Joint work with

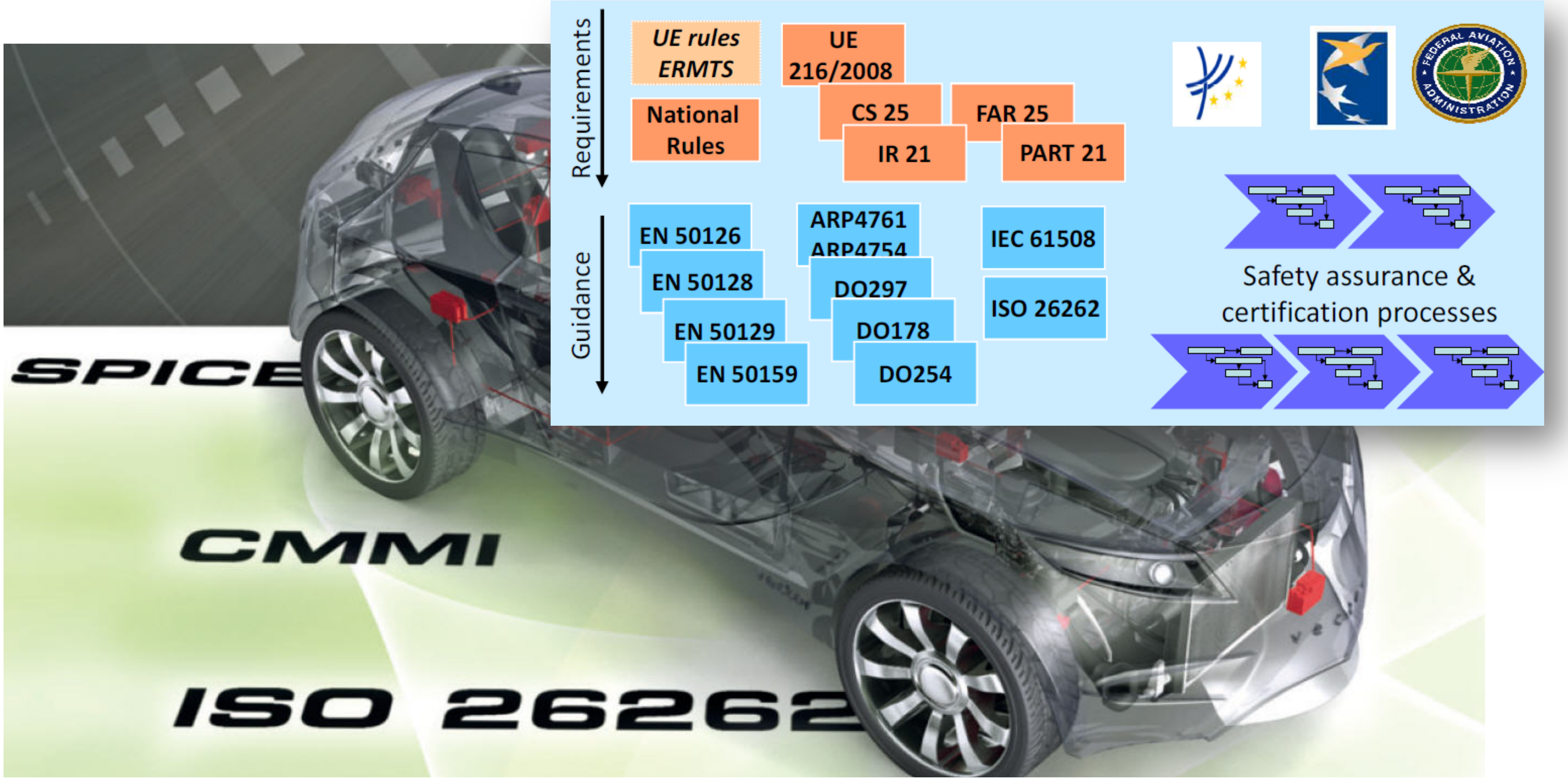
- Yaping Luo (Luna)
- Luc Engelen
- Martijn Klabbers

Model Driven Engineering

- Model Driven Engineering (MDE) is a (software) development methodology focusing on creating and using (domain) models
  - models are first class citizens

- Functional safety is the part of the overall safety of a system or piece of equipment that depends on the system or equipment operating correctly in response to its inputs, including the safe management of likely operator errors, hardware failures and environmental changes.

Background: standards



Requirements

UE rules ERMTS

UE 216/2008

National Rules

CS 25

FAR 25

IR 21

PART 21

Guidance

EN 50126

EN 50128

EN 50129

EN 50159

ARP4761 ARP4754

DO297

DO178

DO254

IEC 61508

ISO 26262

Safety assurance & certification processes

Recalls

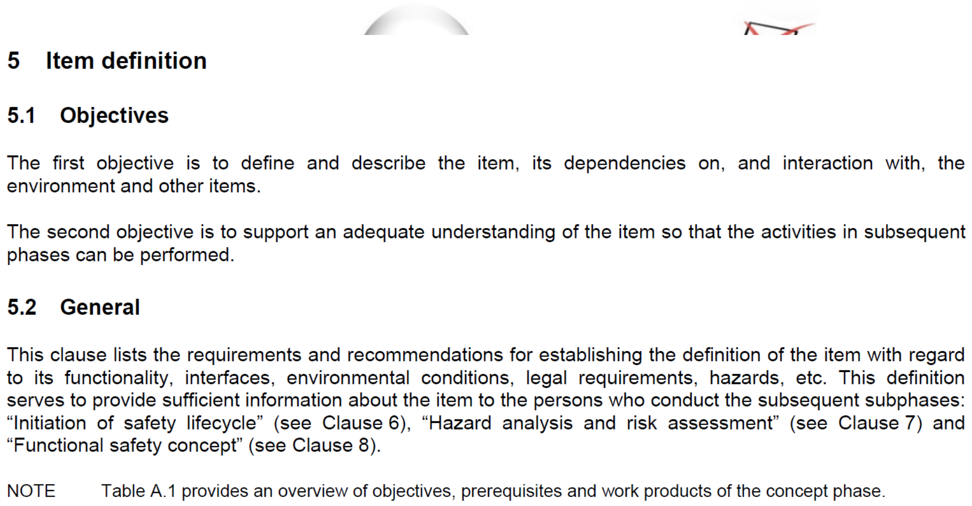
- Audi is recalling about 850,000 cars worldwide for a software problem that could cause airbags to fail to operate properly
- National highway traffic safety administration has recalls defects information: http://www.nhtsa.gov/Vehicle+Safety/Recalls+&+Defects
  - November 4: 5,412 Infiniti hybrid vehicles from 2014. Recalled for a software error which may cause the electric motor to stop working.
  - October 29: 132,223 Chrysler vehicles from 2014. Recalled for an issue with software that may disable the Electronic Stability Control.

Autonomous and connected cars

Background: certification

Compliance argument

Standards



5 Item definition

5.1 Objectives

The first objective is to define and describe the item, its dependencies on, and interaction with, the environment and other items.

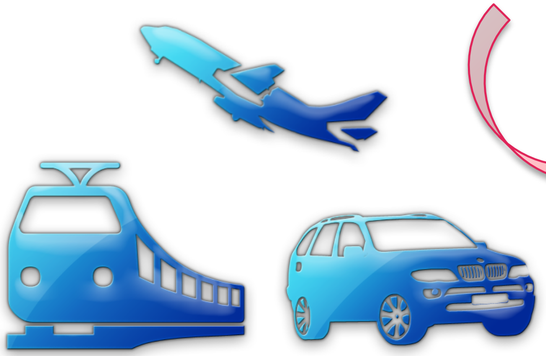
The second objective is to support an adequate understanding of the item so that the activities in subsequent phases can be performed.

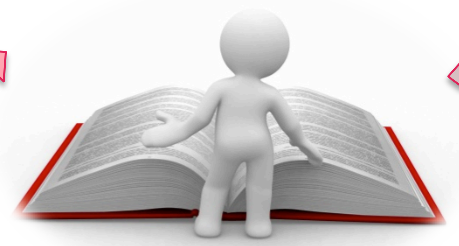
5.2 General

This clause lists the requirements and recommendations for establishing the definition of the item with regard to its functionality, interfaces, environmental conditions, legal requirements, hazards, etc. This definition serves to provide sufficient information about the item to the persons who conduct the subsequent subphases: “Initiation of safety lifecycle” (see Clause 6), “Hazard analysis and risk assessment” (see Clause 7) and “Functional safety concept” (see Clause 8).

