# Seminar: Safe Agile Developments



**The "Safe Agile Developments" seminar was held at the Wellcome Collection in London, on 1st May 2025 and hosted by Mike Parsons. This seminar was for those introducing or using Agile techniques with safety-related developments. It was aimed at developers, change managers, safety engineers and project managers.**

Mike Parsons opened the seminar saying that there is a perception that Agile development and safety do not mix well and he hoped the seminar would help determine if this indeed was the case or whether techniques and approaches have now been developed to allow Agile principles to be used successfully on safety-related endeavours.

There were seven speakers in total:

- **Dewi Daniels**, Software Safety Ltd - 24 years on from the Agile Manifesto: What have we learned?
- **Bill Blackburn**, Consultant - Scaled Agile for High Integrity Services
- **Oumaima Fasih**, Functional Safety Engineer & Scrum Master - Bringing Agility to Functional Safety: A Practical Approach Aligned with ISO 26262
- **Fred Heath**, Faria Education Group - Can agility and safety coexist?
- **Paul Lister**, Equiniti - How Agile helps you hit the complexity bullseye
- **Núria Mata**, Fraunhofer Institute for Cognitive Systems IKS - Building blocks for the development of safety-critical automated driving functions in a holistic DevOps approach
- **Thor Myklebust**, Sintef - The AI Act and The Agile Safety Plan

## Dewi Daniels

Dewi Daniels kicked off the seminar covering the history of software development. Dewi first mentioned Dave Thomas who he had worked with in the past, and was a cofounder of the *Agile Manifesto*. Dewi's early engagement with Agile was actually in "lean" development and its principles that came from the Japanese car industry as described in books like "The Machine That Changed The World".




Dewi introduced the Correctness by Construction idea he developed when at Praxis and ran through the principles. Dewi then went on to discuss his time at Silver Software and then Verocel and Callen-Lenz Associates, his agile work and applying these to safety critical projects. Dewi said that in 2015 Dave Thomas stated that "Agile is Dead" as people had developed methodologies for agile which was what the manifesto was trying to avoid (treating agile as a noun).

Dewi then went on to discuss:

- "The Good" – testing is now fashionable, it is more responsive to change, delivery is more predictable and there are excellent tools for version control
- "The Bad & Ugly" – misunderstandings rather than failures with Agile in itself and short termism – preoccupation with current "Sprints"

Dewi then went on to discuss applying Agile principles to safety-critical software development and said it is fundamentally different from commercial software, particularly in testing, where 40-60% of a safety project will be spent on verification. Formal methods and supporting tools are used more often in safety projects.

Dewi said that after 24 years of the manifesto, the age of early adoption is over and he concluded that, in his experience, Agile principles can be applied to safety critical systems.

## Bill Blackburn



Bill was our second speaker of the morning covering high-integrity services and in particular how Agile can scale, not specifically on safety programmes but where high integrity is paramount. Bill provided a recap of Agile and earlier methods such as DSDM and its principles which are similar to Agile principles.

Bill then introduced a diagram which is a framework for scaled agile, which showed the collection of components such as roles, and the Agile Release Train and the continuous delivery pipeline.

Bill then covered three case studies in Life Sciences, Financial Markets and Public Sector.

The Life Sciences case study was for a pharmaceutical company operating in a highly regulated industry that recognises the importance of safety, which is called Pharmacovigilance. For this project, the focus was on product assurance and compliance. Bill worked on evolving the business to be more Agile such as improving management of supply chains and ensuring there is an Agile platform to work upon.

The second project was for an Electronic Swiss Exchange in Switzerland. For this project, Bill took a safety-related approach to business criticality where Agile processes were applied to trading systems.

The third case study was a policing system being replaced with a new customer management system, where he took an architecture-led approach. One misunderstanding he encountered was treating Agile as a silver bullet. Bill mentioned the government's Technology Code of Practice and he said although it doesn't mention Agile, it is aligned with those principles.

Bill concluded with the key mobilisations aspects that realise the overall framework and introduced SAFe (a knowledge base of proven, integrated principles, practices, and competencies for achieving business agility using Lean, Agile, and DevOps).

- Risk-based approaches help deliver benefits of agile with assurance
- There are good industry practices
- Collaborative culture and right skills are imperative
- Regulators need to be on board and need a platform

## Paul Lister



After a coffee break, Paul Lister from Equiniti discussed how agile can help manage complexity. He started by defining complexity with models of interactive "agents" in complex networks. Paul introduced the idea of "Safety First" where risks of unwanted agents are mitigated and detected and removed. But no system is truly closed, and work "as imagined" is not often "work as done" and doesn't cover emergent behaviours.

