Change Impact analysis

and the safety standard IEC 61508:2010 series

Author and presenter: Thor Myklebust
SINTEF ICT

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

N T N U

SINTEF

Change Impact analysis (CIA)

Topics

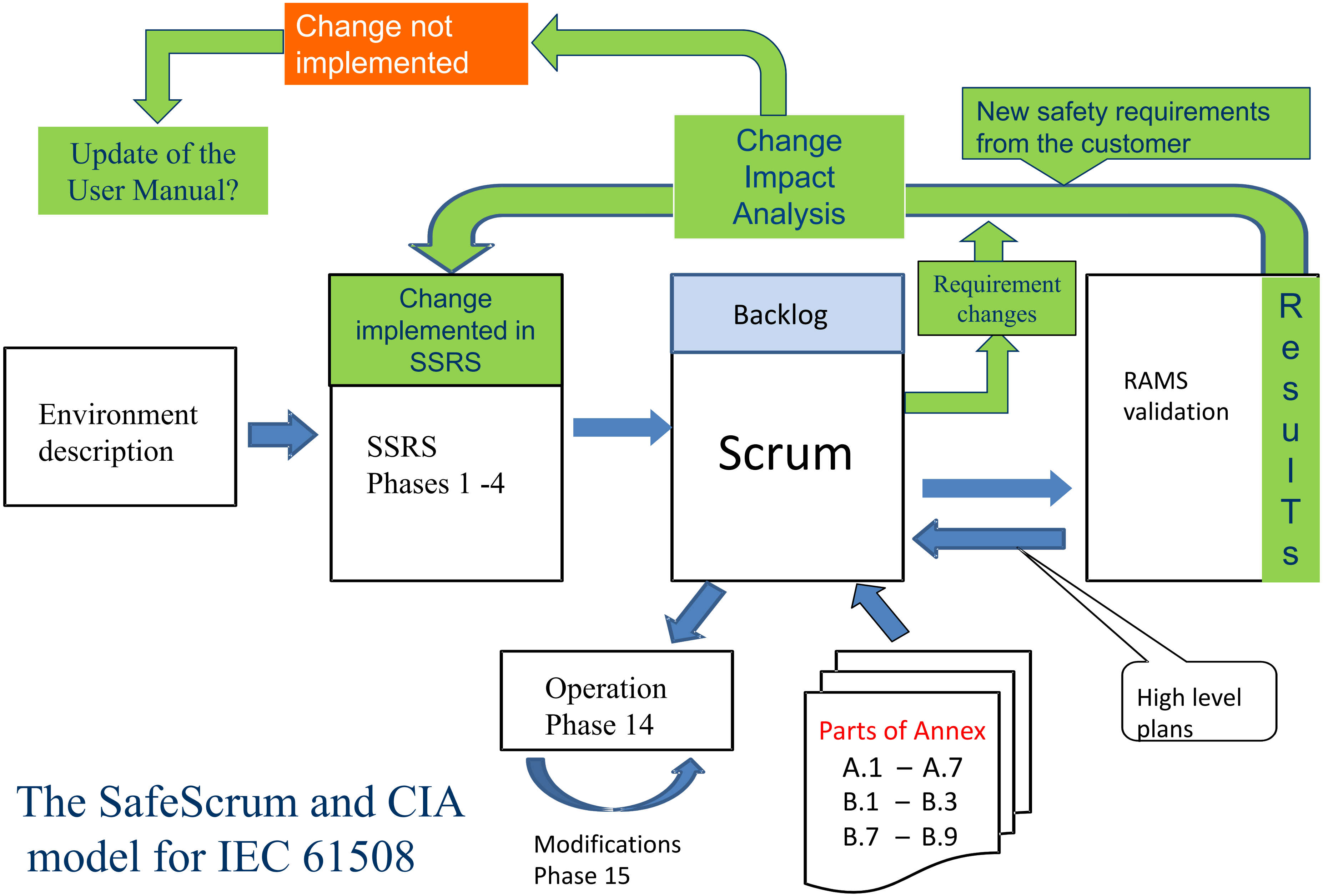
- Introduction and relevant definitions
- Scrum and CIA
- Requirements related to <u>Modification</u> and <u>Impact analysis</u>
- Related standards
- <u>**CIA Report/information** (or e.g. a tool or database)</u>

NTNU

SINTEF

Scrum

A scrum is a method of restarting play in rugby football



The SafeScrum and CIA model for IEC 61508

Related standards

ISO, IEEE and CENELEC have already issued standards presenting requirements for

safety, quality and project plans	analysis and review techniques	
Safety plan EN 50126-1:1999 ch.6.2.3.4	FMECA	IEC 60812:2006
	FTA	IEC 61025:2006
Software safety plan IEEE 1228:1994	Design review	IEC 61160:2006
Project plan ISO 10006:2003	HAZOP	IEC 61882:2001
Quality plan ISO 10005:2005	Markov	IEC 61165:2006
	RBD	IEC 61078:2006