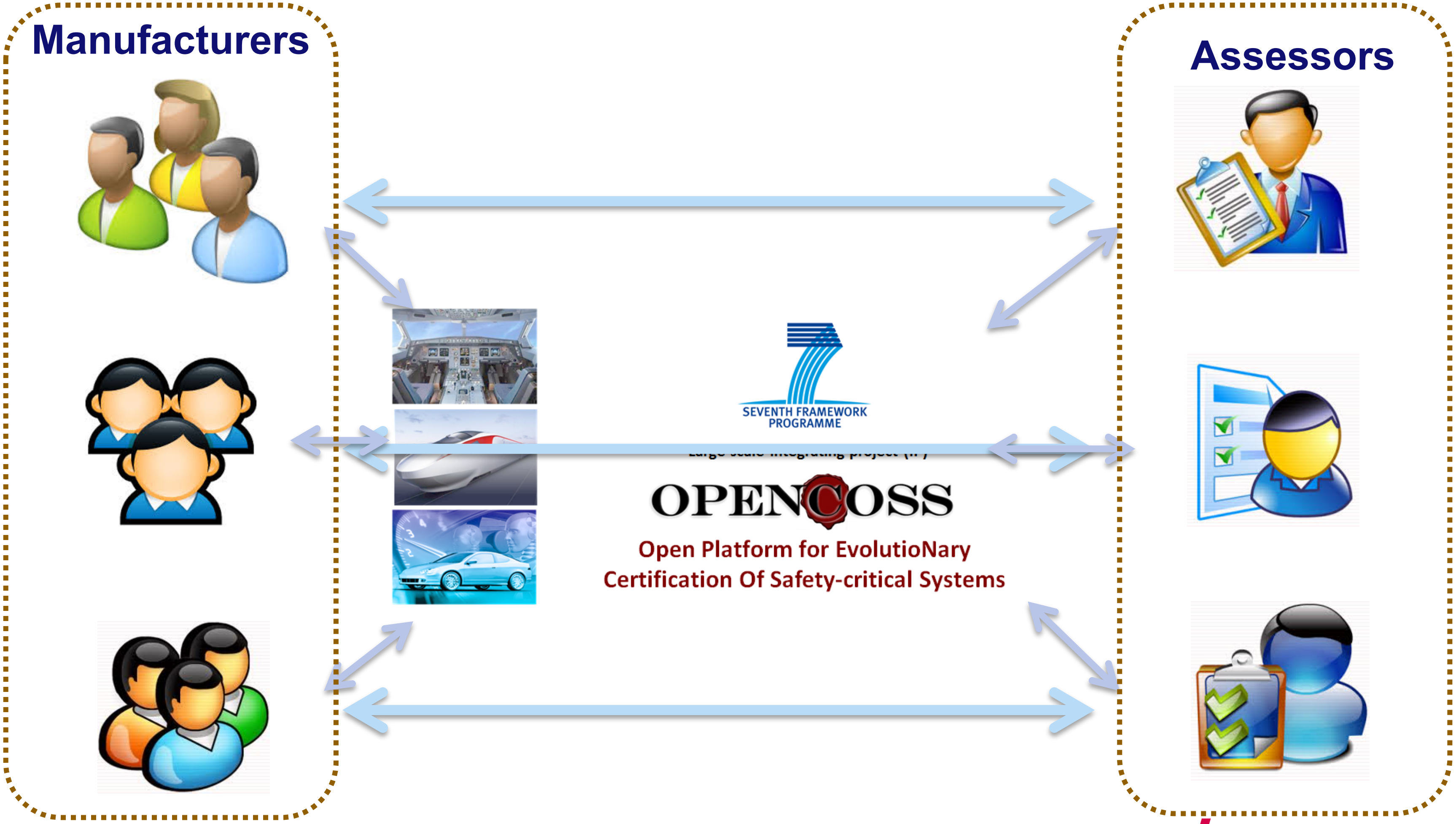
NOTE Table A.1 provides an overview of objectives, prerequisites and work products of the concept phase.

Experts





Background: OpenCOSS



Manufacturers

Assessors

SEVENTH FRAMEWORK PROGRAMME

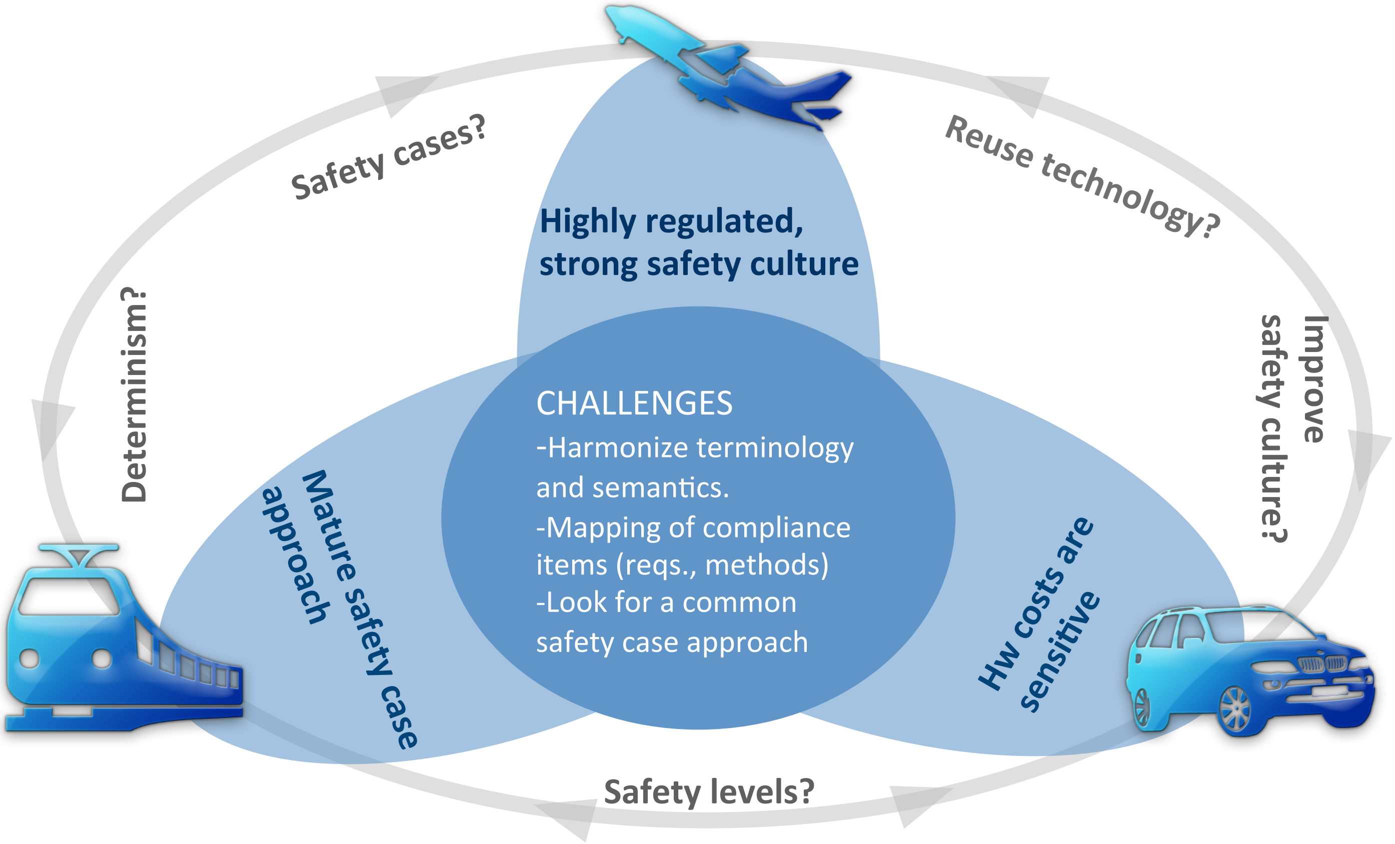
Large-scale integrating project (IP)

OPENCOSS

Open Platform for EvolutioNary Certification Of Safety-critical Systems

TU/e Technische Universiteit Eindhoven University of Technology

Challenge: cross-domain framework



Highly regulated, strong safety culture

Mature safety case approach

Hw costs are sensitive

CHALLENGES

-Harmonize terminology and semantics.

-Mapping of compliance items (reqs., methods)

-Look for a common safety case approach

Safety cases?

Reuse technology?

Determinism?

Improve safety culture?

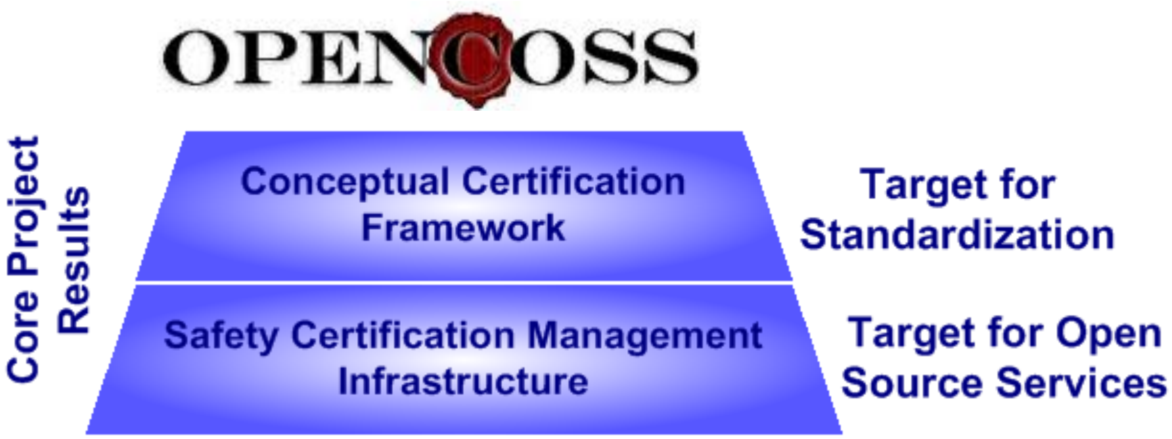
Safety levels?

TU/e Technische Universiteit **Eindhoven** University of Technology

Goals of OpenCOSS

- Support for product development process;
- Common Certification Language is designed for those 3 domains;
- Generic Meta Model (GMM) has been developed.

1


OPENCOSS
Core Project Results
Conceptual Certification Framework
Safety Certification Management Infrastructure
Target for Standardization
Target for Open Source Services

2

- Use safety case to demonstrate safety;
- Common Safety Case Approach to manage certification data and reduce the cost.

