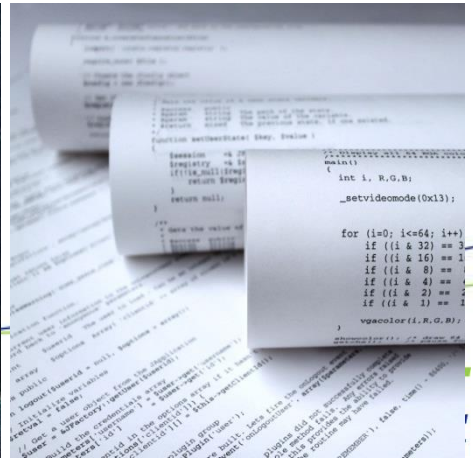
5th Scandinavian Conference on
SYSTEM & SOFTWARE SAFETY

Workshop on Safety critical software and agile development
Scandinavian Conference on System and Software Safety
2017- 05-23 Stockholm







Workshop Agenda:
Safety critical software and agile development

- **Workshop purpose**:
  Discuss how agile and safety development fit together.
  Based on **participant's experience** identify problems and opportunities in an **interactive format**.
- **13:00 – 13:10: Introductions and workshop agenda**
- **13:10 – 13:30: Drivers for agile development**
- **13:30 – 15:00: Conflicting areas**
- **15:00 – 15:30: Break**
- **15:30 – 16:45: Applying agile**
  - *Can we fulfill **regulatory requirements in a more agile way**?*
  - *What **aspects of agile** can be applied **without conflict with regulatory requirements?***
- **16:45 – 17:00: Summary**

addalot QUALITY IMPROVEMENT

Workshop participants

- Jens Gunnarsson
- Mikael Lindbergh
- Richard Wiik
- Babak Rostamzadeh
- Katarina Myrehed
- Simon Plogmann
- Nicolas Martin-Vivaldi
- Vikash Katta
- Lisa Alm
- Catarina Harde Åkesson
- Leif Hellström
- Tord Wullt
- Thomas Lidén
- Per Löfvenberg
- Tor Stålhane
- Johan Sundell
- Martin Hedén
- Sten-Åke Bergman
- Mats Ingves
- Claes-Göran Gustavsson

addalot QUALITY IMPROVEMENT

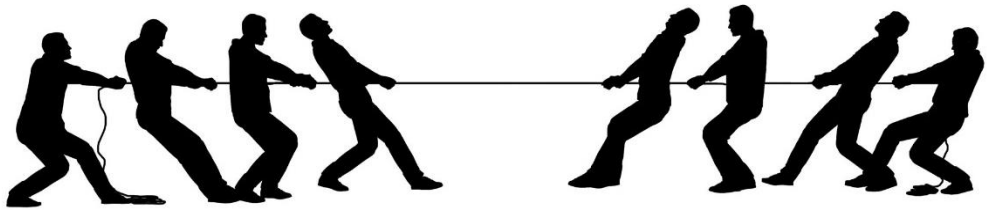
Drivers for agile development

Potential drivers for agile development:

- Time to market
- Flexibility (handle requirement changes)
- Productivity
- Customer satisfaction
- Quality
- Innovation
- Cooperation
- Visibility
- Employee satisfaction
- Latest trend…

addalot QUALITY IMPROVEMENT

Conflicting areas



- Safety standards typically include
  - Documentation
    - Product documentation (eg: req, architecture, design, och test reports)
    - Process documentation (eg: process descriptions, templates)
    - Project documentation (eg: plans, review reports)
  - Traceability between requirement, architecture, design code and test
  - Review of documents and code (with tangible output)
  - Risk activities (with tangible output)
  - Independent control of adherence

➔ Not prioritized in the Agile Maniphesto

- Safety development and Agile differences

Safety development	Agile
Safety standards invites to ”silo development” with many hand overs	Cross functional teams
Implementing Units	Implementing Features
Focus on scope, Adjust ??? Safety functions cannot be excluded	Focus on time - Adjust scope
Extensive verification and validations before customer use	Frequent deliveries, Customer feedback

addalot QUALITY IMPROVEMENT

Three important conflict areas

Assuming that the product shall be certified, there are issues that must be taken care of:

- Proof of compliance – PoC => extra documentation
- Traceability => extra work
- Changes to code or requirements => extra work

Proof of Compliance

Proof that we have done what is required by the relevant standard. Two things are important to document:

- Proof that the job is done
- Proof that the job is done properly

What is relevant proofs must be agreed with the assessor before the job is done

Trace

Traces between requirements, design, code and tests is always useful.

