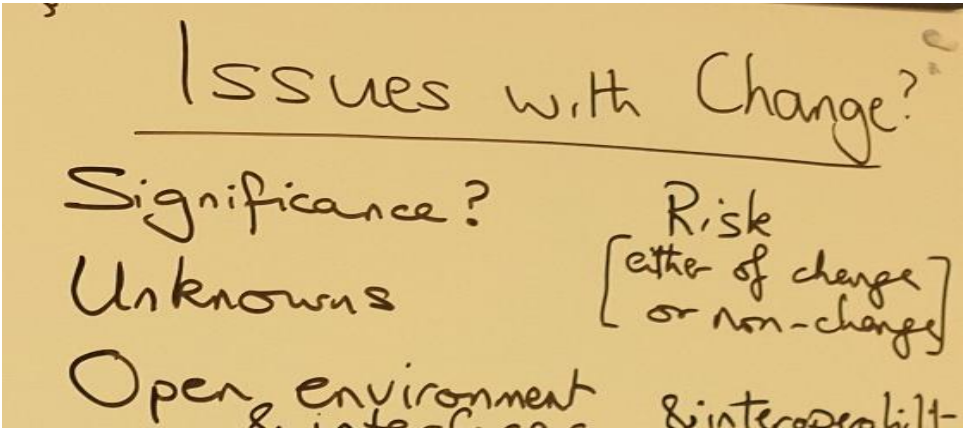
Management of Change in an Ever-Changing World



This year, the Safety-Critical Systems Symposium (SSS'25) held a number of parallel workshops covering a wide range of topics. Wendy Owen reports on a workshop that she led, supported by Stephen Bull, focused on managing change in a world of rapidly changing technology, increasing cyber threats, and adapting systems for climate change and the development / update / modification of safety cases on such projects.

Introduction

How do you manage change in a world of rapidly changing technology and ever-changing priorities? Change is of particular concern where there are – or could be – safety, security, and/or environmental implications.

Consider the roles of Management of Change (MoC) and Change Management (CM) in the context of systems being designed, built, and operated today:

- MoC is the high-level approach i.e. policy, strategy or framework
- CM refers to the detailed process of managing changes

It is not that significant technological changes have not happened in previous decades, they have. However, the nature, functionality and complexity of today's systems place a particular onus on traceability, auditability, and assurance, to ensure that these systems are safe and fit for purpose both for today's operating environments and those of the future. MoC and CM are important for security (cybersecurity), safety, and environmental reasons, as – done well – they capture the raison d'être of the change(s). This can then feed into the safety, security, and environmental cases.

In a world of rapidly changing technology, increasing cyber threats, and adapting systems for climate change, it is becoming increasingly important to manage change at all levels. MoC enables intelligent business decisions at every stage of the project, system and safety lifecycles. Within the MoC process, consideration is given to the delivery of outcomes or overall goals rather than specific outputs. Acknowledgement and integration of CM within companies, engineering teams and projects is increasingly important for high-quality outputs and outcomes. Both MoC and CM can better support longer-term business goals and Key Performance Indicators (KPIs) in an ever-changing world. In today's world, it is thus also important to manage change to enable outcomes, not only outputs.

However, in such a changing world and with an increasing number of KPIs linked to external factors, such as societal or environmental changes, assessments and documentation can also quickly become out-of-date. It is thus essential to link the safety case version to the system version, or any arguments in the safety case can quickly become redundant and the safety case invalidated (the same applies to security and environmental cases). Ideally, the links should be between elements in the system specification (both requirements and design) and elements of the safety case. Linking (traceability) at this level of detail means it is much easier to identify relevant elements of the safety case that need to be re-examined in the light of changes to the system.



Legacy systems being upgraded with modern technology, or adapted for reasons of climate change, are a particular example where many changes could be implemented and require significant assessment and documentation updates.

At the time of writing, developments in digital twins, cybersecurity, autonomous systems, and artificial intelligence are all 'in the picture'. Technical publications, as well as the news more generally, are now full of such stories. How safe will all these new systems be without full lifecycle traceability of their origins and builds, and a sufficient safety justification? How will they be accepted for use [by technical authorities, approval bodies, regulators and end users]?

Focus of the Workshop

The focus of the MoC workshop at SSS'25 was on how managing change relates to systems assurance and development / update / modification of safety cases. The discussion thus pertained to the design of systems and related processes, rather than organisational changes.

