Disambiguation of Industrial Standards through Formalization and Graphical Languages

Daniel Dietsch, Sergio Feo-Arenis,
Bernd Westphal, Andreas Podelski

Albert-Ludwigs-Universität Freiburg

UNI FREIBURG

Validation Problem

Stakeholders

Interpretation

Interpretation

Requirements Specification

Problem Setting

Certificate Authority (CA)

Certification

Small-to-Medium sized Enterprise (SME)

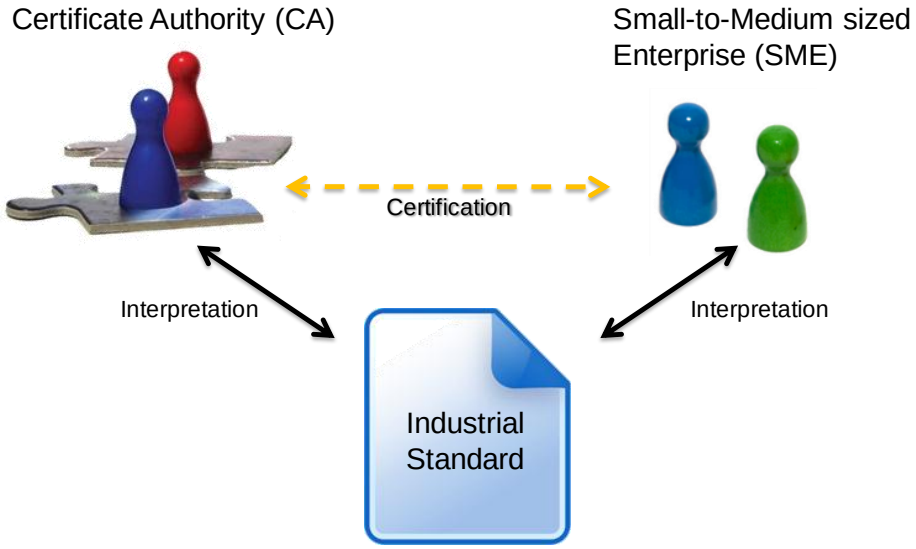
20 Employees
3 Developers

Interpretation

Interpretation

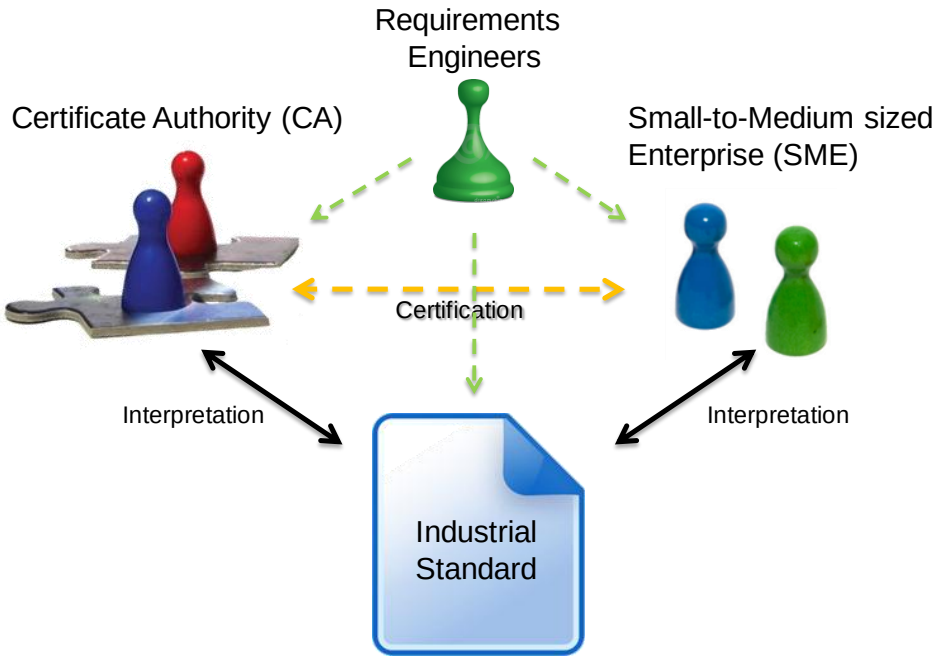
Standard
EN-54
Parts 2,25

Problem Setting



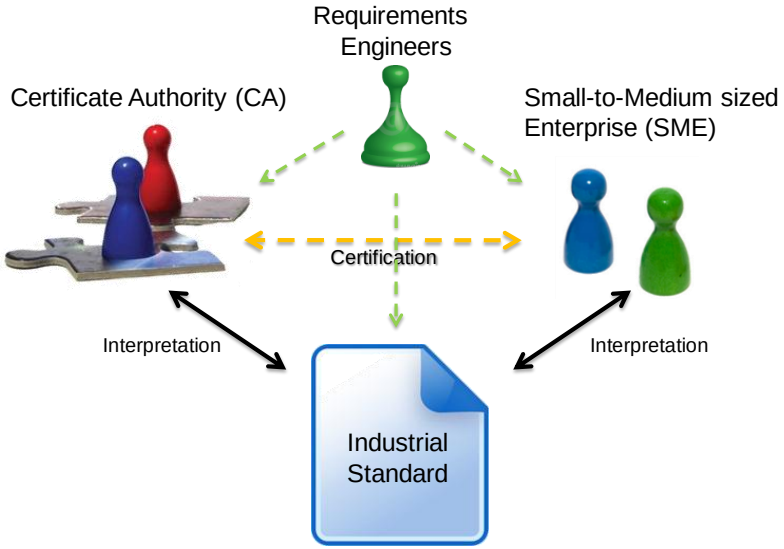
- Situation in SMEs is understudied [AEW07].
- Industrial Standards are:
  - Non-negotiable.
  - Ambiguous.
- Structural inequality: CA vs. SME.

Approach



- Gradually introduce requirements engineering methods through outsourcing / consulting for critical projects.

Approach



- Apply RE with analysis through formalization:
  - Elicitation.
  - Requirements formalization.
  - Conflict analysis.
  - Validation with both stakeholders (CA and SME).

Elicitation

UNI FREIBURG

- Create a lexicon based on the working jargon at the company.
- Extract requirements from the standard.
- Rephrase requirements in terms of the lexicon.

- EN-54: Fire Detection and Fire Alarm Systems
  - Part 2: Control and indicating equipment.
  - Part 25: Components using radio links.

Requirements vs. Test Specifications

UNI FREIBURG

4.2.6 Loss of communication
The loss of the ability of the system to transmit a signal from an HF-connected component to the central unit within the in EN-54 specified time bounds has to be detected in less than 300s and has to be displayed in less than 100s.

System requirements

8.2.8 Test to detect loss of communication on a connection
8.2.8.1 Purpose
Proof of the receiver's ability to recognize the loss of communication with a transmitter in the system. The test must demonstrate the basic function of the system.
8.2.8.2 Test procedure
The manufacturer must provide an appropriate testing instrument and sufficient details of the measures for ensuring the correct and proper operation of the HF-connection. [. . .]
The transmission of monitoring signals of a randomly selected component has then to be prevented for at least 300s, for example by disrupting the power supply of the transmitter.
