ITEA 2

INFORMATION TECHNOLOGY FOR EUROPEAN ADVANCEMENT

SAFE

Safe Automotive soFtware architEcture

(SAFE)

Project Presentation

SAFE project partners

SPONSORED BY THE

Federal Ministry of Education and Research

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

dgcis

EUREKA

Content

- **Motivation**
- Concept Level
- Implementation Level
- Organization

SAFE – Motivation
Issues in Safety Analysis*)

SAFE

The coherency issue

- How do safety analysis results relate to the actual design?
- How can safety engineers keep track with ongoing evolvements and changes in design models?

The plausibility issue

- How can a system designer relate a cut set to „his“ model?
- How can he understand, how the cut-set can arise?
- How can the propagation of a failure be traced in the system?

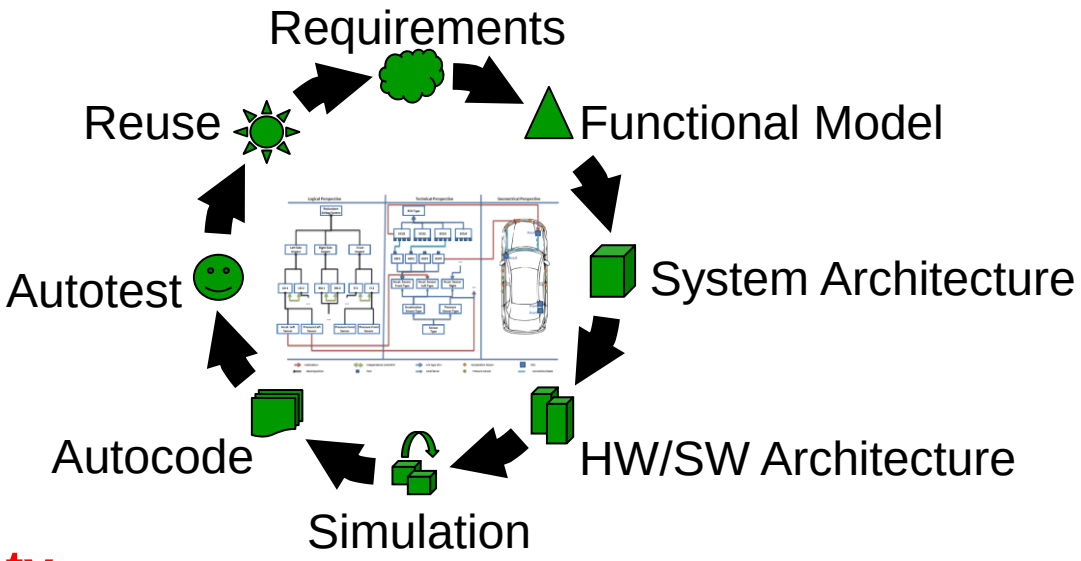
The accuracy issue

- How can mission phases be assessed without over-engineering?
- How can numerical thresholds be assessed?

The completeness issue

- How can a safety designer assert, that all minimal cut sets have been identified?
- How can it be assessed that all relevant effects have been considered?

PART 1 – The Project
Challenges

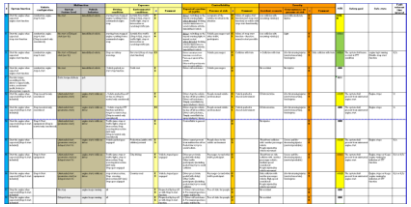


How to keep safety related aspects consistent?

We base the entire development cycle around the model!

Why not the safety analysis?

- Safety Goals modelling
- Requirements Traceability
- Safety Case
- Variant Management
- Assessment methodology
- …



Source: Model-Based Safety Analysis – University of Minnesota

SAFE – Motivation

Model Based Development Safety Analysis

Common Model for Development and Safety Analysis

- To represent safety properties and requirements in the same notation of the development models
- To perform safety analysis having the possibility to trace back through the results in the system model in order to understand expected behavior

