church of England. If you permit me to explain a little of what he thought, I think there's some merit in reading across some of his principles.

Martin Luther, the great theologian of the protestant reformation age, was a big fan of *sola scriptura* (scripture alone). This is the theological principle that Christian scriptures are the sole infallible source of authority for Christian faith and practice. Luther railed against some of, in his opinion, the accreted practices and ceremony of the Roman Catholic church. This protestant position was the one adopted and endorsed by Henry VIII. However, adding to this position, Richard Hooker introduced the other legs of reason and tradition. First, by introducing reason, he suggested that where the bible was plain and clear, it should simply be followed, but where it is not, we should be using all of our critical reasoning skills and faculties to help us determine our position. Secondly, he said (if I summarise simplistically for a moment) that the church would be unwise to completely ignore the tradition handed down to it, given that in many cases, it was the result of much discussion, debate and experience.

So, *scripture*, *reason* and *tradition*. Does this model have any merit for safety critical systems and software development and assurance? Let's tackle them one by one. Scripture … *Ah!* This is perhaps where we first become unstuck. Do we have anything approaching an analogue of scripture in the field of safety critical systems development? I'm sure many of you remember John McDermid's article – *Software Safety, Where's the Consensus?* If you haven't read it, it's worth a read. Within that paper, John highlights the many safety standards (or dare I say '*holy books*') that exist within the safety domain. Sometimes we almost seem to divide ourselves into different churches – The church of DO-178C, or the church of IEC 61508, or the church of ISO 26262. *Which one do you belong to?* Of course, unfortunately, as John highlights, they don't all agree. It's hard to adopt a 'Lutheran' position that these safety standards present an infallible source of authority when such inconsistency is present. It's also easy to provide counter examples to their scripture and verse (e.g. the ineffectiveness of using MCDC testing to reveal functional failures in testing Bayesian Networks and Artificial Neural Networks, as discussed by my PhD student Mark Douthwaite some conferences back).

When discussing the idea of this talk with Mike Parsons, he suggested that it would be great if there were some equivalent of the ten commandments for system safety. Indeed it would, but alas, no such 10 commandments exist. I've seen a few attempts online (it's worth a Google) but it's hard to have faith that these are any kind of infallible set.

Some of my work over the last ten years or so with the 4+1 Software Safety Assurance principles (that can now be found in Def Stan 00-55 and 00-56) was an attempt to provide some immutable principles that sit over and above the variations in detail of the different safety standards. However, I'd be one of the first to spot another flaw in providing such lofty principles, good as they may be. The more abstract the principles the harder they can sometimes be to apply. They need interpretation and implementation (cue discussion of reason and tradition). But before I leave the topic of standards, the safety scriptures if you will, I just wanted to flag one other connection I've made between my two worlds. Whilst I do believe in the holy and inspired position of the Bible for Christians, I also acknowledge that ultimately, the words were written down and arranged by human authors. As such we need a *hermeneutical* approach when reading the bible. Hermeneutics is the theory and methodology of interpretation, especially the interpretation of biblical texts. Alongside a literal reading of the words, we should consider the context of writing, the significance of the chosen words of the text, and the challenges of application of the text to a contemporary situation.

It strikes me that such an approach has merit in adopting a thinking approach to the use of safety standards. Safety standards, despite what some may think, do not simply appear on tablets of stone. They are written by humans, in many cases committees of humans, trying their best to capture their thinking and advice. In many cases, they are a product of their time, context and authorship. Sensibly therefore, when reading standards for contemporary application, we would be wise to consider the context in which they were originally written. We also should think carefully about their choice of words. I forget where it was, but I was particularly aggrieved when I saw a rewriting of Principle No. 2 (From the 4+1 principles) which I originally stated as being that *the intent of safety requirements should be preserved throughout system development.* The rewrite simply paraphrased this as: *requirements traceability should be maintained*. No … no … no! My original wording was carefully chosen and meant something. Alter this wording at your peril. Finally, a critical mind is required when thinking about how best to apply the requirements of a safety standard to a current project. To apply unthinkingly the letter of the law, rather than think how best to understand and apply the intent of the law, would be a mistake, and so easily could miss the point – e.g. congratulating ourselves on a SIL 4 Artificial Neural Network inference engine that perfectly executes faulty inferences learnt through poorly selected data.