The new processes such as "Safety II" accept this and protocols are emergent based on work done and accidents don't have a single cause.

Paul introduced a four-level scheme for the levels of understanding and control for an endeavour and mapped this to the 4 important aspects of Why?, What?, When? and How? as seen on a 'bullseye' diagram and he gave real-life examples of different scenarios.

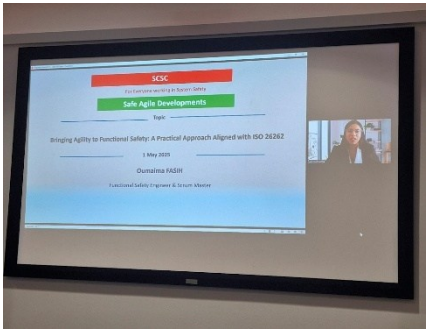
Paul showed how the principles of the Agile Manifesto can help in each of the four area and summarised the principled as Outcome of Output and Trust over Control. He then covered "Lean" principles and in particular cutting out waste and focussing on generating value.

Paul then introduced "Scrum" with the focus on building small things and having small teams with the appropriate skills and doing the work in small amounts of time.

The next stage is then examining what has been done that requires transparency, inspection and adaptation and a number of "Scrum events" (planning, daily scrum, sprint review and retrospective) effectively using complexity to fight complexity. Paul concluded with key takeaways:

- no matter the task it happens in the open
- understand complexity with visualisation
- utilities Agility to mitigate risk and inspect and adapt

## Oumaima Fasih




After lunch we heard from Oumaima Fash from Stellantis presented remotely and discussed a practical approach to bringing agility to functional safety aligned with ISO 26262.

Oumaima introduced her talk by asking 'Why Agile?' and said that agility is now highly prevalent in everything we now do from online ordering to over the air updates in cars and so there is a desire and benefits for agile approaches. But this level of agility brings challenges for safety and she showed that there has been a marked increase in vehicle recalls.

Oumaima described the history of ISO 26262 – a safety standard for the automative industry and showed a process overview and 'V' model for ISO 26262. She then focussed on the V model in more detail and concluded that it is ostensibly a linear waterfall methodology. She then reprised the Agile Manifesto and highlighted the similarities and conflicts with ISO 26262, such as agile having minimal upfront planning where ISO 26262 requires detailed planning before development begins.

Oumaima then showed how safety roles and terminology apply to the Scrum methodology. For example, there is a Safety backlog (outstanding work to be done) along with Safety Validation acting as a kind of Sprint Retrospective.

Oumaima concluded with six tips:

- Start small, scale gradually
- Engage cross-functional teams early
- Establish safety backlog early
- Regular reviews and feedback loop
- Address compliance in the Agile Safety Model
- Use digital tools to help generate the documentation required by ISO 26262.

## Fred Heath




Fred Heath from Faria Education Group was next up and asked the broad question of whether Agile and safety can co-exist. Fred said he was not a safety engineer as such but works in a safety-related educational environment where children's data needs to be protected.

Fred started by explaining the issues that led to the crash of the Mars Climate Orbiter where there were discrepancies on the units of measurements being used between two teams. Fred stressed that nothing in the manifesto conflicts with safety objectives and he thought Scrum was the best framework for safety-critical systems. Fred covered the benefits of Agile and mentioned SafeScrum as a successful adaption of RTCA/DO-178C. There are concerns however for using Agile in safety-related projects and Fred dispelled some of the myths and misconceptions.

Fred provided more details of the Scrum framework and the concept of splitting activities into a "sprint", the "backlog" of agreed work tasks and the general process of Plan, Implement and Inspect & Adapt and the important aspect of the "Definition of Done".

For safety-critical projects Fred said that sprint planning requires more refinement and will take longer. He then discussed and gave examples of Behaviour-Driven Development (BDD) which is a superset of test-driven development applied at the system level. As the definition is structured, a test stub can be automatically generated. BDD provides automated validation, documentation and traceability.

Fred then returned to the earlier concerns on using Agile in safety-critical projects and for each showed how each can be addressed. Fred concluded with references to his books on safety.

## Thor Myklebust

Thor Myklebust from Sintef then discussed the AI Act and the Agile Safety Plan, which is encapsulated in a published book based on interviews with 35 risk experts and 18 companies.




