Scrum, documentation and the IEC 61508-3:2010 software standard

Author and presenter: Thor Myklebust, SINTEF ICT

Authors: Tor Stålhane, IDI NTNU
Geir Hanssen, SINTEF ICT
Tormod Wien, ABB
Børge Haugset, SINTEF ICT

Agenda

IEC 61508-3 (SW) and documentation

- Introduction
- Industrial challenges
- SafeScrum
- Trust
- Requirements
- Classification and evaluation of the documentation
- Conclusion

NTNU

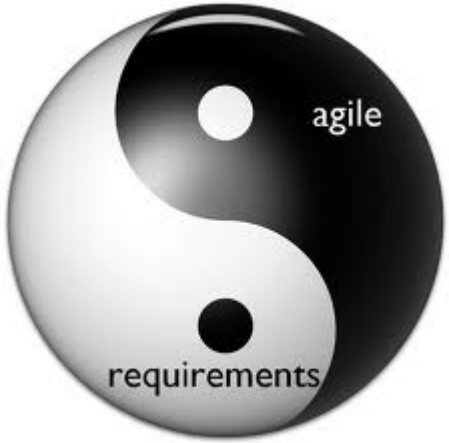
SINTEF

Introduction

- Agile methods
  - Scrum
- Several documents
- Too much time spend on documentation
- Simplicity and pragmatism
- How can information from an Agile SW development process be used to reduce the documentation costs imposed by IEC 61508-3?

Documentation

Industrial challenges:



- document-driven, process-heavy standard.
- strictly defined processes
- change is lower in IEC 61508 projects
- rigid requirements on the documentation process
- Tests must be implemented at all levels (unit, functional, system) with unique traceability