Generic vs Specific Meta Model

- GMM ------ for all those three domains, designed for certification data reuse

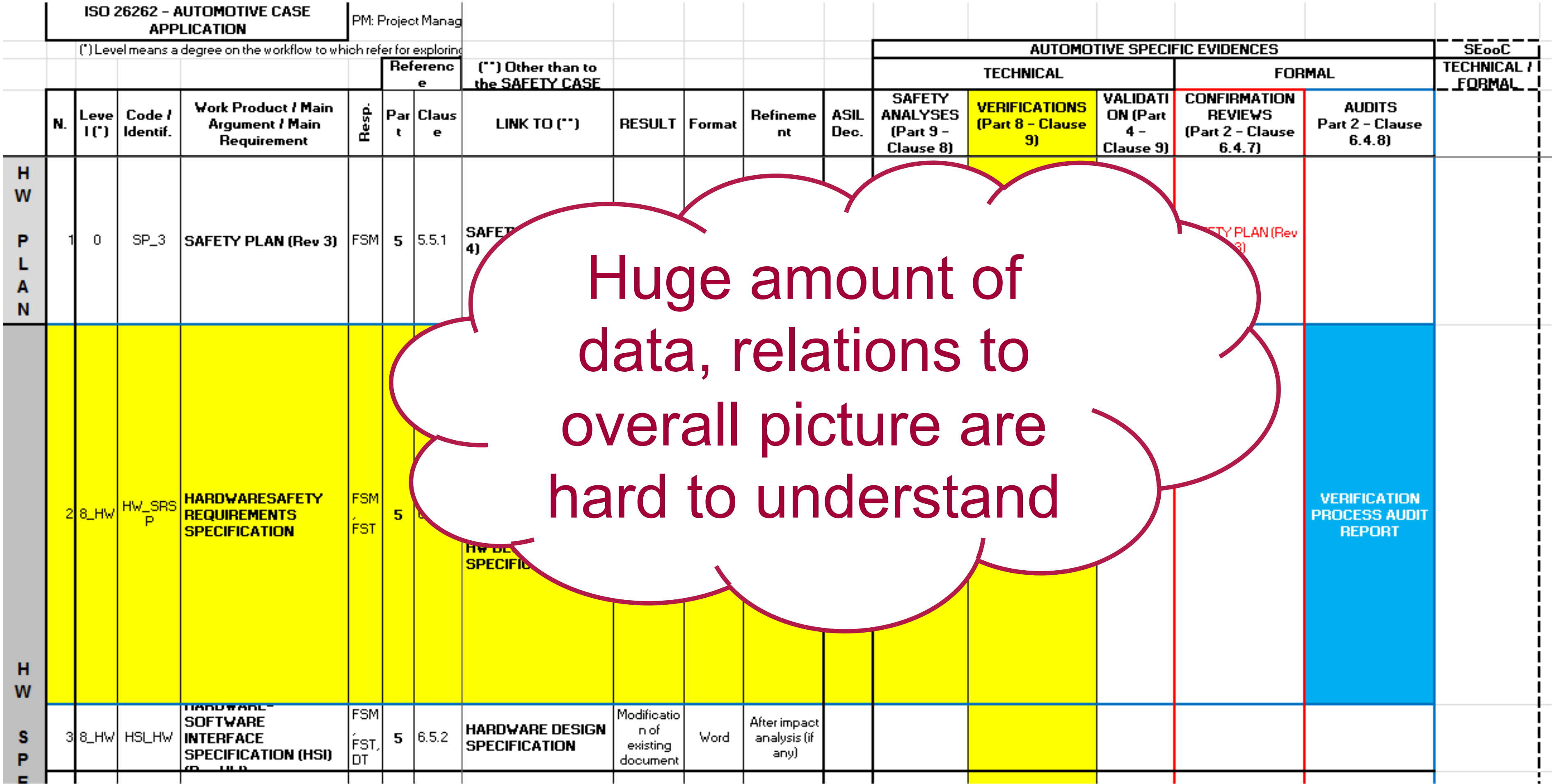
- Why a Specific Meta Model
  - Different ways of addressing safety:
    - per domain
    - per company
    - per project
  - For each domain, user need to change their current way of working to conform to GMM. Although it is good for reuse, but for other part, the costs may increase.

Standards

- **Most important requirement in automotive:**
  - ***A vehicle should not harm its passengers or (people in) its environment***

- **Safety related standards for automotive:**
  - **IEC 61508 (Functional Safety standard)**
  - **ISO 26262 (Functional Safety standard)**

Developing a Safety Case



ISO 26262 – AUTOMOTIVE CASE APPLICATION

PM: Project Manag

(*) Level means a degree on the workflow to which refer for exploring

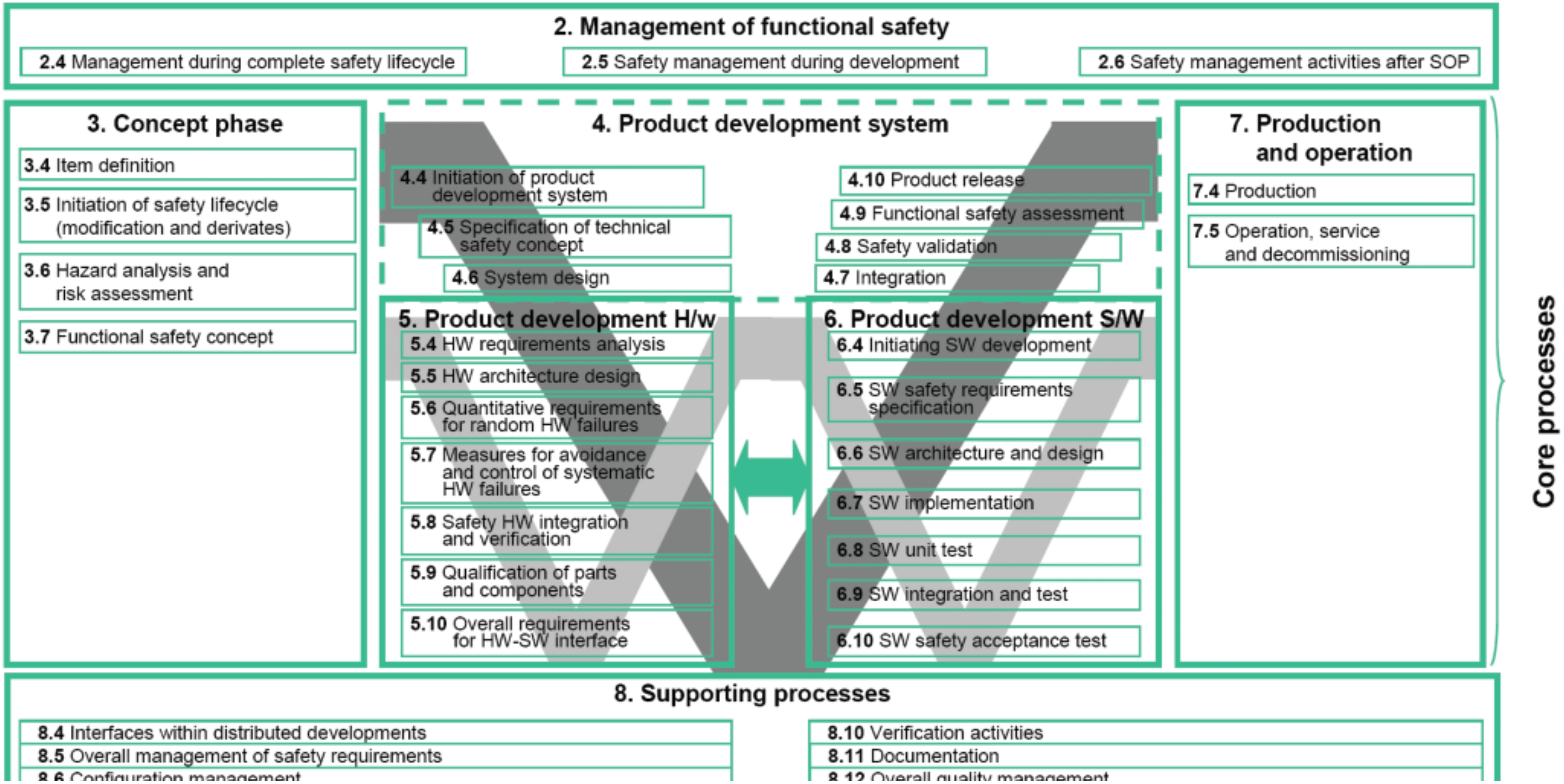
						Reference		(**) Other than to the SAFETY CASE					AUTOMOTIVE SPECIFIC EVIDENCES					SEooC
													TECHNICAL			FORMAL		TECHNICAL / FORMAL
	N.	Level (*)	Code / Identif.	Work Product / Main Argument / Main Requirement	Resp.	Part	Clause	LINK TO (**)	RESULT	Format	Refinement	ASIL Dec.	SAFETY ANALYSES (Part 9 – Clause 8)	VERIFICATIONS (Part 8 – Clause 9)	VALIDATION (Part 4 – Clause 9)	CONFIRMATION REVIEWS (Part 2 – Clause 6.4.7)	AUDITS Part 2 – Clause 6.4.8)	
HW PLAN	1	0	SP_3	SAFETY PLAN (Rev 3)	FSM	5	5.5.1	SAFET 4)								ETY PLAN (Rev 3)		
	2	8_HW	HW_SRSP	HARDWARESAFETY REQUIREMENTS SPECIFICATION	FSM, FST	5		HW DE SPECIFI									VERIFICATION PROCESS AUDIT REPORT	
HW SPE	3	8_HW	HSI_HW	HARDWARE-SOFTWARE INTERFACE SPECIFICATION (HSI)	FSM, FST, DT	5	6.5.2	HARDWARE DESIGN SPECIFICATION	Modification of existing document	Word	After impact analysis (if any)							

Huge amount of data, relations to overall picture are hard to understand

Standards

- ISO 26262 is the adaptation of IEC 61508 to comply with needs specific to the application sector of E/E systems within road vehicles:
  - Provides an automotive safety lifecycle (management, development, production, operation, service, decommissioning) and supports tailoring the necessary activities during these lifecycle phases.
  - Provides an automotive-specific risk-based approach for determining risk classes (Automotive Safety Integrity Levels, ASILs).