Without the use of tools, tracing is an expensive and error-prone activity.

Some standards – e.g., IEC 61508 – requires tracing all the way through development

Changes

When the customer's needs change, the software must be changed.

Changes is important in agile development. It is also one of the reasons why many companies use agile development.

Several standards require a Change Impact Analysis – what will be the safety consequences of the change?

Alternatively, the developers must document that no Change Impact Analysis is needed.

What is a document

ISO 9000:2015 has a new definition of “document”:

“Examples of documents are record, specifications, procedure document, drawing, report, and standards.

The medium can be paper, magnetic storage, electronic or optical computer disc, photograph or master sample, or combination thereof”.

The standards put no conditions on the format, language or formalization. We can choose whatever we think is appropriate. Our choice should be agreed with the assessor early in the project.

Conflicting areas – Discussion

addalot QUALITY IMPROVEMENT

Applying agile

- *Can we fulfill **regulatory requirements in a more agile way**?*
  Identify some regulatory aspects that must be met – and how these aspects could be implemented in a more agile manner

- *What **aspects of agile** can be applied **without conflict with regulatory requirements?***

addalot QUALITY IMPROVEMENT

Regulatory requirements in a more agile way

- Can we separate safety critical functionality through system architecture?
  ➔ Development cost vs Product cost
- Analyse the additional work:
  - What must be done initially?
  - What can be done through iterations?
  - What can be done informally in iterations, and formal in the last iteration?
  - What can be done in specific iteration?
- Can some of the requirements on documentation/activities be included in existing practices instead of creating new?

Regulatory requirements

Can we fulfill regulatory requirements in a more agile way?

Our experience is that you should

- Look at all the regulatory requirements
- See which requirements that are
  - Simple to meet
  - Difficult to meet

Requirements difficult to meet

Useful strategy

1. Decide what the **goal** of the requirement is
2. Look for other ways to fulfil the requirement's goal – ways that are more easily adapted to your process
3. Get an agreement with the assessor on how to fulfil the goal

Remember!

You can get the assessor's acceptance for how you plan to deal with the requirements

You cannot ask the assessor to suggest how to deal with the requirements

Our experience is that assessors often are fairly flexible

Regulatory requirements in a more agile way

Applying agile

- *Can we fulfill **regulatory requirements in a more agile way**?*
  Identify some regulatory aspects that must be met – and how these aspects could be implemented in a more agile manner

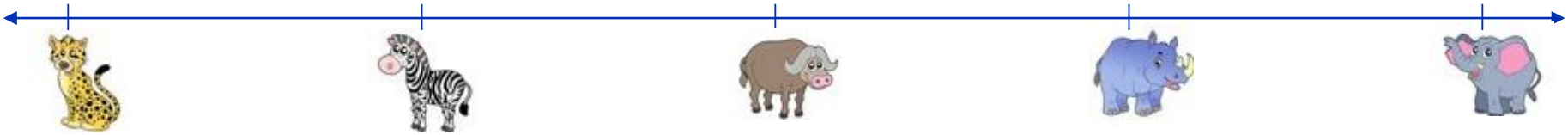
➡ *What **aspects of agile** can be applied **without conflict with regulatory requirements?***

addalot QUALITY IMPROVEMENT

How Agile can you be?

Individuals and interactions
Working software
Customer collaboration
Responding to change

processes and tools
comprehensive documentation
over contract negotiation
over following a plan



Nbr of People
Complexity
Dynamism
Team co-location

Criticality
Experience
Culture
Supplier set up

addalot QUALITY IMPROVEMENT

Can agile can be applied without conflict with regulatory requirements

- Customer focus (Product owner; Minimum Viable Product;)
- Prioritization of scope and requirements
- Planning (Iterative and Incremental)
  - Control over Req's/Features ready for development / further investigation
  - Refinement of large tasks to ensure sprint fit
  - Dependencies and Synchronization between teams
- Encourage and Manage Changes
- Agile development techniques
  - Continuous design
  - Clean code / Refactoring
  - Common code / Joint ownership
  - Always ready to deliver
  - Automated unit tests
- Cross-functional teams
- Effective documentation
- Frequent delivery
- Continuous learning

“Excellent firms don't believe in excellence - only in constant improvement and change.”

In Search of Excellence - Tom Peters

Nicolas.Martin-Vivaldi@addalot.se
+46 706 800 521

addalot
QUALITY IMPROVEMENT