Agile Lifecycle
From Concept to Maintenance

May 30, 2016

Thor Myklebust
Research and certification manager
IEC 61508 Committee member

SINTEF

NTNU

KPN skisse

Livs-syklus drift og vedlikehold av sikkerhetskritiske systemer

Standarder for utvikling av safety-systemer fokuserer mest på utviklingsfasen fram til et system er satt i drift.

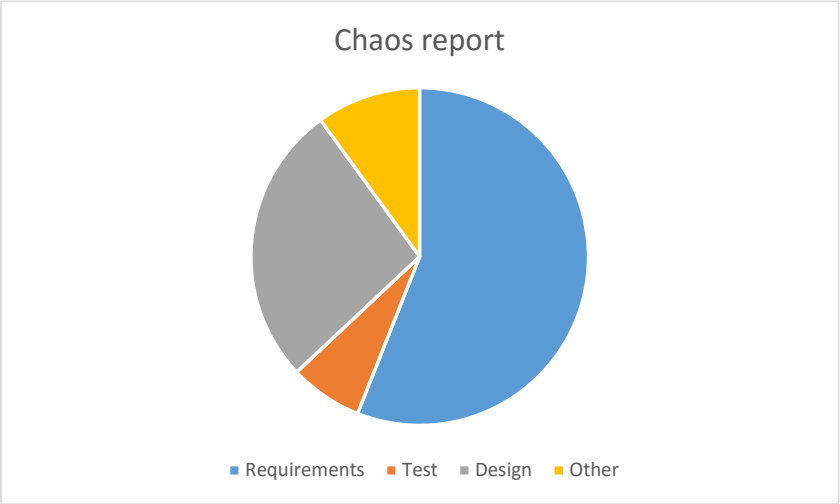
Etablere ny kunnskap om hvordan

- safety-systemer bør utvikles
- retting og utvidelser av safety-systemer *i drift* skal håndteres for å gjøre safety-systemer mer
  - sikre
  - robuste i et operativt miljø som blir stadig mer
    - komplekst,
    - sammenkoblet og
    - utsatt for angrep

Life-cycle

- Agile requirement management
  - Best practice from Agile and "Waterfall"
  - And the relation to Gate models
  - How to make requirements testable
  - Practices: "Backlog Splitting/refinement", stepwise integration, definition of done, epic, stories, communication, test driven requirement, ubiquitous language, use case

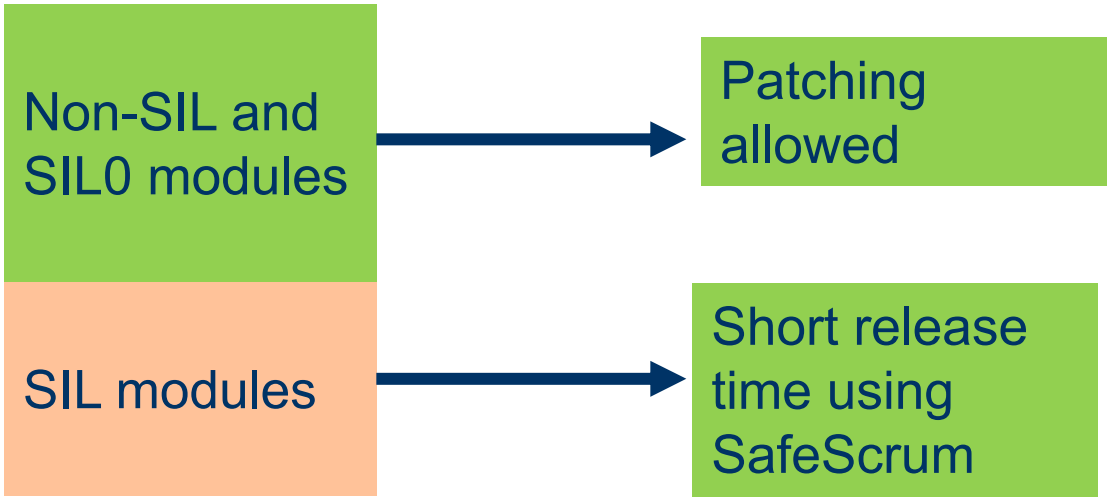
- Documentation and Information
  - Agile: Working software over comprehensive documentation
  - The Agile Safety case



Separation of Concern

Upfront activities	After sprints
• Safety requirements • Hazard/Risk • Architecture • System design • High level plans	• Remaining validation activities • RAMS evaluations • Remaining parts of "The Agile Safety Case" or similar

Frequent updates: Market needs and security



IEEE std 24765 definition. Patch:
a modification made to a source program as a last-minute fix

Regression
When you fix one bug,
you may introduce several newer bugs

Lifecycle

We also need to develop a product and we thus add software development practices

- Communication
- Planning
- Development

According to [Kniberg], sprint planning is a critical meeting, probably the most important event in Scrum

Agile practices

Agile practices	Comments
Prioritized work list	Do the most valuable work first
Backlog splitting	Safety manager may be involved in the prioritization.
Daily Scrum	Early problem solving
Iterations/sprints	Test and view working/useful SW
Incremental development together with stepwise integration	A stepwise integration as part of sprints is an integrated part of the SafeScrum approach. Often there are a few iteration sprints before an integration (increment) are performed into a testable system.
Acceptance testing and (S)TDD	Acceptance testing is of crucial importance when developing safety critical systems
Sprint planning	Additional high level plans are required together with The Agile Safety Plan
Sprint review	Necessary changes to design

Safety standards and use of an Agile method

Topics to be addressed when complying to safety standards

1. Terminology
   - general safety and agile terms together with standard definitions
2. Lifecycle requirements
3. Configuration management
4. Change Impact Analysis
5. Documentation
6. Regression testing
7. RAMS (Reliability, Availability, Maintenance, Safety)
8. Roles
9. Development tools

Why Formal Methods?

- Find errors not detected by other methods

- Less on-site tests. Reduced scope of module-tests and integration tests
  - Experience exists, not only research

- Ensure abstraction. A key element of good software design. Helps encapsulate behavior, decouple software elements, having more self-contained modules and manage complexity

Why Formal Methods?

- Current IEC 61508-3:

7.4.7 Requirements for software module testing

7.4.7.2 This verification shall show whether or not each software module performs its intended function and does not perform unintended functions.

*NOTE 2 Where the development uses **formal methods**, formal proofs or assertions, **such tests may be reduced in scope.** See Annex C of IEC 61508-7 for these techniques*

- Part of improvement of IEC 61508 ed.3
  - Receive FM draft document 6th of June 2016
  - Finished in 2019?

- DO-333:2011 Formal Methods Supplement to DO-178C:
  - provides guidance for software developers wishing to use formal methods

DO-178C Software Considerations in Airborne Systems and Equipment Certification DO-278A Software Integrity Assurance Considerations for Communication, Navigation, Surveillance and Air Traffic Management Systems