Standards



2. Management of functional safety

2.4 Management during complete safety lifecycle

2.5 Safety management during development

2.6 Safety management activities after SOP

3. Concept phase

3.4 Item definition

3.5 Initiation of safety lifecycle (modification and derivates)

3.6 Hazard analysis and risk assessment

3.7 Functional safety concept

4. Product development system

4.4 Initiation of product development system

4.5 Specification of technical safety concept

4.6 System design

4.7 Integration

4.8 Safety validation

4.9 Functional safety assessment

4.10 Product release

5. Product development H/w

5.4 HW requirements analysis

5.5 HW architecture design

5.6 Quantitative requirements for random HW failures

5.7 Measures for avoidance and control of systematic HW failures

5.8 Safety HW integration and verification

5.9 Qualification of parts and components

5.10 Overall requirements for HW-SW interface

6. Product development S/W

6.4 Initiating SW development

6.5 SW safety requirements specification

6.6 SW architecture and design

6.7 SW implementation

6.8 SW unit test

6.9 SW integration and test

6.10 SW safety acceptance test

7. Production and operation

7.4 Production

7.5 Operation, service and decommissioning

Core processes

8. Supporting processes

8.4 Interfaces within distributed developments

8.5 Overall management of safety requirements

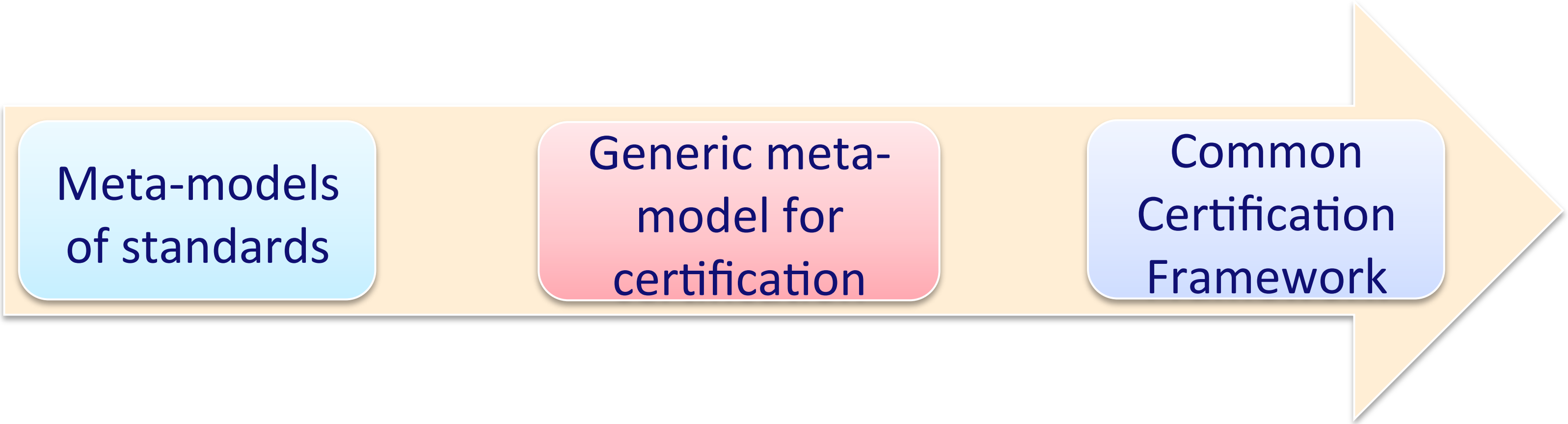
8.6 Configuration management

8.10 Verification activities

8.11 Documentation

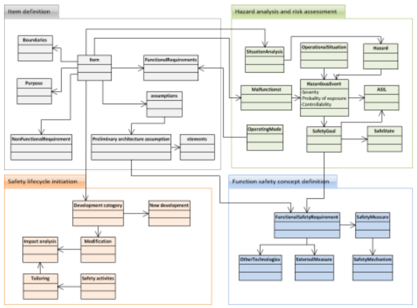
8.12 Overall quality management

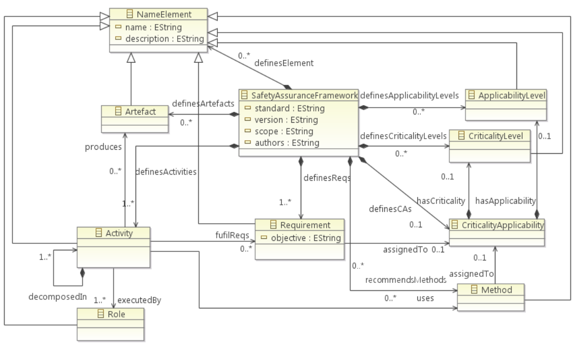
Approach

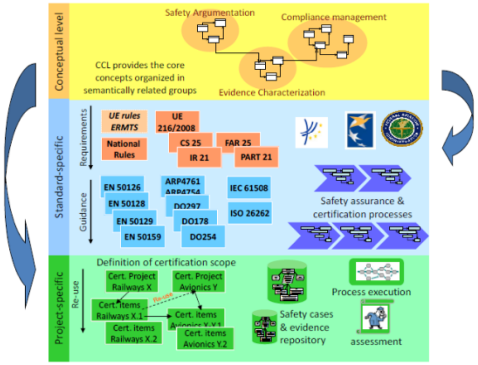

Meta-models of standards

Generic meta-model for certification

Common Certification Framework

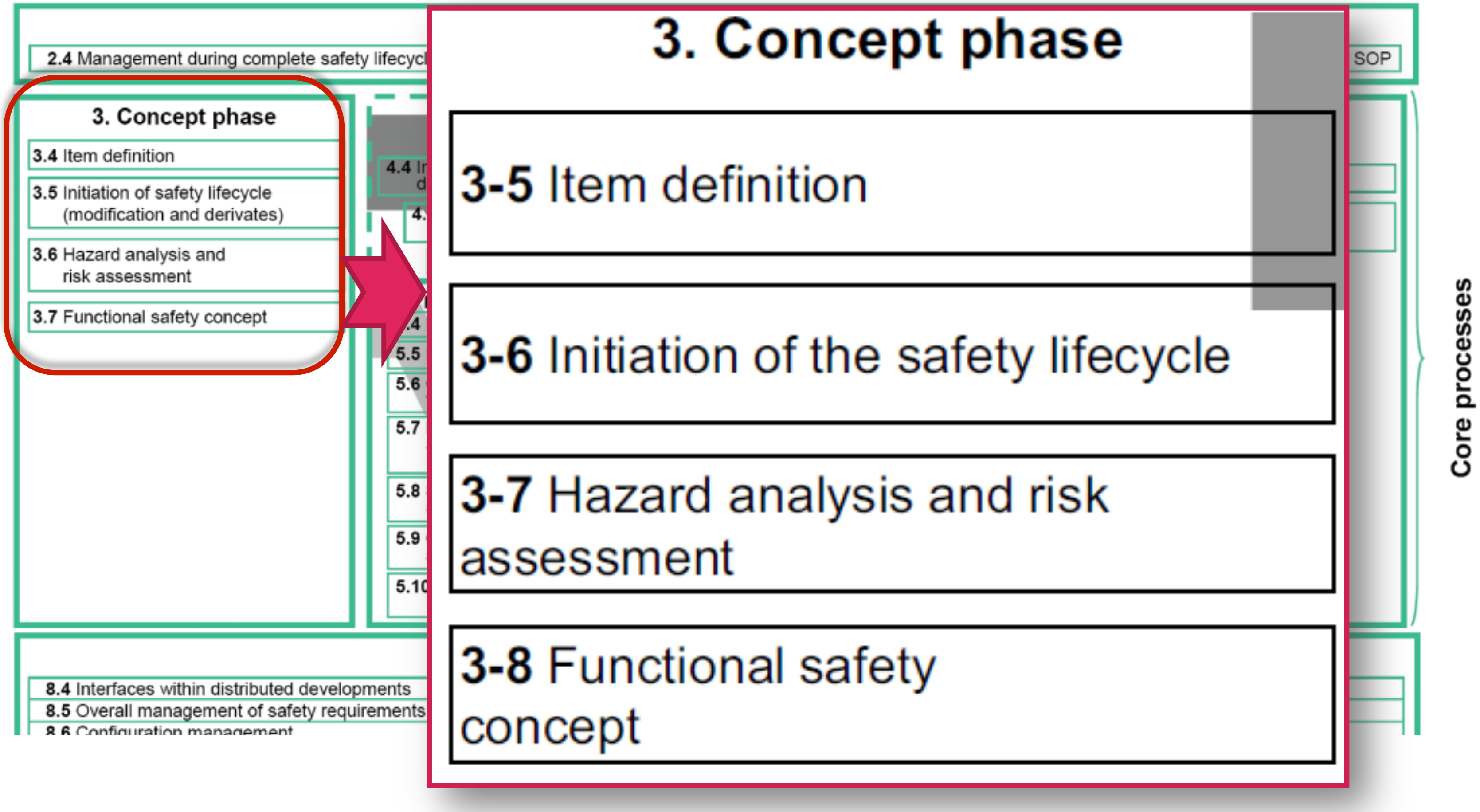

Item definition
Hazard analysis and risk assessment
Safety lifecycle initiation
Function safety concept definition





Technische Universiteit
Eindhoven
University of Technology

Overview of ISO 26262


2.4 Management during complete safety lifecycl
SOP
3. Concept phase
3.4 Item definition
3.5 Initiation of safety lifecycle (modification and derivates)
3.6 Hazard analysis and risk assessment
3.7 Functional safety concept
4.4 In
4.
5.5
5.6
5.7
5.8
5.9
5.10
8.4 Interfaces within distributed developments
8.5 Overall management of safety requirements
8.6 Configuration management
Core processes