He described the wide range of safety projects he is involved in such as Hyperloop, transportation and offshore. Thor said that there have been a lot of changes since he started work on IEC 61508 with more companies becoming involved over time.

Thor discussed the EU Artificial Intelligence Act and presented the 4-tiered risk levels in the Act. He said there are different interpretations of the Act and showed the process for developing harmonised standards, which might take many years.

AI safety plans and cases involving AI are still in their infancy and the act is likely to change again but as with previous speakers, he stressed the importance and benefits of Agile.

Thor referred to "SafeScrum" an adaptation of Scrum for safety-critical projects but said there were challenges with collaboration between the different disciplines and in particular, there are safety planning challenges. Thor also covered challenges with software, data, documentation, compliance, procurement (reluctance to buy certified products) and AI with, for example, being bad at outliers, and explainability for different stakeholders. Thor said AI systems are more like a grey-box and you should use the information you have although some treat it as a black box.

Thor covered the pitfalls with producing a safety argument and said good design might reduce the burden on argumentation. SafeScrum can be adapted for AI lifecycles with new AI roles. Thor said that prototypes can be developed quickly in Python to show the client and then developed in RUST. There has been more use of tools but this can be a disadvantage as it may mean they need to be qualified.

## Núria Mata

The final talk of the day was given by Núria Mata from Fraunhofer Institute for Cognitive Systems. She discussed building blocks for the development of safety-critical automated driving functions. Highly automated driving imposes high demands on ensuring safety and updating vehicle functions after delivery is a challenge for safety, performance, efficiency and hence customer acceptance.




Núria said the Dev Ops methodology can be used to support the automotive development. There are challenges however:

- Need to navigate unpredictable real-world conditions
- Need to interpret vast amounts of data
- Need to make critical decision prioritising safety of all road users
- Need to test and validate Automated Driving Systems (ADS) for a wide array of real-world scenarios
- Need to ensure coverage of diverse environment conditions, traffic patterns etc.

Núria introduced the building blocks to help address these issues. In the Development Phase there is a product quality model, use of design contract an uncertainty mode and a reasoning framework for assurance arguments. She said that post-development, there will always be residual uncertainty that is handled by operation time assurance.

Núria then showed how safe DevOps works in practice and gave an example of construction detection for traffic cones. Rather than handing over to the human who may not be able to react in time, there is rather, a change in mode and deactivation of lane keeping. If this goes wrong, for example, an unknown cone not in training data, then Continuous Safety Engineering assesses the issues and this drives updates.

There is also a layered monitoring architecture for continuous safety assurance and for the operations phases, there is a managing system component covering things like missing cone detection and runtime monitors.

Núria said it looks theoretical but it has been employed in real customer projects.

Núria summarised by saying highly automated functions impose higher safety demands. Adopting a DevOps approach within field observation and runtime monitoring addresses the challenge of preserving the intended functionality. The Fraunhofer IKS framework for high-risk system supports DevOps practices for continuous safety assurance drawing on strengths of current standards.

## Mike Parsons – Discussion

Mike Parsons then hosted a general discussion starting with asking whether existing standards can be adapted for Agile?

Stephen felt this would be a challenge; for certain things we need the right level of documentation. There may be cases where you need to understand the system and its functionality before you can do anything Agile.

Mike then asked if there is a danger that engineers focus on particular sprints and lose the overall picture?



Fred thought there is a misconception that the focus is just on iterations, and there is still planning for the bigger picture.

Andy said there are challenges with attitudes between Safety and Development teams; with release pressures, safety can be seen as just compliance and a blocker. Bill thought the focus is on the product owner and perhaps training and guidance might be good.

Núria said safety cultures are critical and essential for AI and Agile/Devops helps promote the awareness through collaboration.

Tim said that he's seen high degrees of reliability on equipment and it is more often the people causing the problem and perhaps AI could be used to improve human errors.

Bill said big companies are doing more on responsible AI and firms like Amazon are doing more in this area on documentation.

Núria said it is about trustworthiness of AI. Although not 100% reliable, the risk may be acceptable.

Stephen also thought it might be more about trust and how it has been developed and confidence rather than having lots of documentation at the end.

Paul asked if we really need a paradigm change from a regulatory perspective with more active engagement from regulators on the ground during the developments – a form of "continuous regulation". Stephen agreed and said there was a precedent for this in the railway sector he was working in.

**Report by Paul Hampton, SCSC Newsletter Editor**