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 Worshop on Technologies for Regulatory Compliance – TeReCom 2018
Groningen, December 12, 2018

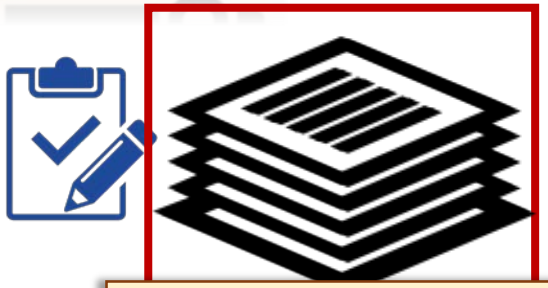
Context

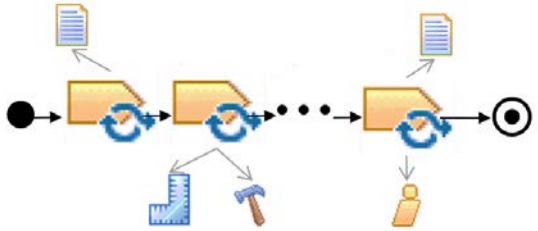
ISO 26262

Safety plan

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

Compliance Justification





FCL Specification

Regorous
[Governatori, 2015]

Formal Contract Logic (FCL) [Governatori, 2005]

- Represent legal requirements.
- Automatic reasoning.

Talk Outline

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

Talk Outline

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

Background

ISO 26262 [ISO, 2011]

Clauses

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

From clause 5

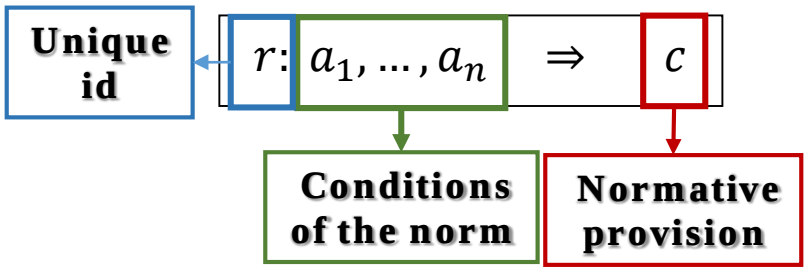
- X. Clause Title
- X.1. Objectives
- X.2. General
- X.3. Prerequisites
- X.4 Requirements and Recommendation (R&R)
- X.5. Work Products

Notes | Examples

Background

Formal Contract Logic (FCL)

[Governatori, 2005]



Deontic Notions

- **Obligations**
- **Prohibition**
- **Permision**

Superiority relation

Safety Compliance Pattern (SCP)

[Castellanos et al, 2017]

Describe **commonly occurring normative safety requirements.**

Example:

Pattern: AddressPhase

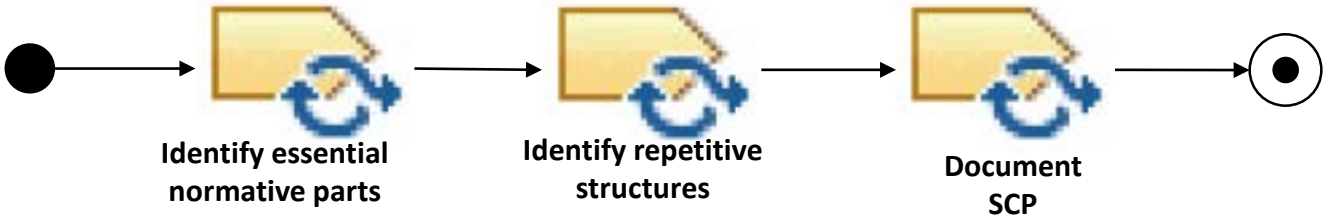
Obligation of addressing every phase of the safety lifecycle

$$r: \Longrightarrow [O]address\{Phase\}$$

Talk Outline

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

Formalization oriented pre-processing of ISO 26262



Formalization oriented pre-processing of ISO 26262

1. Scope

2. N. References

3. Terms

4. Requirements for compliance

Tailoring | Tables

From clause 5 = Phases of the safety process

X. Clause Title

X.1. Objectives

X.2. General

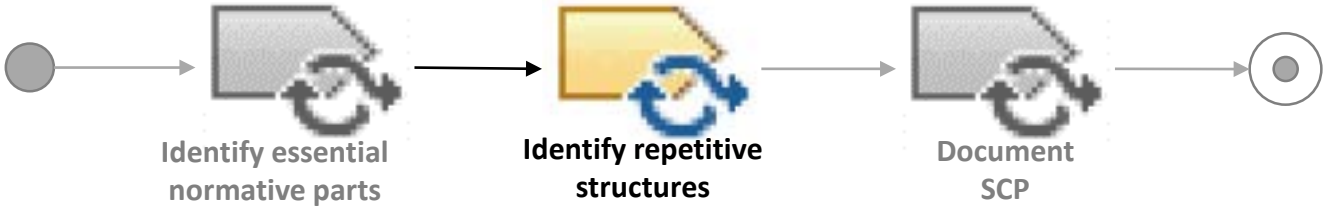
Notes | Examples

X.3. Prerequisites

X.4 Requirements and Recommendation (R&R)