3. Concept phase

3-5 Item definition

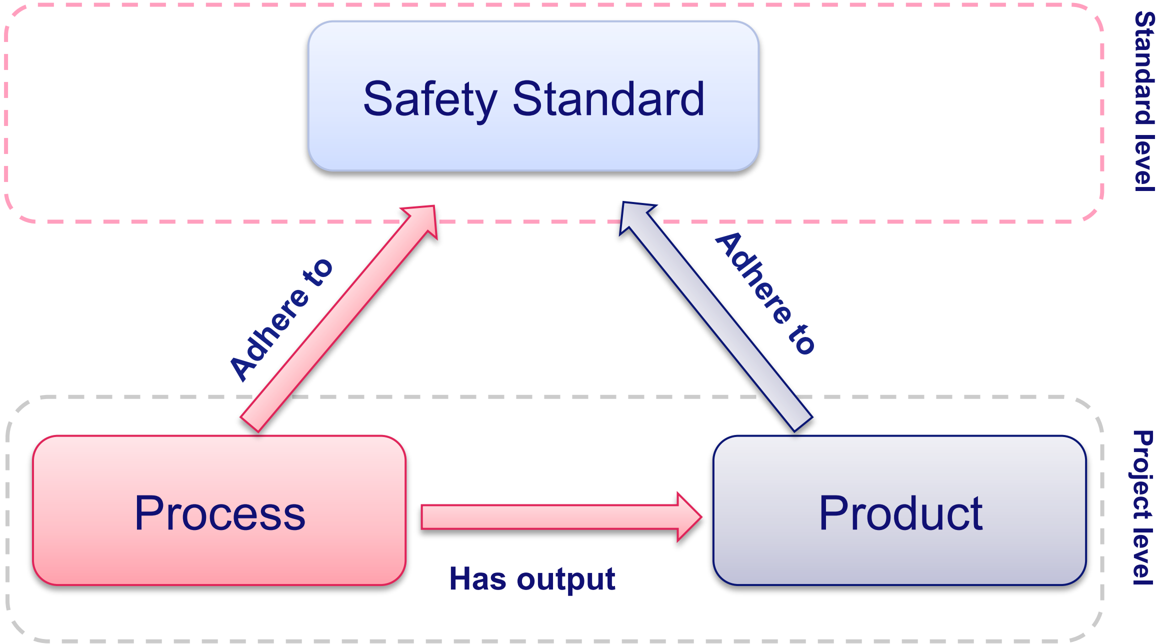
3-6 Initiation of the safety lifecycle

3-7 Hazard analysis and risk assessment

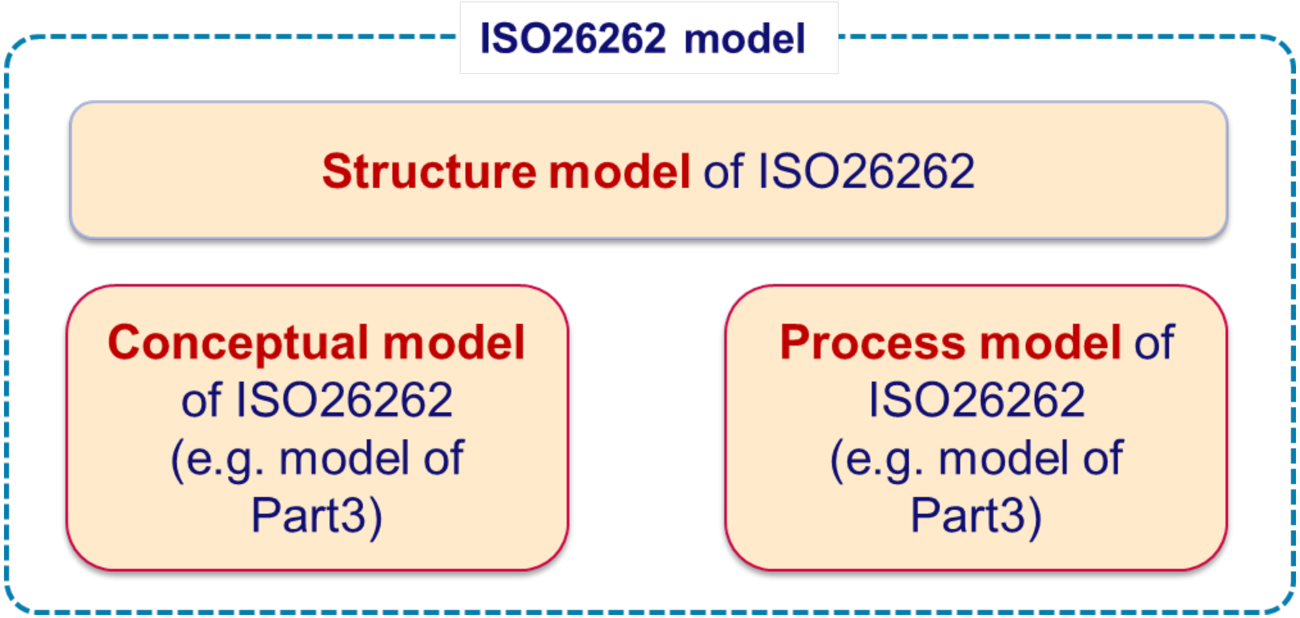
3-8 Functional safety concept

Look from 3 different views

—relationships between standard and project



Modeling for safety reuse



ISO26262 model

Structure model of ISO26262

Conceptual model of ISO26262 (e.g. model of Part3)

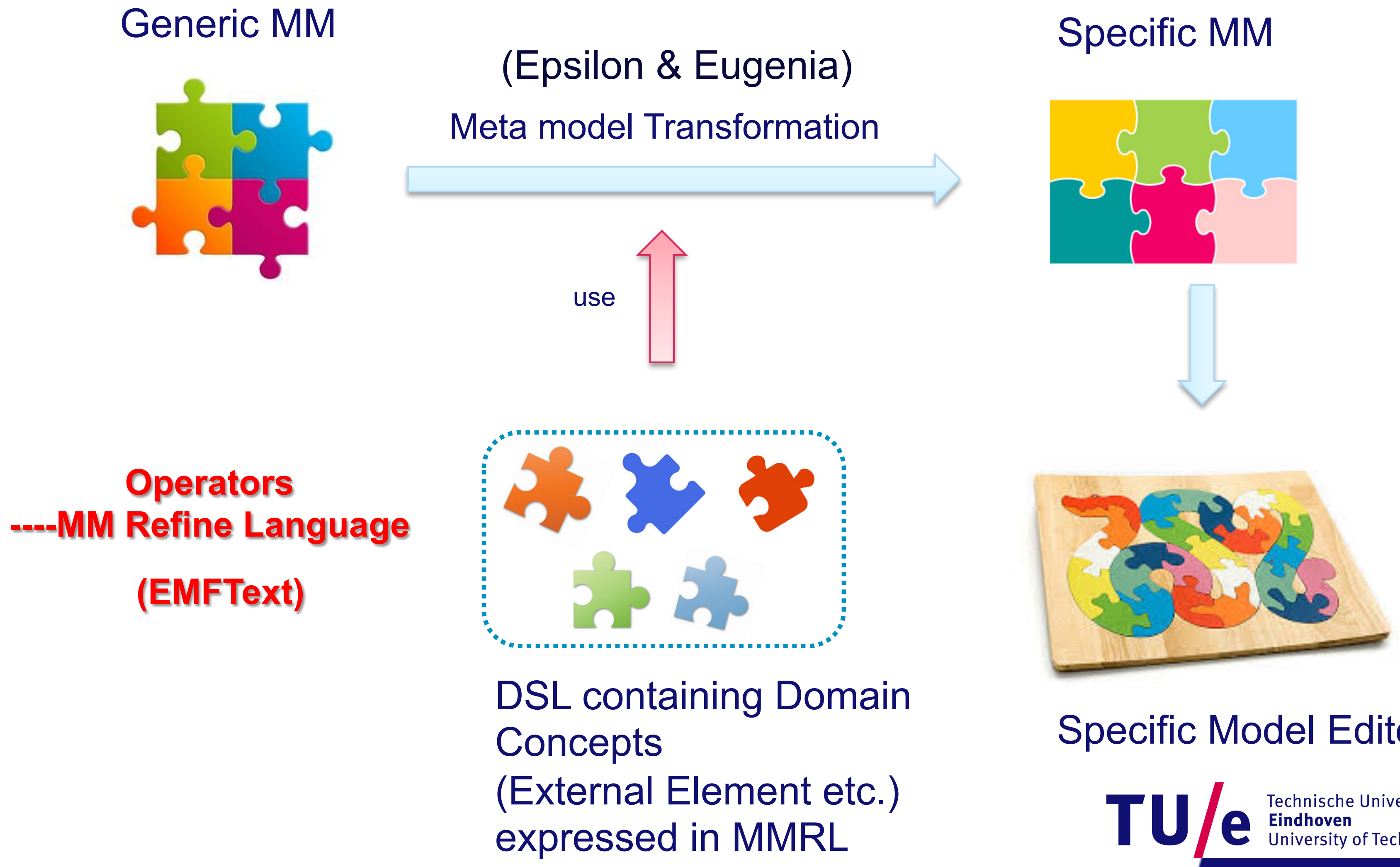
Process model of ISO26262 (e.g. model of Part3)

Model driven approach

- Result is an ad-hoc mapping from Generic Meta Model (GMM) to Specific Meta Model (SMM)
  - Manual work
  - Error prone
  - Hardly any traceability

- Alternative approach based on meta model transformations

Meta model Transformation



Generic MM

(Epsilon & Eugenia)

Meta model Transformation

Specific MM

use

Operators
----MM Refine Language

(EMFText)