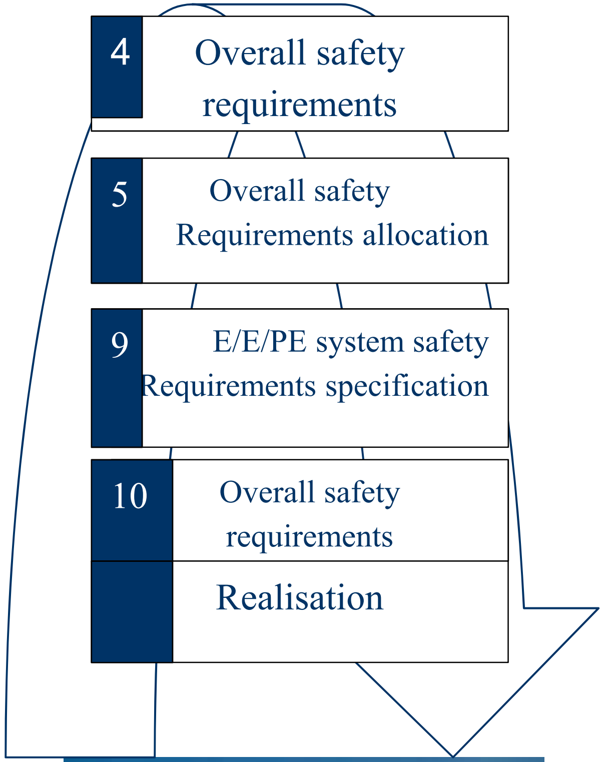
IEC 61508:2010 Requirements

Part 1:

7.16 Overall modification and retrofit

7.16.2.3 An impact analysis shall be carried out that shall include an assessment of the impact of the proposed

7.16.2.6 All modifications that have an impact on the functional safety of any E/E/PE safety related system shall initiate a **return to an appropriate phase** of the overall, E/E/PE system or software safety lifecycles.


4
Overall safety requirements
5
Overall safety Requirements allocation
9
E/E/PE system safety Requirements specification
10
Overall safety requirements
Realisation

Change Impact Analysis Report

Sources:

- IEC 61508:2010 series
- EN 5012X series (Railway)
- ISO 26262:2011 series (Road vehicles)
- EU Directives
- Standards for FMEA (IEC 60812), FTA (IEC 61025) etc
- EXIDA book: Functional Safety – An IEC 61508 SIL3 Compliant Development Process. 2011
- Several CIARs (Change Impact Analysis Reports)
- www.sintef.no/SafeScrum

Change Impact Analysis Report

Motivation for a CIAR

Source: http://en.wikipedia.org/wiki/File:ST_vs_Gloucester_-_Match_-_23.JPG

- Agile: frequent changes to existing Code and Requirements
- Satisfy IEC 61508 requirements
- Overview (for all involved parties)
- Less faults and errors
- Improved planning
- Improved information to the validator and to the assessor
- Improved process towards the assessor
- Improved process for the design team and scrum team

Change Impact Analysis Report

Content of an CIAR:

1. Title page
2. Distribution
3. Names of authors and signatories
4. Revision history
   - Summarize the changes in 1 - 3sentences
   - Version number
   - Date
5. Table of content
6. Introduction
   - Definitions
7. Modification/change request
   - Reference to database or
   - relevant "change request form"
   - "No change"

Impact Analysis Report

Content of an IAR continued:

8. **Description of existing problem or reason for change**
   - Reference to database or
   - relevant "change request form"

9. **Description of suggested change**
   - Summarice the change (or each change) being considered in one or two sentences

10. **Description of proposed change(s)**
    - Details of proposed changes are described or
    - Reference to relevant document(s)

Impact Analysis Report

Content of an IAR continued:

11. Potential safety impact without change

- Impact of existing behaviour
- Root cause of problem
- SRAC (safety related application condition) necessary?
  - EN 50129:2003
- Impact on existing systems

Impact Analysis Report

Content of an IAR continued:

12. Potential safety impact of change

- Functional Safety impact
- Hazards affected and new hazards
- EMC, ATEX, LVD, RTTE, Railway interoperability etc
  - Technical file, Technical documentation
- Areas that are not being directly changed
  - Interfaces
  - Execution order
  - Timing

Change Impact Analysis Report

Content of an IAR continued:

13. Names of participants including information related to competence (experience)
    - Selection of relevant and sufficient number of experts is important part of an Impact analysis
    - EMC experts, SW experts, HW experts etc

14. Relevant dates
    - Analysis dates
    - Meeting days
    - etc

Impact Analysis Report

Content of an IAR continued:

15. **Any deviations from normal operations and conditions that occur as a result of this change**
    - Failure behavior related to the change
    - Hazop necessary?
    - The condition list or e.g. SRAC (safety related application condition) list should be checked.

16. **Re-entry point into life cycle**
    - Required in Part 1: 7.16.2.6 and Part 3: 7.1.2.9

17. **Required verification**

18. **Required validation**

Impact Analysis Report

Content of an IAR continued:

19. Assessor aspects

- New assessor?
- Special interpretations of the standards in the new design that should be discussed with the assessor in the beginning of the project?

20. Certification and authorisation aspects

- New certification body
- More countries?

21. Required document changes

- Several reasons to include a list of all the documents affected

Impact Analysis Report

Content of an IAR continued:

22. Conclusion/summary

23. Document references

Change Impact Analysis

Questions?

thor.myklebust@sintef.no

PSAM 12
Probabilistic Safety Assessment and Management
22-27 June 2014 • Sheraton Waikiki, Honolulu, Hawaii, USA
O'ahu

www.sintef.no/sjs (Railway)

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

www.sintef.no/SafeScrum (Software development)