During the test the maximum number of components as specified by the manufacturer has to be connected to the base station.
[. . .] The test has to be conducted on a randomly selected part and repeated twice.
8.2.8.3 Requirements
The central unit has to change its state to the fault state after the loss of communication within the in 4.2.6 specified times.

Test procedures

Lexical and Semantic Conflicts

4.2.6 Loss of communication
The loss of the ability of the system to transmit a signal from an HF-connected component to the central unit within the in EN-54 specified time bounds has to be detected in less than 300s and has to be displayed in less than 100s.

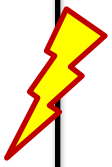
System requirements

8.2.8 Test to detect loss of communication on a connection
8.2.8.1 Purpose
Proof of the receiver's ability to recognize the loss of communication with a transmitter in the system. The test must demonstrate the basic function of the system.
8.2.8.2 Test procedure
The manufacturer must provide an appropriate testing instrument and sufficient details of the measures for ensuring the correct and proper operation of the HF-connection. [. . .]
The transmission of monitoring signals of a randomly selected component has then to be prevented for at least 300s, for example by disrupting the power supply of the transmitter.
During the test the maximum number of components as specified by the manufacturer has to be connected to the base station.
[. . .] The test has to be conducted on a randomly selected part and repeated twice.
8.2.8.3 Requirements
The central unit has to change its state to the fault state after the loss of communication within the in 4.2.6 specified times.

Test procedures

Lexical and Semantic Conflicts

7.1.3 Except for [. . .], the time required for the extraction process or the processing of signals of detectors [. . .] may not delay the display of a fire alarm state [. . .] by more than 10s.
7.1.4 The central unit has to change to the fire alarm state within 10s after the activation of a non-automatic fire detector.



8.2.3.2 Test procedure
10 components have to be triggered simultaneously by the manufacturer-supplied means in order to send or receive an alarm signal. [. . .]
8.2.3.3 Requirements
The first alarm signal has to be displayed within 10s and the last alarm message within 100s. No alarm signal may be lost. [. . .]