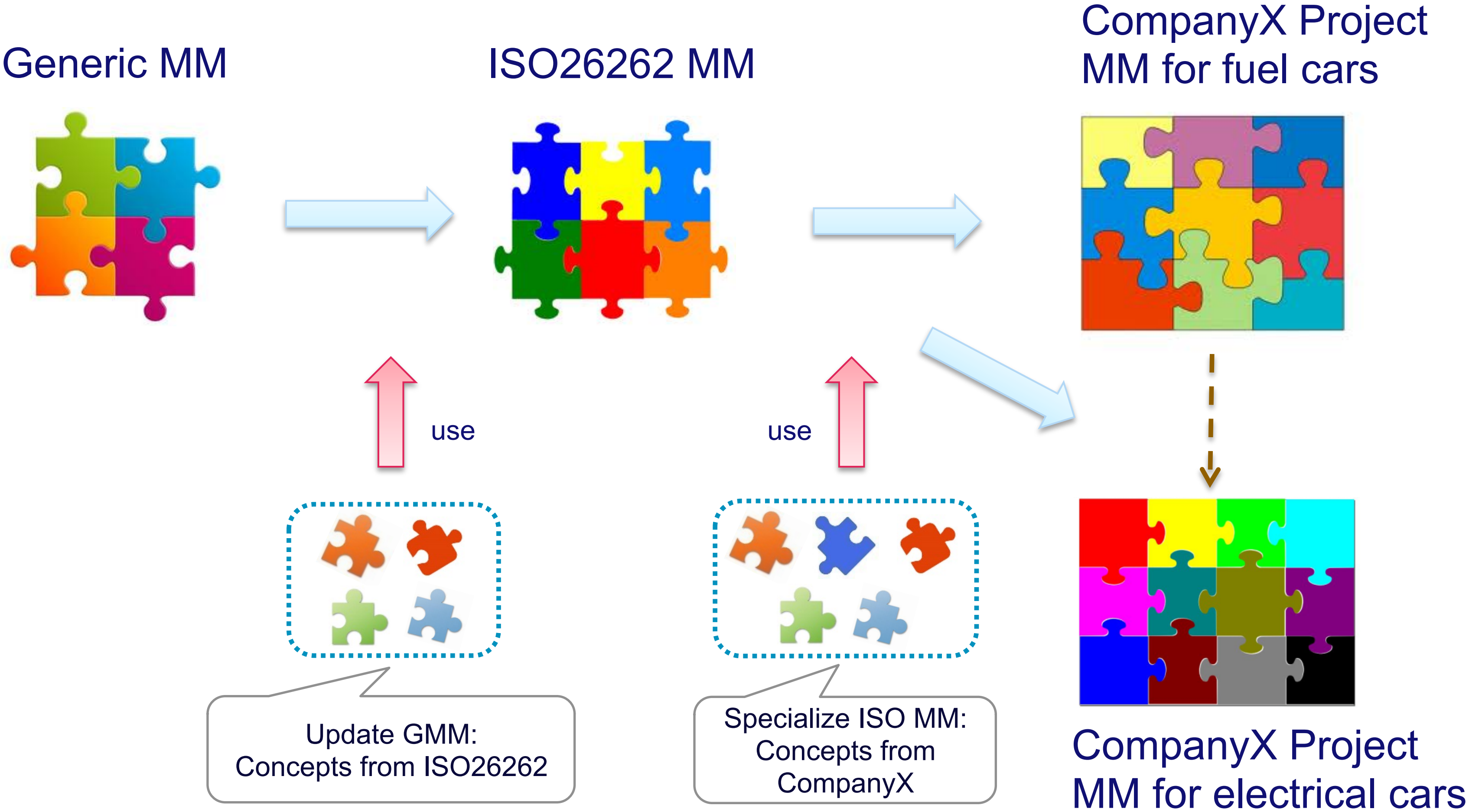
DSL containing Domain Concepts
(External Element etc.)
expressed in MMRL

Specific Model Editor

Model driven approach

- Why MMRL & MMT?
  - Using modeling techniques to reduce those extra cost introduced by GMM.
  - Recorded traceability.
  - Provide a user friendly language.
  - A editor based on SMM could be generated automatically.
    - User can keep their current way of working.

Reuse via Model Transformations



Generic MM

ISO26262 MM

CompanyX Project MM for fuel cars

use

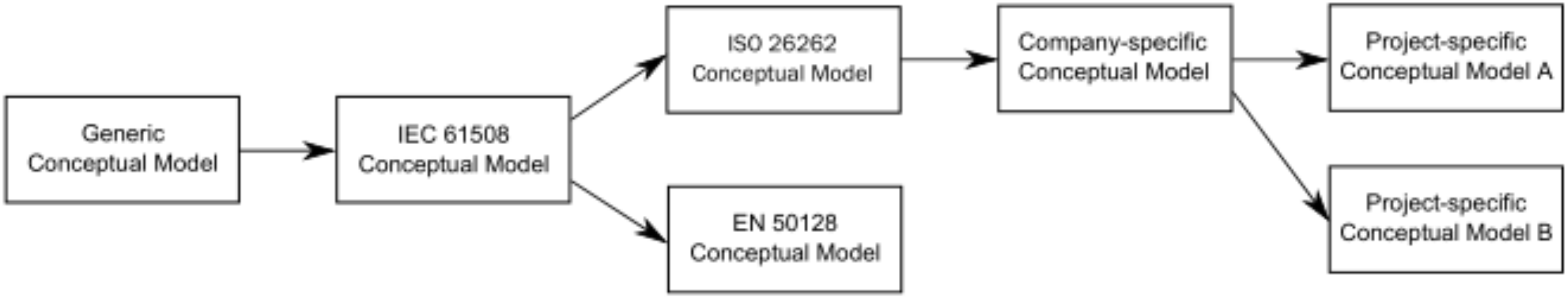
use

Update GMM: Concepts from ISO26262

Specialize ISO MM: Concepts from CompanyX

CompanyX Project MM for electrical cars

Sequences of transformations

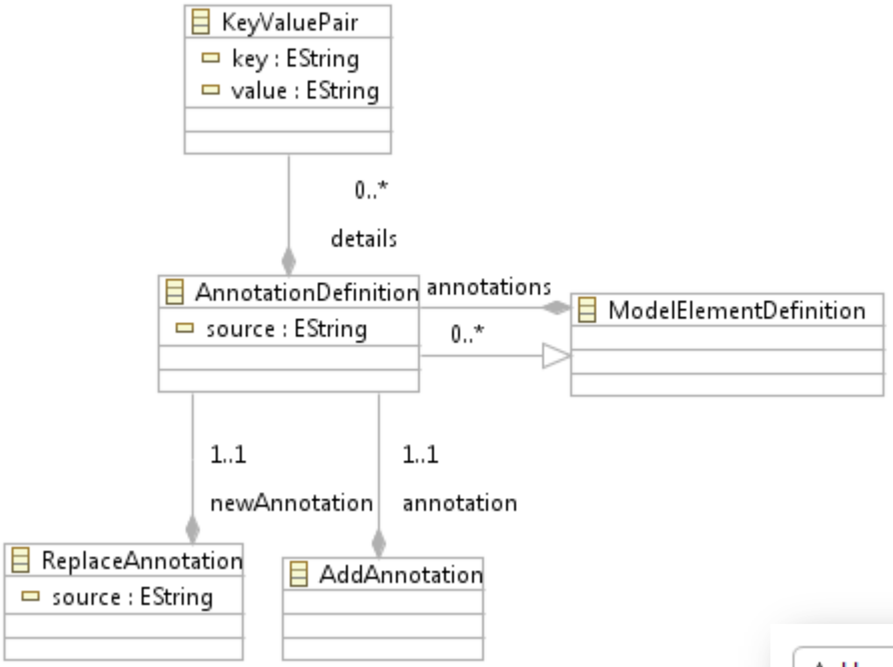

Generic Conceptual Model
IEC 61508 Conceptual Model
ISO 26262 Conceptual Model
EN 50128 Conceptual Model
Company-specific Conceptual Model
Project-specific Conceptual Model A
Project-specific Conceptual Model B

Meta Model Refinement Language

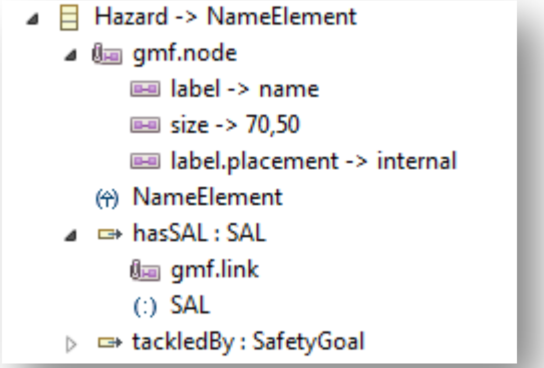
- MMRL operations:
  - Structural
    - AddPackage, AddClass, AddAttribute, AddDataType and AddReference
  - Annotation
    - ReplaceAnnotation and AddAnnotation
  - Enumeration
    - AddEnum and AddEnumLiteral
  - Modification
    - Abstract and RenameElement

MMRL Operations Definition

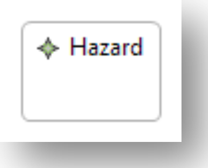
- **Add annotation ------ for editing (Eu**



```
add annotation "gmf.node" {
  "label" = "name",
  "size" = "70,50",
  "label.placement" = "internal"
} to gmm.Hazard
  gmm.HazardEvent
  gmm.SafetyGoal
add annotation "gmf.link" {
} to gmm.Hazard.hasSAL
gmm.HazardEvent.determinedBy
gmm.Hazard.tackledBy
```