Attendee representation at the workshop included those who are currently working within, or who had previously worked in, sectors such as Healthcare, Energy (Nuclear, O&G), Transport (Rail, Aerospace, Maritime, Autonomous Vehicles), Defence, Retail (payment systems, Business Information Systems (BIS)), Process, Mining and Construction.

Ten had registered to attend the MOC workshop, but over twenty attended on the day. All had previously experienced, or were currently working through or considering, notable technical and/or cultural changes.

Participants were asked: What is important to your work or projects, or your industry sector?

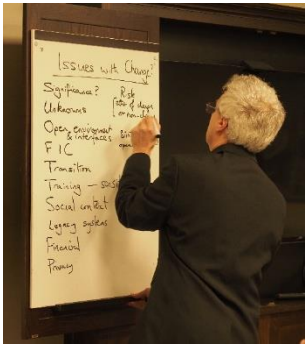
Pointers for discussions included:

- Discuss why managing changes is important, and even essential in some cases, what you need to achieve through managing changes, when you need to manage changes, who should be involved, and an outline approach
- Discuss the relationship of change management to version control and configuration management, its significance in safety-critical applications, and why it is more of a necessity in today's world of rapidly changing technology
- Organisations that adopt a continuous improvement methodology can be of concern. There is an argument that something that keeps changing is harder to assure. If anything, this tells us that it is even more important to manage change in such environments
- Changes are often related to safety, performance, reliability, or availability targets, or other KPIs; for example, tightened safety targets, or related to improved performance
- Functional change and upgrades are prevalent in industry

The following notes are a summary of the discussion, *supplemented with commentary in italics by the leader of the workshop.*

Issues With Change

It was evident that the general feeling of the group in the room – and by implication the safety engineering community – was that there are "issues" with change, with the concept of change, or of dealing with change.



This is believed to be due to the fact that safety cases, once finalised at each major stage gate of a project, tend to be "static". There is no "dynamic" approach to generating a safety case (noting that within safety cases, "dynamic hazards" may still be covered as part of the analysis). This aspect was thought as a fundamental point, almost a dilemma, behind many of the discussions. How can we deal with change if we don't have a dynamic safety case? *(it was thus very timely that one of the academic papers presented in the following session in the same room, the Young Engineer competition, covered exactly this topic!)*

Another fundamental observation was that many participants in the room did not immediately realise they were, in fact, working on changes. There is a school of thought that all developments, whether changes to an existing system or the creation of a completely new system, should be regarded and managed as changes. The argument is that even for a new system, this forces you to think about what changes will affect stakeholders and what will happen in the environment of the system. This approach can be very successfully applied to all sizes of systems.

The introduction of a change to a system or within a project introduces a change – or at the minimum a review – to the case for safety. *As we appreciate, lots of changes take place*

within projects, and also once systems are in-service, so on reflection it is no surprise that safety engineers have issues with changes, because every change that happens has to be scrutinised to a greater or lesser extent.

Other highlighted discussions have been grouped under the following headings:

The Change Itself

- Significant changes or the significance of the change. More significant changes tend to imply a significant amount of work required to update the safety case
- Risk of change. Either of the change itself or, conversely, of not doing the change
- Unknowns. Some changes can result in unknown, uncertain or unpredictable hazards. To pick these up, or at least reduce the likelihood of them, it's important to avoid group-think and have, for example, very diverse teams in HAZOPs (Hazard & Operability Studies) and design reviews. Workshops should occur before the change – SWIFT (Structured What-If Technique), HAZOPs etc. capturing the change, as well as the diversity of perspectives of the change. "Pre-mortem" rather than "post-mortem" should be the norm
- Unquantifiable changes. Not knowing the impact of greatest risk, which could be unquantifiable, is a concern (c.f. Rumsfeld Matrix)
- Innovation. It is accepted that changes due to innovation can be good; but innovation done badly can also result in potential harm. "Over-innovation" with lack of safety foresight was cited as a particular concern.
- FIC (first in class)/FOAK (first of a kind). Sometimes a change represents a "first". Something new in the operational picture, something added on for the first time, something innovative or wholly different to what was there previously. Managing FIC/FOAK is a particular challenge for safety analysts as there is often no or little comparable data, or similar systems or applications from where to draw confidence
- At the opposite end of the spectrum are changes to Legacy Systems – dealing with obsolescence, add-ons and updates to legacy systems, sometimes decades old (or in extreme cases, hundreds e.g. Victorian era railway tunnels being fitted with digital asset monitoring equipment)
- Reliance on tech. Over-reliance on technology was also noted, leading to loss of personnel or corporate knowledge