And so to *reason*. This is an easy one for me in terms of its merits for safety engineering. If anyone knows anything about what I have attempted to promote through the development and application of the Goal Structuring Notation (GSN), it was the clear application of reason and hopefully (when done well) critical thinking skills. In the domain of theology, Hooker said that we should never be afraid to test what we read and inherit against the whole armoury of our critical thinking and reasoning skill. Similarly, it is essential to the development and assurance of safety critical systems that reasoning is explicated, and tested. This should be the main aim of safety case development. Two of my SCSC newsletter articles come to mind – *Are Safety Cases Working?* and *There's No Substitute for Thinking*. The first of these captured my pre-Haddon Cave concerns of situations where safety cases somehow were missing the mark through becoming mundane, routine, or simply an end in themselves. The later article, *There's No Substitute for Thinking* was written in response to suggestions from some at the time, that all we really needed was safety evidence and what really was the point of this argument stuff anyway, and suggestions that all would be well if we could just persuade people to reduce their safety justifications to a few sides of A4. Both positions terrified me at the time because they served to diminish the position of exposing and criticising the otherwise implicit reasoning as to why people believed their position of acceptable safety. So, I'm with Richard Hooker – *reason* is a key pillar!

And then to *tradition*. In Hooker's case, he wanted to encourage respect for the handed down traditions of the church. They were often there for good reason. They had been found to be useful practices. As with reason, I don't believe it's difficult to see the utility of this concept when read across to the safety domain. Notwithstanding my earlier comments of sometimes needing a hermeneutical approach to reading safety standards, safety standards *do* capture much collective wisdom. Another of my biggest fears of people unthinkingly adopting a safety case approach, was that the safety case author would simply eschew and reject all existing safety guidance and standards "Don't worry I'll do it my way" (indeed this was one of Nancy Leveson's erroneous strawman objections to the safety case approach). I would say instead, that it's a foolhardy safety engineer that says they can ignore the body of knowledge contained in existing safety standards.

I'm a fan of Hooker's three-legged stool, and not just because I'm a good Anglican. Although I've talked about how each leg is useful and has read-across when applied to the safety domain, it is perhaps the concept of the stool itself that is perhaps the most useful thing – being willing to hold these three things in tension. I've already mentioned how in the safety domain, false oppositions have sometimes been manufactured between different legs. Such as, it's safety standards or safety cases, but not both – a hopefully obviously fallacious position. We are required to hold the positions in tension and check them against one another. Reason should not be allowed to overrule fundamentally understood principles. Tradition shouldn't be blindly followed if it runs contrary to reason or defies critical investigation.

This talk has given me only a chance to scratch the surface of the links that I find myself making as I settle into my new vocation. My thoughts on the importance of robots that are capable of following Jesus' commandment to us all to love one another, will have to wait for another occasion. Watch this space – although I have little desire to gain another academic qualification – this is the area I'm studying for my Theology master's degree. Incidentally, let me just say for now, that you have to be very careful when you put the phrase "love robots" into Google. And of course, to that million dollar question – have I found myself being able to deploy my beloved GSN in my new context? Well so far, I've yet to explicitly inflict GSN on the congregations of Beverley Minster and associated churches. However, I *have* received some positive feedback on my sermons along the lines of "Your sermons always seem very logical and easy to follow". There may just be a reason for that.

Finally, given that I've been talking about the relationship between my former and present careers, I wanted to end with one particular joke that struck me as being appropriate:

> *An engineer dies and reports to the Pearly Gates. Saint Peter checks his dossier and not seeing his name there, accidentally sends him to Hell. It doesn't take long before the engineer becomes rather dissatisfied with the level of comfort in Hell.*
>
> *He soon begins to design and build improvements. Shortly thereafter, Hell has air conditioning, flush toilets and escalators. Needless to say, the engineer is a pretty popular guy.*
>
> *One day, God calls Satan and says: "So, how are things in Hell?"*
>
> *Satan replies: "Hey, things are going great. We've got air conditioning, flush toilets, and escalators. And there's no telling what this engineer is going to come up with next."*
>
> *"What!" God exclaims: "You've got an engineer? That's a mistake - he should never have been sent to Hell. Send him to me."*
>
> *"Not a chance," Satan replies: "I like having an engineer on the staff, and I'm keeping him!"*
>
> *God insists: "Send him back or I'll sue."*
>
> *Satan laughs uproariously and answers: "Yeah, right. And where are you going to get a lawyer?"*