X.5. Work Products

Formalization oriented pre-processing of ISO 26262



4. Requirements for compliance

Tailoring	Assessed rationale
Tables	• Consecutive entries • Alternative entries

Phases of the safety process

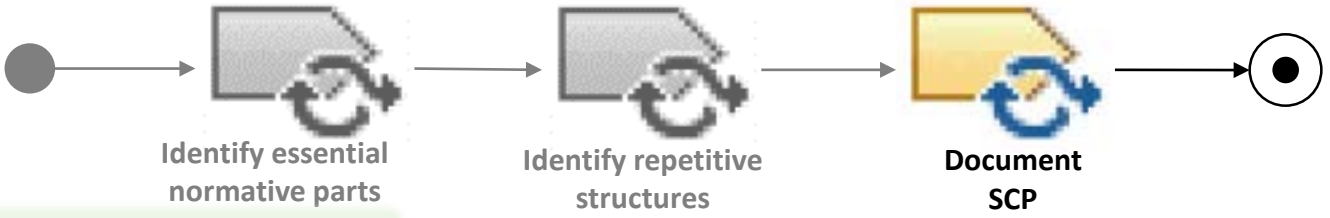
X. Clause Title + **X.3. Prerequisites**

X.5. Work Products

X.4 From R&R

- **Guidance**
- **Constitutive tables**

Formalization oriented pre-processing of ISO 26262



Guidance example

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

a) functional concept
b) operational constraints.
c) …

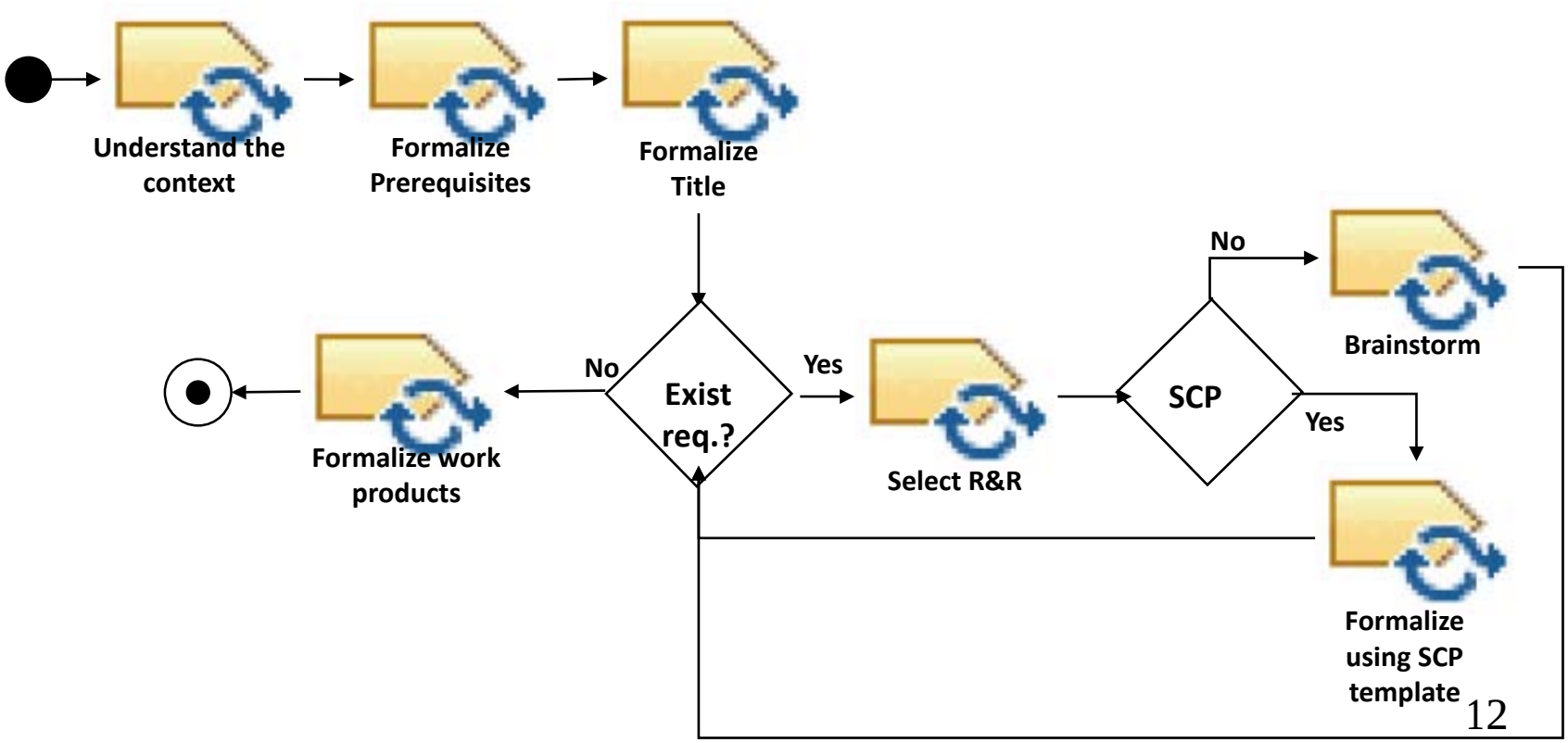
First Element
First Element
n Element

$$r \,\#.a: \Longrightarrow [O]provide\{firstElementInGuidance\}$$
$$r \,\#.b: \Longrightarrow [O]provide\{secondElementInGuidance\}$$
$$\dots$$
$$r \,\#.n: \Longrightarrow [O]provide\{nElementInGuidance\}$$

$$r \,\#: [O]provide\{firstElementInGuidance\}, \dots, provide\{nElementInGuidance\} \Longrightarrow [O]provide\{Element\ ConformedByGuidance\}$$

Formalization oriented pre-processing of ISO 26262

Methodological Guidelines



Talk Outline

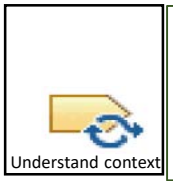
1. Background
2. Formalization-oriented pre-processing of ISO 26262
3. **Illustrative example**
4. Conclusions and future work

Illustrative Example

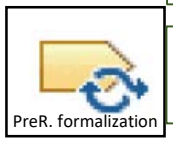
Formalization of ISO 26262 part 3: Concept Phase

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

$$r5: \Longrightarrow [O]addressItemDefinition$$

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

Guidance

r5.4.1.a: $performItemDefinition \Rightarrow [O]provideFunctionalConcept$

r5.4.1.b: $performItemDefinition \Rightarrow [O]provideOperationalConstraints$