Safety analysis based on formal models

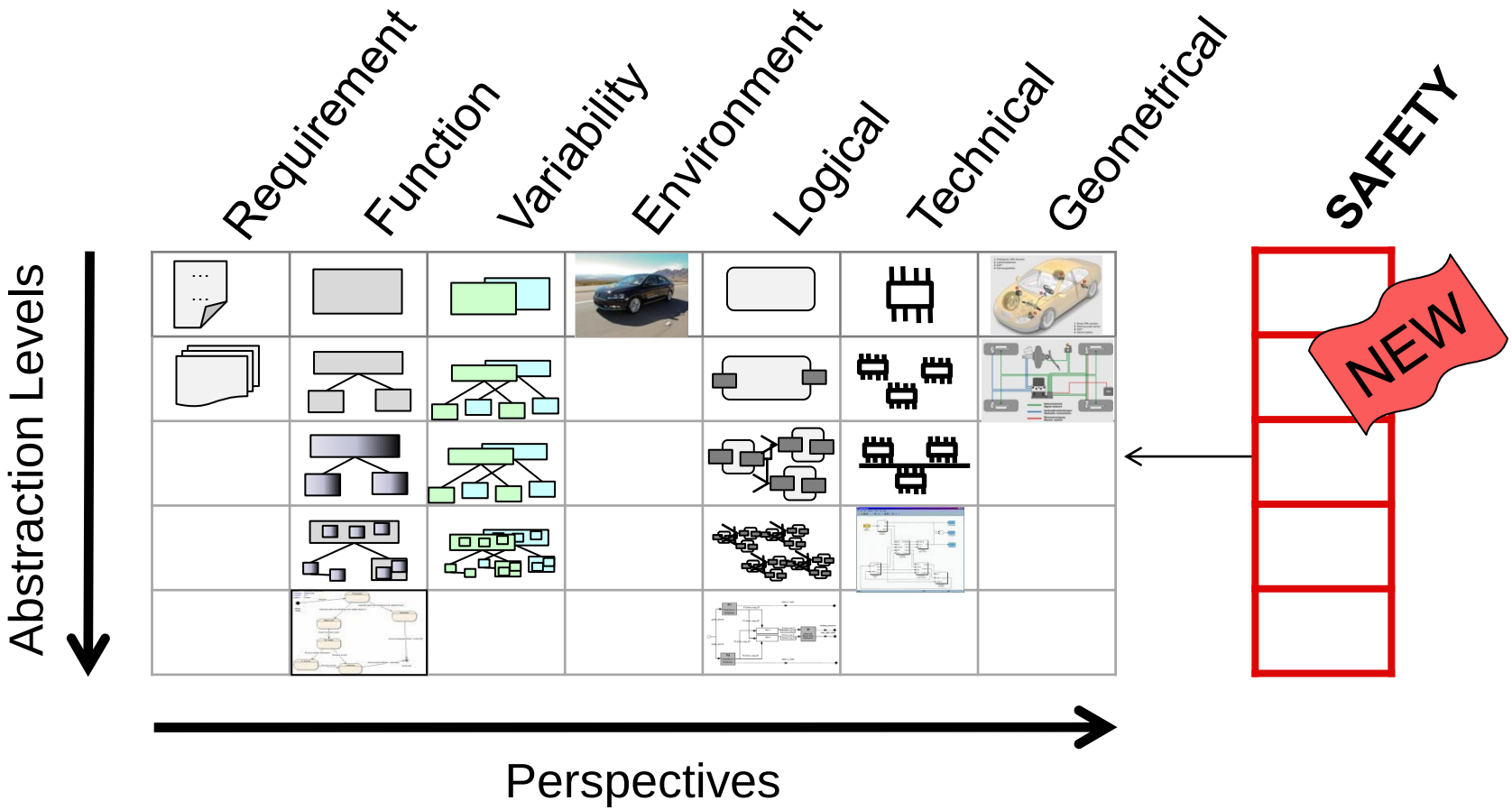
- Facilitates consistency in safety analysis
- Facilitates completeness of safety analysis
- Makes safety analysis more systematic and repeatable

Reduced manual effort in error-prone areas

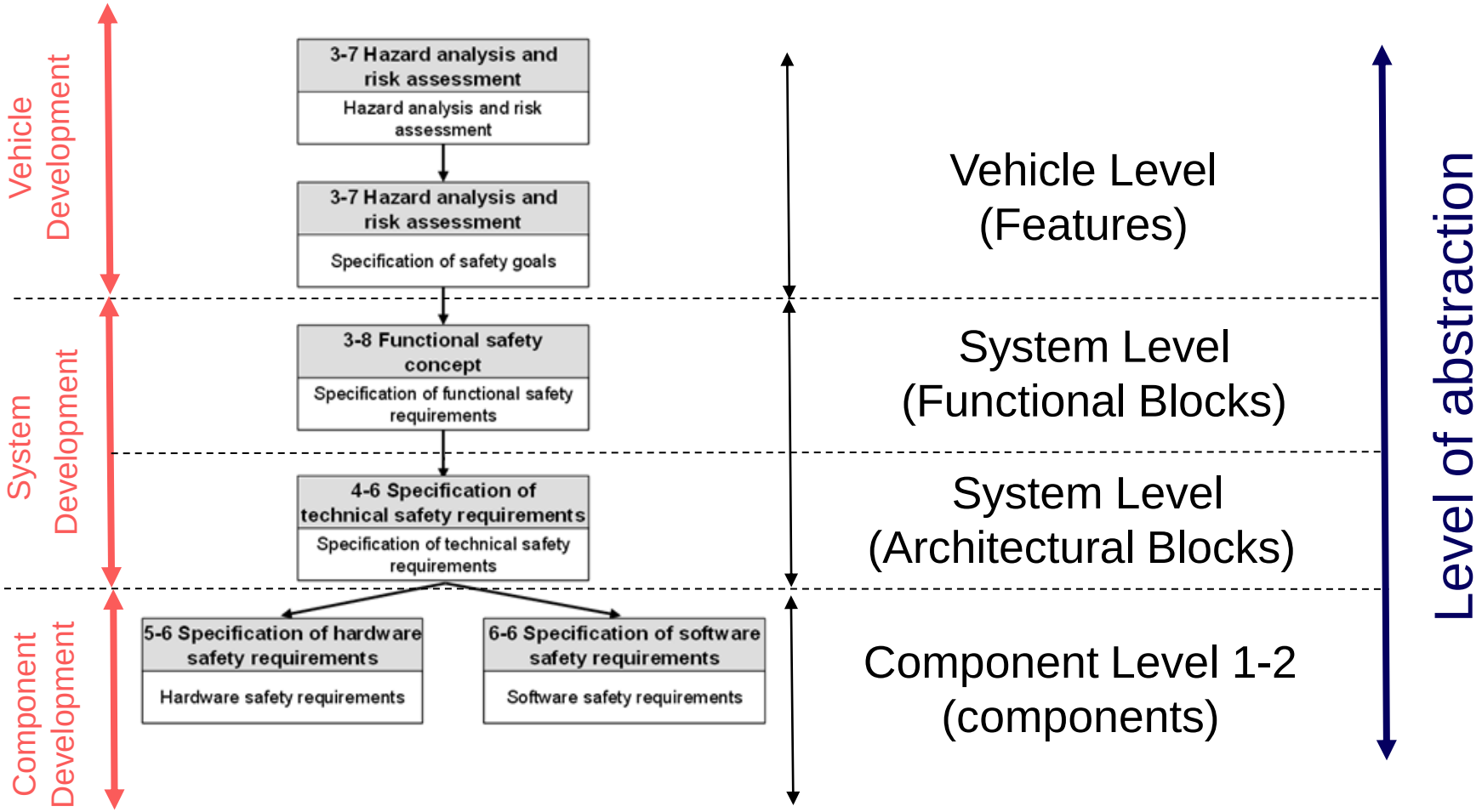
- Automated support for safety analysis
- Explore various failure scenarios