Formalization

- Conflict resolution through formalization.
- Simplistic formal model for real-time systems.
  - Distinction between input and output observables.
  - Model the interaction of the test engineer with the system.
- Used visual narratives for efficient validation with stakeholders.

Formalization

- $FS(t_0)$: System has switched to fully operational mode.
- $Disab_S(t_1)$: Test engineer just disabled component S.
- $Det_S(t_2)$: System just detected failure at component S.
- $Disp_S(t_3)$: Central unit just started displaying the failure of component S.

$$\begin{aligned}
&\exists\, t_0, t_1, t_2, t_3 \bullet t_0 \leq t_1 \leq t_2 \leq t_3 \\
&\quad \wedge\, FS(t_0) \wedge Disab_S(t_1) \wedge Det_S(t_2) \wedge Disp_S(t_3) \\
&\quad \wedge\, t_2 \leq t_1 + 300 \wedge t_3 \leq t_2 + 100 \\
&\quad \wedge\, \forall\, t \bullet t \geq t_0 \wedge t \neq t_1 \wedge t \neq t_2 \wedge t \neq t_3 \implies \emptyset(t)
\end{aligned}$$

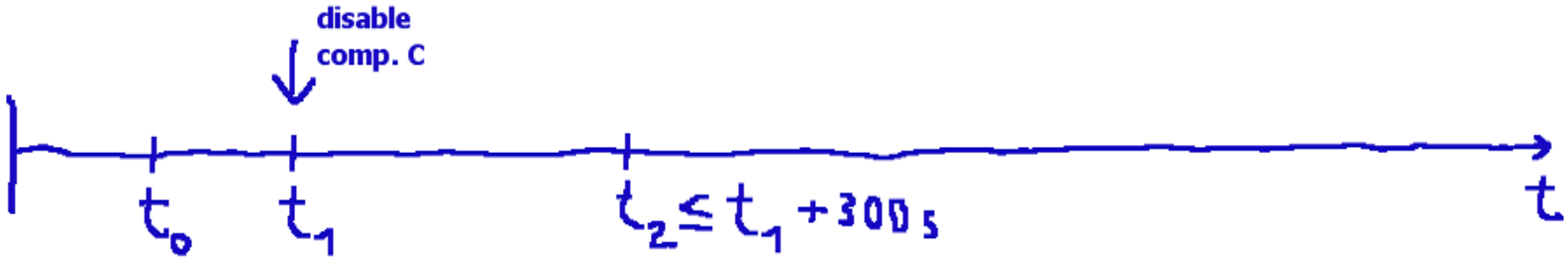
Validation

Validation

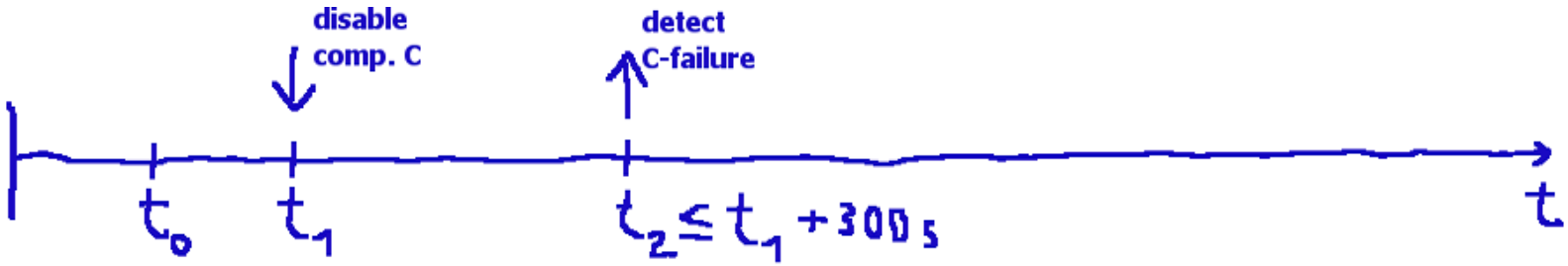
Validation

Validation

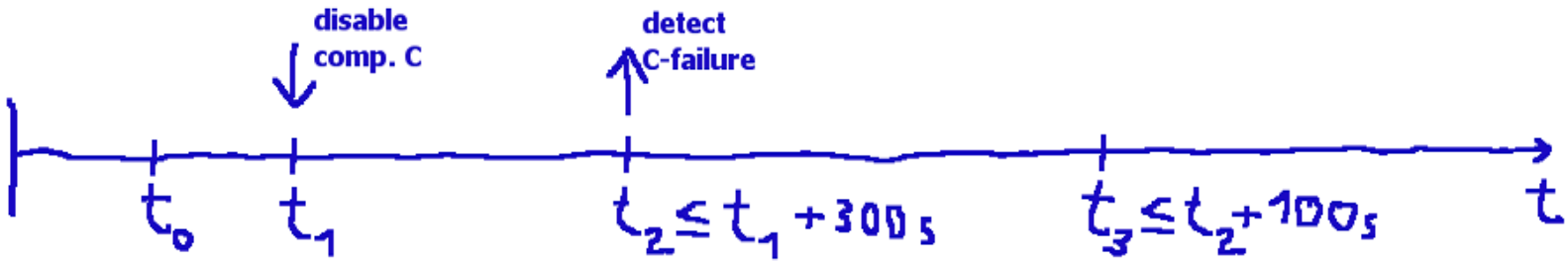
Validation



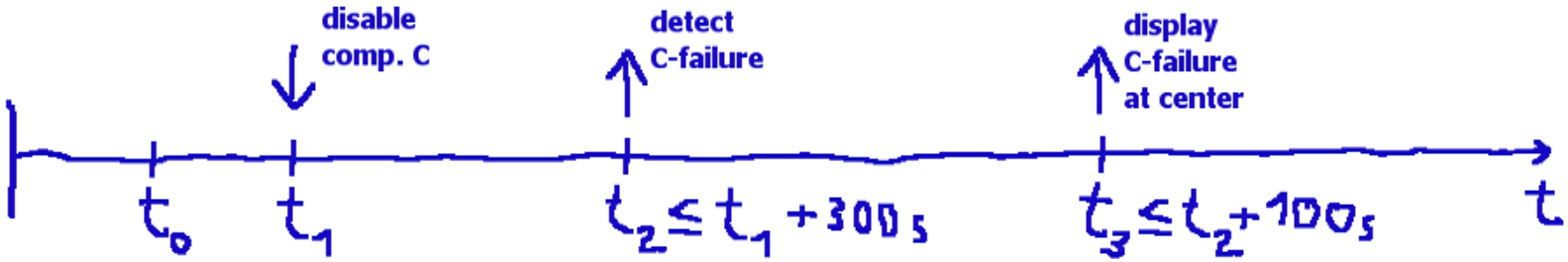
Validation



Validation


disable
comp. C
detect
C-failure
t_0
t_1
$t_2 \leq t_1 + 300_s$
$t_3 \leq t_2 + 100_s$
t

Validation


disable
comp. C
detect
C-failure
display
C-failure
at center
t_0
t_1
$t_2 \leq t_1 + 300_s$
$t_3 \leq t_2 + 100_s$
t

Validation

- Initial validation with the company (internal).
  - Workshops & Phone.
  - Resolved conflicts as far as possible.

- Validation with the certification authority (external).
  - Resolve the remaining conflicts.

Lessons Learned

UNI FREIBURG