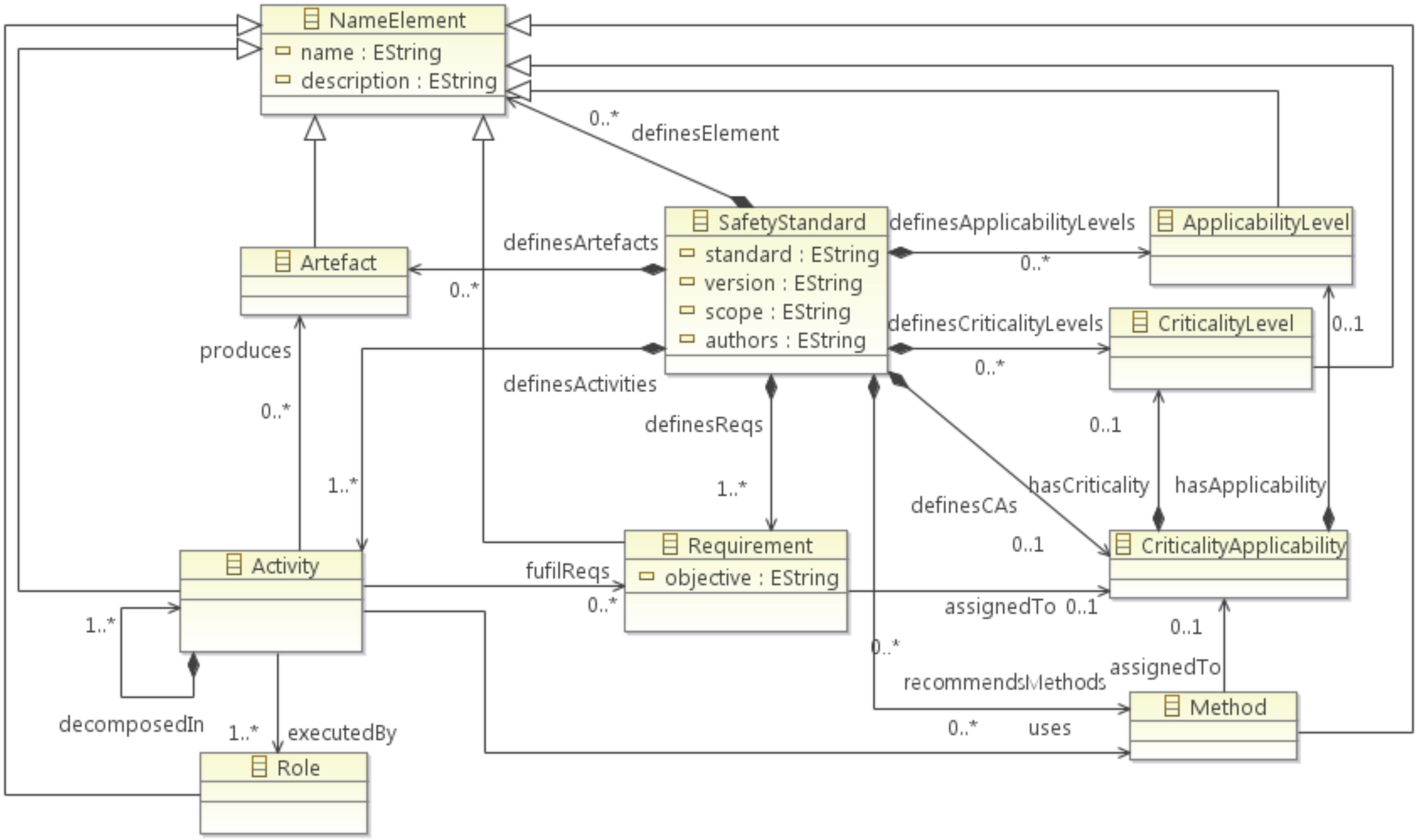


```
Hazard -> NameElement
  gmf.node
    label -> name
    size -> 70,50
    label.placement -> internal
  NameElement
  hasSAL : SAL
    gmf.link
    SAL
  tackledBy : SafetyGoal
```

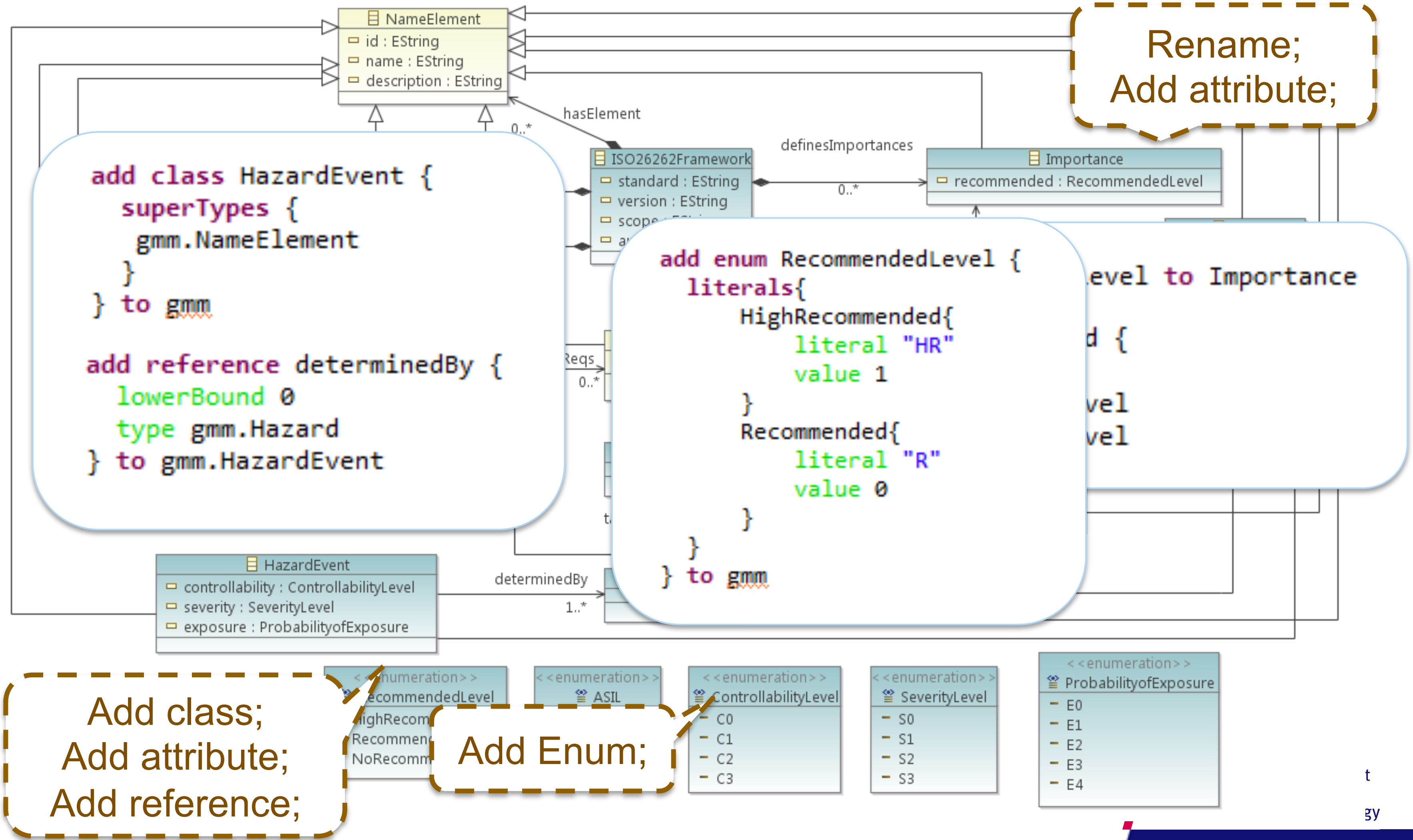


Technische Universiteit **Eindhoven** University of Technology

Case study: Common Certification Language



Case study-MM Refine Language (MMRL)



Rename;
Add attribute;

```
add class HazardEvent {
  superTypes {
   gmm.NameElement
  }
} to gmm

add reference determinedBy {
  lowerBound 0
  type gmm.Hazard
} to gmm.HazardEvent
```

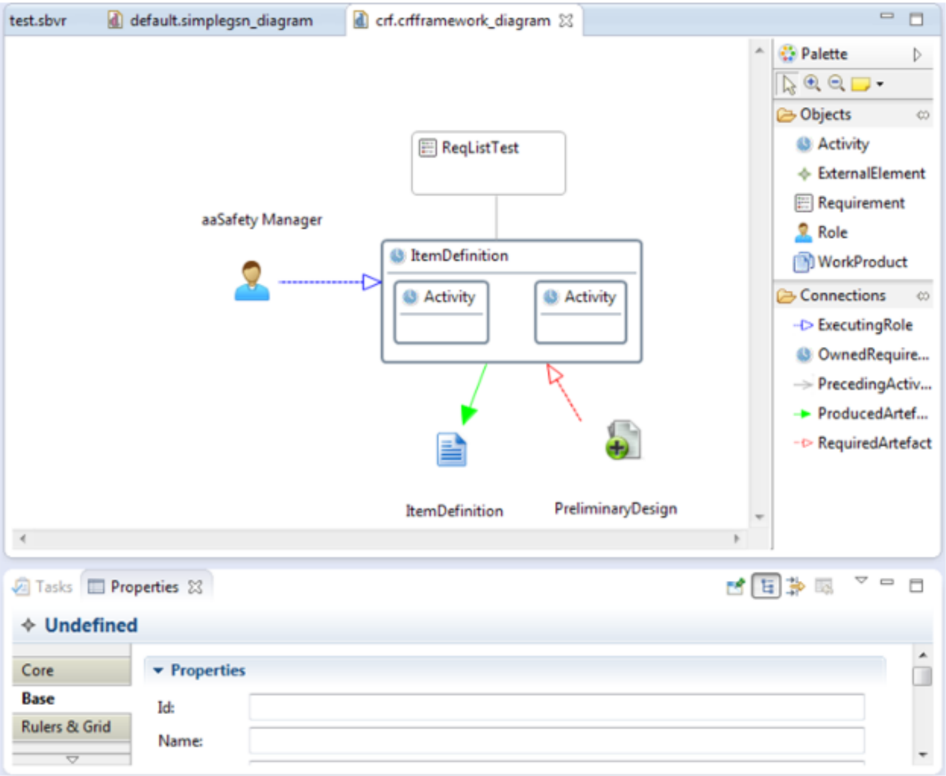
```
add enum RecommendedLevel {
  literals{
      HighRecommended{
          literal "HR"
          value 1
      }
      Recommended{
          literal "R"
          value 0
      }
  }
} to gmm
```

```
evel to Importance

d {

vel
vel
```

Add class;
Add attribute;
Add reference;

Add Enum;