r5.4.1: $provideFunctionalConcept, provideOperationalConstraints \Rightarrow [O]provideFunctionalAndNonFunctionalRequirements$

r.5.5: $provideFunctionalAndNonFunctionalRequirements \Rightarrow [O]produceItemDefinition$

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

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.

Talk Outline

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

[**Gallina et al, 2018**] B. Gallina, F. Ul Muram, and J. P. Castellanos Ardila, "**Compliance of Agilized (Software) Development Processes with Safety Standards: a Vision**," in *4th international workshop on Agile Development of Safety-Critical Software*, 2018.

[Governatori, 2015] G. Governatori, "**The Regorous approach to process compliance**," in *IEEE 19th International Enterprise Distributed Object Computing Workshop*, 2015, pp. 33–40.

[Governatori, 2005] G. Governatori, "**Representing business contracts in RuleML**," *Int. J. Coop. Inf. Syst.*, pp. 181–216, 2005.

[ISO, 2011] International Standards Organization, "**ISO 26262. Road vehicles – Functional safety**.," 2011.

[Castellanos et al, 2017] J. P. Castellanos Ardila and B. Gallina, "**Formal Contract Logic Based Patterns for Facilitating Compliance Checking against ISO 26262**," in *1st Workshop on Technologies for Regulatory Compliance*, 2017, pp. 65–72.

[Weber, et al, 2000] R. Weber, D. Aha, and I. Becerra-Fernandez, "**Categorizing Intelligent Lessons Learned Systems**," in *IAAAI Technical Report WS-00-03*, 2000, pp. 63–67.

[OMG, 2008] Object Management Group Inc., "**Software & Systems Process Engineering Meta-Model Specification. Version 2.0.,**" *OMG Std., Rev*, p. 236, 2008.

[OMG, 2003] Object Management Group, "**UML 2 . 0 Diagram Interchange Specification**," 2003.