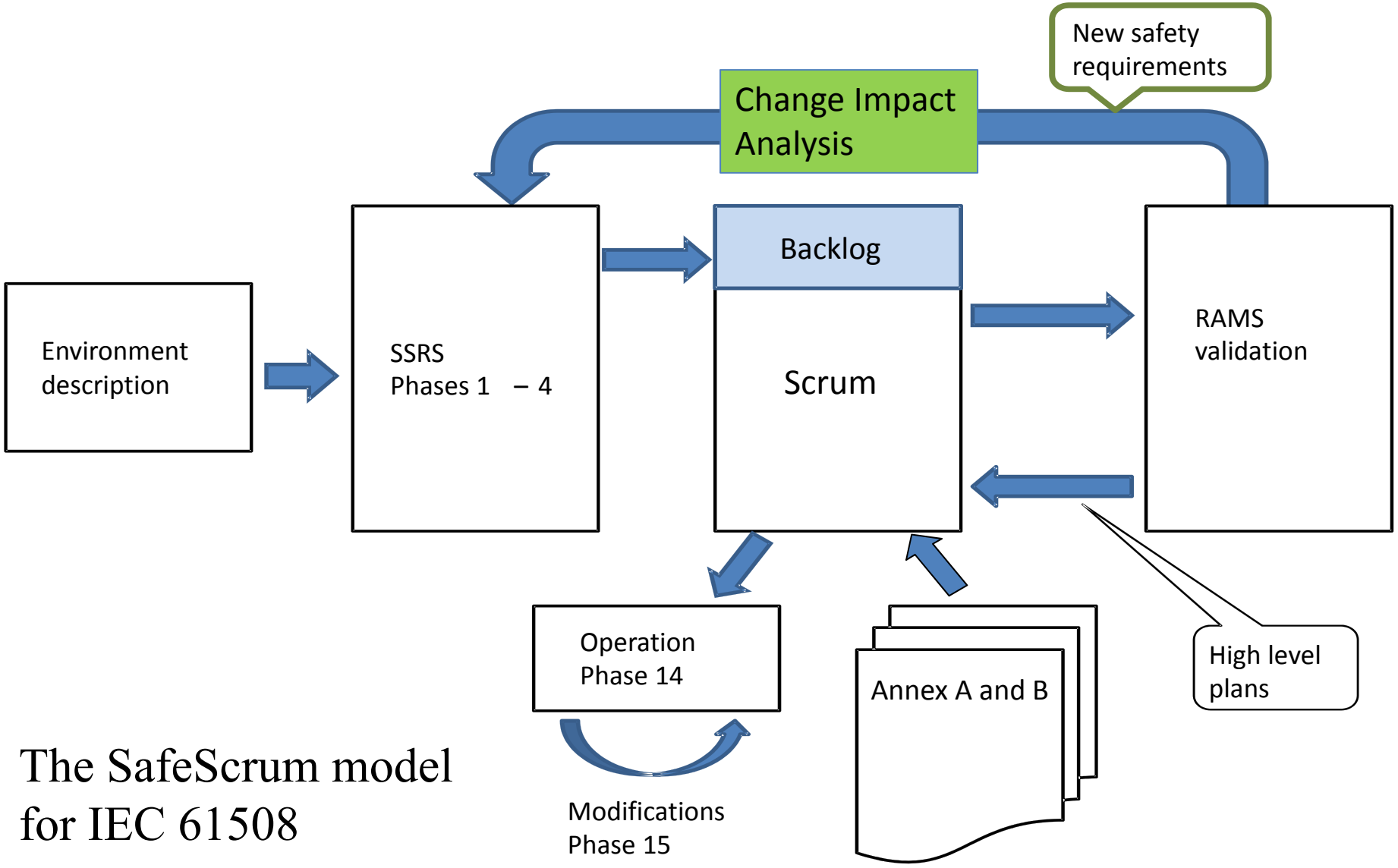
NTNU

SINTEF

Scrum

A scrum is a method of restarting play in rugby football

SafeScrum



The SafeScrum model for IEC 61508

Documentation and trust

Trust and relevant ISO/IEC standards

- The level of trust may affect the level of documentation required by the assessor

- ISO/IEC 17021:2011. Familiarity (or trust) threats: threats that arise from a person or body being too familiar with or trusting of another person instead of seeking audit evidence.

Documentation and trust

- Trust is a subjective issue

- As a result it is often important to discuss
  - Level of details
  - Pragmatism

  with the assessor early in the certification process

IEC 61508 Requirements

Targets:

- Reduce the lead time

- Reduce the number of new documents
  - Use templates, generated documents or reuse

Method related to Documentation:

- Walkthrough of chapter 5 "Documentation" in Part 1
  - 11 issues
  - Five was OK
  - One was not "OK".
  - Five needed further investigation

Requirements and what could be done

Improve Scrum by including

- traceability

- the assessor to a greater extent

These improvements are included in our SafeScrum model

Requirements

Requirements in Part 1 and what could be done:

The manufactures could improve the way they work by including

1. General agile methods

2. Reuse of documents, tools and databases

3. Include more automatic tests, especially those tests normally repeated at each sprint

Documentation

Classification of documents

- **Reusable documents** – low extra costs. Standard for reuse: IEEE std 1517
- **Combined -** Identify documents that can be combined into one document
- **Automatically generated documents** – high initial costs but later low costs. This is documents that are generated by one or more tools.
  - Examples are test results and test logs from Jira and requirements documents from e.g. the DOORSs tool
- **New documents** – high costs.

Documentation

The basic document kinds specified in the standard:

- **Specification**: Specifies a required function, performance or activity
- **Description**: specifies a planned or actual function, design, performance or activity
- **Instruction**: specifies in detail the instructions as to when and how to perform certain jobs
- **Plan**: when, how and by whom specific activities shall be performed
- **List**: Provides information on events in a chronological log form
- **Report**: Describes the results of activities such as investigations, assessments, tests etc
- **Request**: provides a description of requested actions that have to be approved and further specified

Overview of document listed in IEC 61508-1:A.3
Example of a documentation structure for information related to the SW lifecycle

Main documents	Comments
11 reports	The standard ISO/IEC/IEEE 29119-3:2013 includes procedures and templates for Test - status report, -completion report, -data readiness report, -environment readiness report, -incident report, -status report and -completion report. The std includes agile examples
6 specifications and 4 test specifications	The standard ISO/IEC/IEEE 29119-3:2013 includes both agile and traditional procedures for specifications and examples regarding Test design, Test case and Test procedure.
4 plans	Validation, safety (can be based on e.g. EN 50126), verification and functional safety assessment
4 instructions	Development tools and coding manuals User, operation and maintenance instructions Modification procedure
2 descriptions	SW architecture design and SW system design

Documentation

Class	Comments
Reusable	Reusable documents should be made more generic by the manufacturer. See e.g. IEEE std 1517:2010 "Reuse processes"
Combined	12 documents can be merged to four documents. • References are simplified. • The general parts are often the same. • The relation between activities etc., is more visible.
New documents	Discuss with the assessor <u>Templates and examples:</u> For some documents templates and examples has already been developed as part of research, standardization and organizational work

Documentation

New documents	Manhours
New tools.	Depending on the tool and the tool class > 30 manhours
SW safety validation	> 40 manhours
SW modification request	> One manhour
SW modification impact analysis	> 40 manhours Template exists
SW modification log	> One manhour

Discussions and conclusions

The acceptance of a system that has safety critical components rests on three pillars –

1. agreements with the assessor
2. trust in the developers and
3. competent work

Agreement with the assessor includes questions as:

1. Which parts of Scrum may pose problems later in the project?
2. What is accepted as PoC for each activity?
3. Which documents are needed, in which form and when?

Conclusion

Our conclusion is simple – the requirement that we need to satiesfy when certifying a system according to IEC 61508 cannot be used as an argument against using the Scrum development process.

Only five of the documents are new documents when doing recertification.

In addition we suggest that new documents should initially be discussed with the assessor, having trust and Scrum philosophy in mind to ensure correct level of documentation.

IEC 61508-3 and documentation

Questions?

thor.myklebust@sintef.no

www.sintef.no/sjs (Railway)

www.sintef.no/IEC61508 (Certification and Consultancy)

www.sintef.no/SafeScrum (Software development)