Tool Support

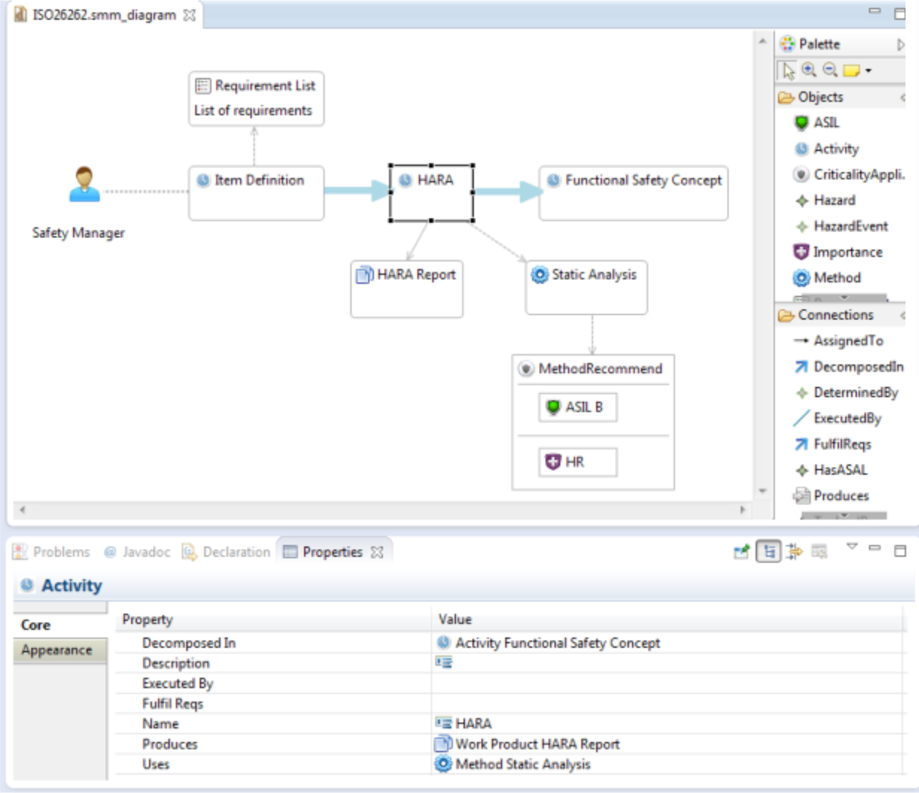


Undefined

Properties

Id:

Name:

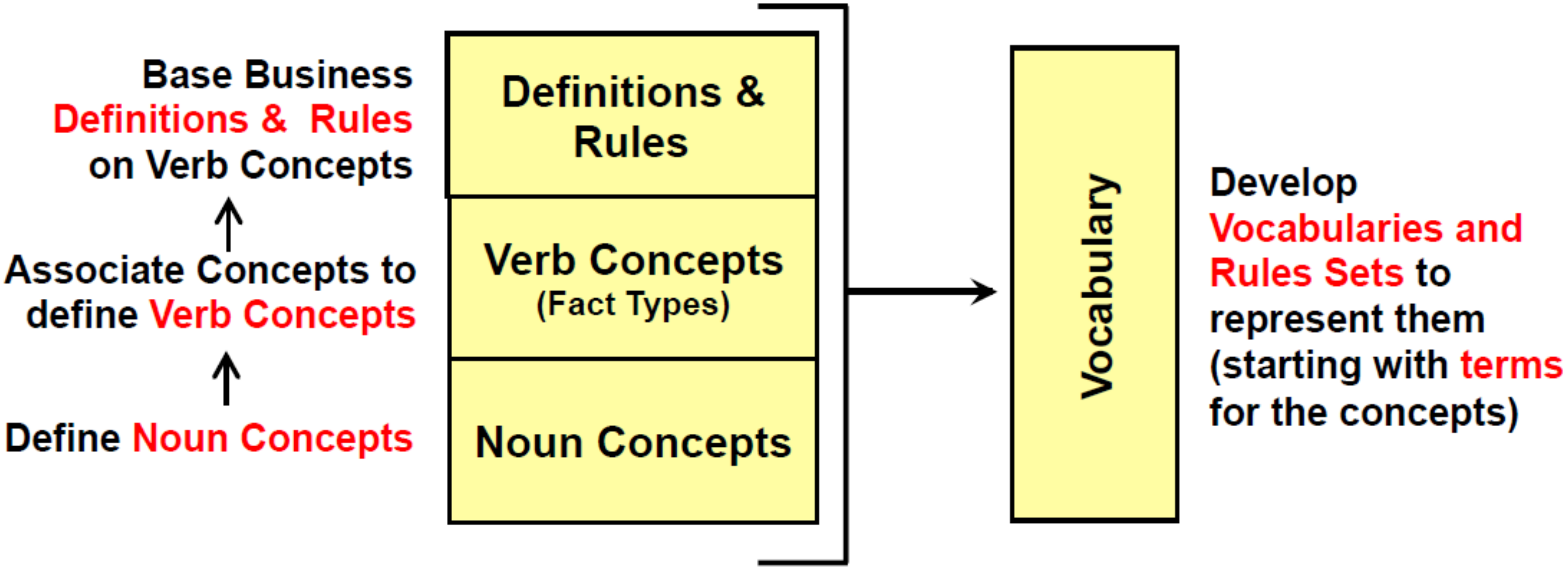


Activity

Property	Value
Decomposed In	Activity Functional Safety Concept
Description	
Executed By	
Fulfil Reqs	
Name	HARA
Produces	Work Product HARA Report
Uses	Method Static Analysis

Future work:

Semantics of Business Vocabulary and Business Rules (SBVR)



Base Business Definitions & Rules on Verb Concepts

↑

Associate Concepts to define Verb Concepts

↑

Define Noun Concepts

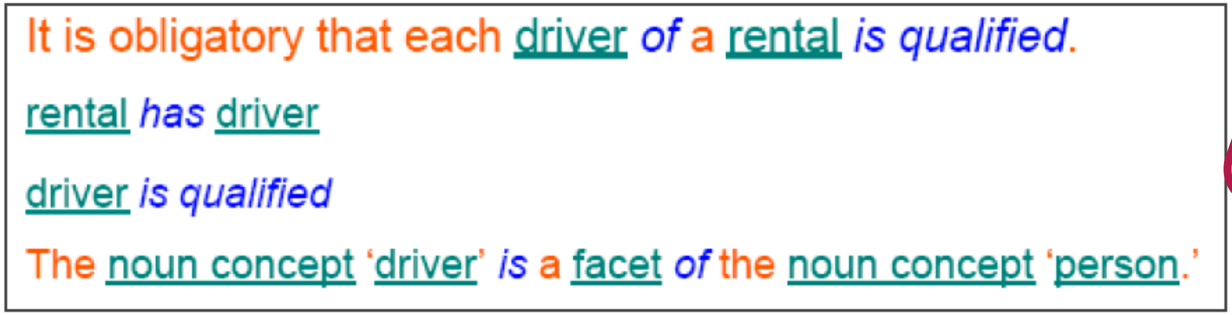
Definitions & Rules

Verb Concepts (Fact Types)

Noun Concepts

→ Vocabulary

Develop Vocabularies and Rules Sets to represent them (starting with terms for the concepts)



It is obligatory that each driver *of* a rental *is qualified*.

rental *has* driver

driver *is qualified*

The noun concept 'driver' *is* a facet *of* the noun concept 'person.'

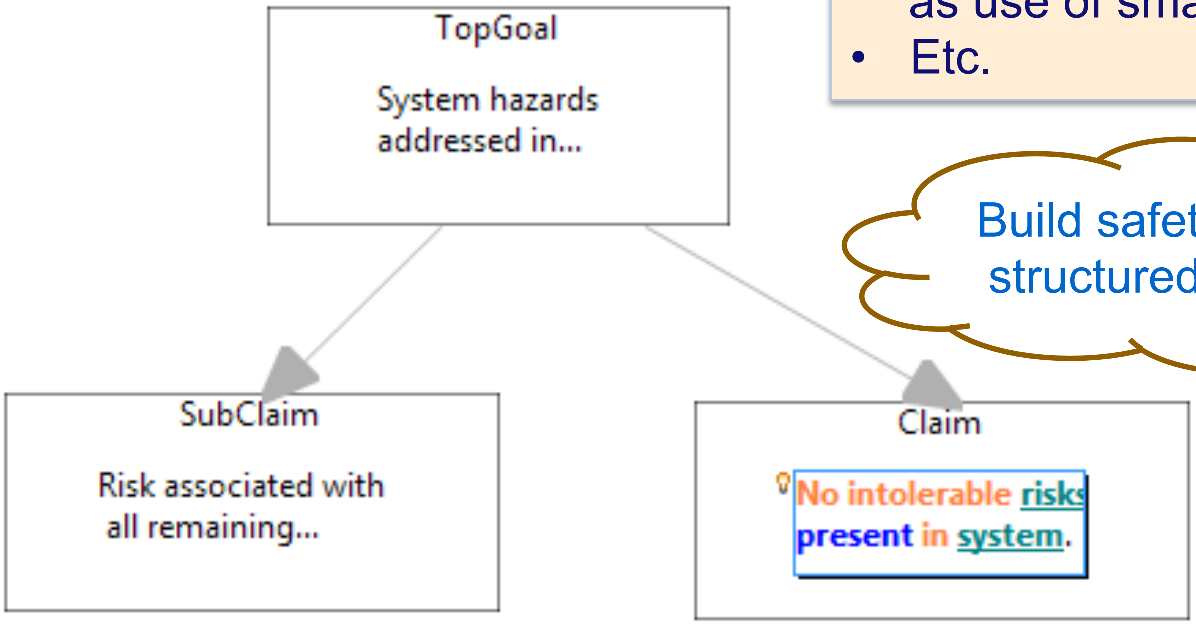
Structured English

Proposed Solution

Language can be controlled:

- Restrict by using a concise vocabulary;
- Limiting the size of sentences;
- Reducing the complexity of sentences;
- Restrict the verbal syntax; such as use of smaller set of tenses;
- Etc.

Build safety case with structured language.



TopGoal

System hazards addressed in...

SubClaim

Risk associated with all remaining...

Claim

No intolerable risks present in system.

Conclusion

- A meta model transformation approach is proposed to facilitate safety assurance
- A meta model refinement language is defined and implemented.
- MMRL can support:
  - comparative mapping between different conceptual models
    - Potential support for safety case reuse
  - Traceability management in the sequence of transformation

Propositions

- Mechanical engineers and electrical engineers are taking over software development
- Software engineers should not become domain experts
- Software engineers should be multi-disciplinary

Thank you !
Questions?