The processes around the change

- Anticipation of change. Anticipation of a forthcoming change is helpful, particularly for "intimidating" changes (for example, those regarded as significant in themselves, ones anticipated to involve a significant amount of work, or that could have a major impact in some form)
- Interoperability. Systems are becoming ever more integrated and inter-connected, and a push towards interoperability is a change in itself. Managing a shift towards interoperability can be complex, across boundaries, across operators, across countries and can put limits on what can be changed if interoperability is to be maintained
- Open environments and interfaces. Some changes result in open or larger interfaces

with other systems or environments. These can be hard to manage, or hard to control
- Operating environments. Major changes to operating environments (which often also include maintenance regimes) require significant management of change generally, and thus significant management of safety during the transition periods
- Changing environments due to climate change are already having impacts on systems design, and by implication, safety and dependability cases
- Transitions. These are situations where the change is effectively a shift, be that gradual, progressive or step-change, that requires attention and requires safety management, to enable the transition to happen safely
- Social context. Sometimes changes also have a social context e.g. accessibility
  Financial impact. Changes often have a financial impact
- Complement of stakeholders. A full complement of stakeholder should be identified as early as possible. There can be different drivers of/for change, and openness is required for safety reasons

Personal Impact

- Loss of agency. A few participants reported a loss of control or independence of their work when changes were made. It would be worth exploring why this happened or was perceived to have happened
- Training, sensitisation and awareness. Informing people that there has been a change to the system or operating environment is key to the success of the implemented system or update
- Privacy. In some circumstances, there are potential privacy, (personal) security or GDPA (general data protection act) issues alongside the system change
- Customer perspectives, including any surrounding deceptions (e.g. hyping or falsification of product claims), also need to be accounted for.

Regulation of Changes



Acceptability of the change – by an official safety approver/regulator, a business, operator, or the public etc (depending on system purpose) – becomes more difficult the more complex the change. Demonstrating the As Low As Reasonably Practicable (ALARP) principle is integral to acceptance of the change, and sometimes this (still) happens too late in the project lifecycle.

The group discussed regulation in several contexts.

- Regulatory changes on systems development
- Lagging regulations
- Regulating the unknown
- Advising the regulator

The latter three appear prevalent in the context of rapidly-shifting technologies and shifts in security threats (with safety implications).

Wrap-up

The reason many – if not arguably all – safety cases (and updates thereof), come about in the first place is due to some engineering or operational change or similar. It is certainly recognised in industry guidance that 'engineering change' is an instigator of the need for a safety case. An engineering change generally takes the form of a wider project, of course.

Safety engineers can be rather cautious about change and dealing with change. Designing for change at an early stage of project, alongside early involvement of the safety team, is preferred or essential. Safety is expensive retrospectively, but safety engineers are still often enough being called in too late in the lifecycle of a change.

Groupthink with not enough diverse thought can impact both the success of a change and its safety implications.

The why of the change, keeping evidence / audit trail and succession planning, are important. When changes occur, safety case managers and regulators are keen on experience, evidence, and being able to show that enough is in place to provide adequate assurance.

With rapid changes, standards and regulations may lag, which can cause delays or problems in presenting a good case for safety.



End Notes

Post-workshop, Wendy observed that *the workshop allocation was only an hour and, with more than double the number of people in the room than who had registered, the session became rushed.*

As the co-author of the originating paper behind this workshop (shortly to be published in the SCSC's e-journal), Keith Collyer provides the following post-workshop comment:

One thing that we did not make explicit in the paper and does not seem to have come out in the discussions is the need to define criteria for the change to be considered successful.

Wendy and Stephen concur that:

- *Further work (or workshop) includes looking at success criteria, including approvals*
- *The concept of static versus dynamic safety cases should also be given more consideration for future SSS presentations/workshops*
- *We need to develop tools for helping safety engineers to respond in a timely manner to the increasing pace of change*

Stephen remarked: *I look forward to exploring this more in a later session, because there's a lot to consider!*

The workshop was led by Wendy Owen (Independent Consultant), supported by Stephen Bull (Ebeni). Post-Workshop Review was by Keith Collyer (Independent Consultant, Systems Engineer).