- We can confirm that SMEs…
  - … often don't practice structured requirements engineering [AEW07], [D+10].
  - … perceive risks through changes to their processes as very large [AEW07].
  - … require evidence that changes are beneficial.
- Tried pattern catalogues [D+99], [Bit01]:
  - Not appropriate for EN 54-25.
- Good lexicons are a crucial starting point.
- Scenarios work very well.

Contributions

UNI FREIBURG

- Successfully supported an SMEs in the disambiguation of an industrial standard.
- Presented a concise and efficient means of communicating formal requirements to/between stakeholders.
- Presented a case where outsourcing RE and FM is economical for an SME.
- Provided a formalization of the industrial standard EN-54 parts 2 and 25.

Further Work

- Incorporate automatic requirement consistency checks [PHP11].

- Give formal semantics to the visual narratives to describe test cases.
  - Investigate scalability.

Thank You.

UNI FREIBURG

- Questions?

References

[AEW07] J. Aranda, S. M. Easterbrook, and G. Wilson, “Requirements in the wild: How small companies do it,” in RE. IEEE, 2007, pp. 39–48.

[D+10] Daniel Dietsch et al. “Abwicklung von Sofwareent-wicklungsaufträgen in KMU – Analyse“. http://www.salomo-projekt.de/survey-results/, 2010.

[D+99] Matthew B. Dwyer et al. Patterns in property specifications for finite-state verification. In ICSE, pages 411–420. ACM, 1999.

[Bit01] Friedemann Bitsch. Safety patterns. In Udo Voges, editor, SAFE-COMP, volume 2187 of LNCS, pages 176–190. Springer, 2001.

[PHP11] A. Post, J. Hoenicke, and A. Podelski, “rt-Inconsistency: A New Property for Real-Time Systems” in FASE 2011, volume 6603 of LNCS, pp. 34-49. Springer 2011