Lessons Learned while Formalizing ISO 26262 for Compliance Checking

Julieth Patricia Castellanos Ardila, Barbara Gallina, Guido Governatori
julieth.castellanos@mdh.se, barbara.gallina@mdh.se, guido.governatori@data61.csiro.au

This work is supported by:
ECSEL JU project AMASS
https://www.amass-ecsel.eu/

2nd Workshop on Technologies for Regulatory Compliance – TeReCom 2018
Groningen, December 12, 2018
Context

ISO 26262

Safety plan

Scrutinized by a safety auditor [Gallina et al, 2018]

FCL Specification

• Represent legal requirements.
• Automatic reasoning.

Formal Contract Logic (FCL) [Governatori, 2005]

Regorous [Governatori, 2015]

TeReCom 2018-Groningen, December 12
Talk Outline

1. Background
2. Formalization-oriented pre-processing of ISO 26262
3. Illustrative example
4. Conclusions and future work
1. Background
2. Formalization-oriented pre-processing of ISO 26262
3. Illustrative example
4. Conclusions and future work
Background

ISO 26262 [ISO, 2011]

1. Scope
2. N. References
3. Terms
4. Requirements for compliance

Tailoring  Tables

From clause 5

X. Clause Title
X.1. Objectives
X.2. General
X.3. Prerequisites
X.4 Requirements and Recommendation (R&R)
X.5. Work Products

Notes  Examples
Background

Formal Contract Logic (FCL) [Governatori, 2005]

- Unique id
- Conditions of the norm
- Normative provision

Obligations
- Prohibition
- Permission

Superiority relation

Safety Compliance Pattern (SCP) [Castellanos et al, 2017]

Describe commonly occurring normative safety requirements.

Example:

**Pattern:** AddressPhase

Obligation of addressing every phase of the safety lifecycle

\[ r: \Rightarrow [O]address\{Phase\} \]
<table>
<thead>
<tr>
<th>1. Background</th>
</tr>
</thead>
<tbody>
<tr>
<td>2. Formalization-oriented pre-processing of ISO 26262</td>
</tr>
<tr>
<td>3. Illustrative example</td>
</tr>
<tr>
<td>4. Conclusions and future work</td>
</tr>
</tbody>
</table>
Formalization oriented pre-processing of ISO 26262

Identify essential normative parts

Identify repetitive structures

Document SCP
Formalization oriented pre-processing of ISO 26262

Identify essential normative parts

Identify repetitive structures

Document SCP

1. Scope
2. N. References
3. Terms
4. Requirements for compliance

From clause 5 = Phases of the safety process

X. Clause Title
X.1. Objectives
X.2. General
X.3. Prerequisites
X.4 Requirements and Recommendation (R&R)
X.5. Work Products

Tailoring  Tables

Notes  Examples
Formalization oriented pre-processing of ISO 26262

4. Requirements for compliance

- Tailoring
- Assessed rationale
  - Consecutive entries
  - Alternative entries

Phases of the safety process

- X. Clause Title
- X.3. Prerequisites
- X.5. Work Products
  - Guidance
  - Constitutive tables
- X.4 From R&R

Identify essential normative parts
Identify repetitive structures
Document SCP
Guidance example

5.4.1. **Functional and non-functional requirements** shall be made available, including:

a) functional concept
b) operational constraints.

c) ...

\[
\begin{align*}
 r \ #. a: & \Rightarrow [O] provide\{firstElementInGuidance\} \\
 r \ #. b: & \Rightarrow [O] provide\{secondElementInGuidance\} \\
 & \ldots \\
 r \ #. n: & \Rightarrow [O] provide\{nElementInGuidance\}
\end{align*}
\]

\[
\begin{align*}
 r \ #: [O] provide\{firstElementInGuidance\}, \ldots, \ provide\{nElementInGuidance\} \\
 & \Rightarrow [O] provide\{Element ConformedByGuidance\}
\end{align*}
\]
Understanding the context

Formalize Prerequisites

Formalize Title

Brainstorm

SCP

Formalize using SCP template

Select R&R

Formalize work products

Yes

No

Yes

No

Exist req.?
Talk Outline

1. Background
2. Formalization-oriented pre-processing of ISO 26262
3. Illustrative example
4. Conclusions and future work
5. Item Definition

5.1. Objectives
Define and describe the item and support its understanding ...

5.2. General
This clause establish the definition of the item with regards to...

5.3. Prerequisites
• None

5.4. Requirements and Recommendation (R&R)
5.4.1. Functional and non-functional requirements shall be made available, including: a) functional concept and b) operational constraints.

5.5. Work Products
Item definition resulting from the requirements of 5.4.

Illustrative Example

Formalization of ISO 26262 part 3: Concept Phase

Three participants:
• Expert formal approaches in legal informatics.
• Expert in Certification in the SCC
• Ph.D Student (focus in compliance checking).

The clauses mentioned model requirements in phases of the safety process and should be formalized since they represent the definition of the item with its parts and support understanding of the item.

This clause does not have prerequisite. Therefore, there is not need of modeling

\( r5: \Rightarrow [O]\text{addressItemDefinition} \)
**5. Item Definition**

**5.1. Objectives**
Define and describe the item and support its understanding ...

**5.2. General**
This clause establishes the definition of the item with regards to...

**5.3. Prerequisites**
- None

**5.4 Requirements and Recommendation (R&R)**

5.4.1. Functional and non-functional requirements shall be made available, including: a) functional concept and b) operational constraints.

... 

**5.5. Work Products**
Item definition resulting from the requirements of 5.4.

---

**Guidance**

- r5.4.1.a: performItemDefinition ⇒ [O] provideFunctionalConcept
- r5.4.1.b: performItemDefinition ⇒ [O] provideOperationalConstraints
- r5.4.1: provideFunctionalConcept, provideOperationalConstraints ⇒ [O] provideFunctionalAndNonFunctionalRequirements

- r5.5: provideFunctionalAndNonFunctionalRequirements ⇒ [O] produceItemDefinition

Verify the rule set manually since there are not available tools.

---

**Illustrative Example**

**Formalization of ISO 26262 part 3: Concept Phase**
1. Background
2. Formalization-oriented analysis of ISO 26262
3. Illustrative example
4. Conclusions and future work
Conclusions and Future Work

Pre-processing ISO 26262 allows us to:
• Identify the normative parts of ISO 26262.
• Derived a methodological guidelines for the formalization of the normative clauses.
• Discover and document a set of additional safety compliance patterns (SCP)

We plan to:
• Develop a course.
• Design and development a pattern-based rule editor.
• Combine this work with previous achieved results regarding automated compliance checking and reusability of compliance proofs.
References