SAFE – Motivation

Model Based Development Safety Analysis



SAFE – Motivation
Additional perspective - ISO26262



SAFE – Motivation
Scope and Goals

Scope

- Automotive electronics architecture

  (system + software + electronic hardware including electrical distribution system)

Goals

- Improve dependability from vehicle to component
- Ensure process compliance to ISO26262
  - at the best cost (automation required, and no over design)
  - matching AUTOSAR requirements
  - methods
    - to reference supplier chain job split, liability and
    - to respect intellectual property rights
- Early evaluation of safety architecture and reuse (quality and cost driven)
- Demonstrate preservation of functional design choice (safety oriented) on component architecture

SAFE – Motivation
Scope with respect to ISO26262

1. Vocabulary

2. Management of functional safety

- **2-5** Overall safety management
- **2-6** Safety management during item development
- **2-7** Safety management after release for production

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

4. Product development: system level

- **4-5** Initiation of product development at the system level
- **4-6** Specification of the technical safety requirements
- **4-7** System design
- **4-8** Item integration and testing
- **4-9** Safety validation
- **4-10** Functional safety assessment
- **4-11** Release for production

5. Product development: hardware level

- **5-5** Initiation of product development at the hardware level
- **5-6** Specification of hardware safety requirements
- **5-7** Hardware design
- **5-8** Hardware architectural metrics
- **5-9** Evaluation of violation of the safety goal due to random HW failures
- **5-10** Hardware integration and testing

6. Product development: software level

- **6-5** Initiation of product development at the software level
- **6-6** Specification of software safety requirements
- **6-7** Software architectural design
- **6-8** Software unit design and implementation
- **6-9** Software unit testing
- **6-10** Software integration and testing
- **6-11** Software verification

7. Production and operation

- **7-5** Production
- **7-6** Operation, service and decommissioning

Core processes

8. Supporting processes

- **8-5** Interfaces within distributed developments
- **8-6** Overall management of safety requirements
- **8-7** Configuration management
- **8-8** Change management
- **8-9** Verification
- **8-10** Documentation
- **8-11** Qualification of software tools
- **8-12** Qualification of software components
- **8-13** Qualification of hardware components
- **8-14** Proven in use argument

9. ASIL-oriented and safety-oriented analyses

- **9-5** Requirements decomposition with respect to ASIL tailoring
- **9-6** Criteria for coexistence of
- **9-7** Analysis of dependent failures
- **9-8** Safety analyses

10. (Informative) Guidelines on ISO 26262

SAFE – Motivation
Approach

ISO26262

3-7 Hazard analysis and risk assessment

3-8 Functional safety concept

4-6 Specification of technical safety requirements

5-6 Specification of hardware safety requirements

6-6 Specification of software safety requirements

SAFE

Modeling Language

Interoperable Toolset

Guidelines, Application Rules

Developer

Requirements

Seamless tool-supported development

HW-SW Component Models

SAFE – Motivation
Results

Concept Level

- **Open meta-model** for description of system, software, hardware
- **Assessment process** to demonstrate compliance to ISO26262

Implementation Level

- **Technology Platform**, i.e. set of interfaces, plug-ins and tools to realize open meta-model
- **Industrial use cases** demonstrating methods and tools

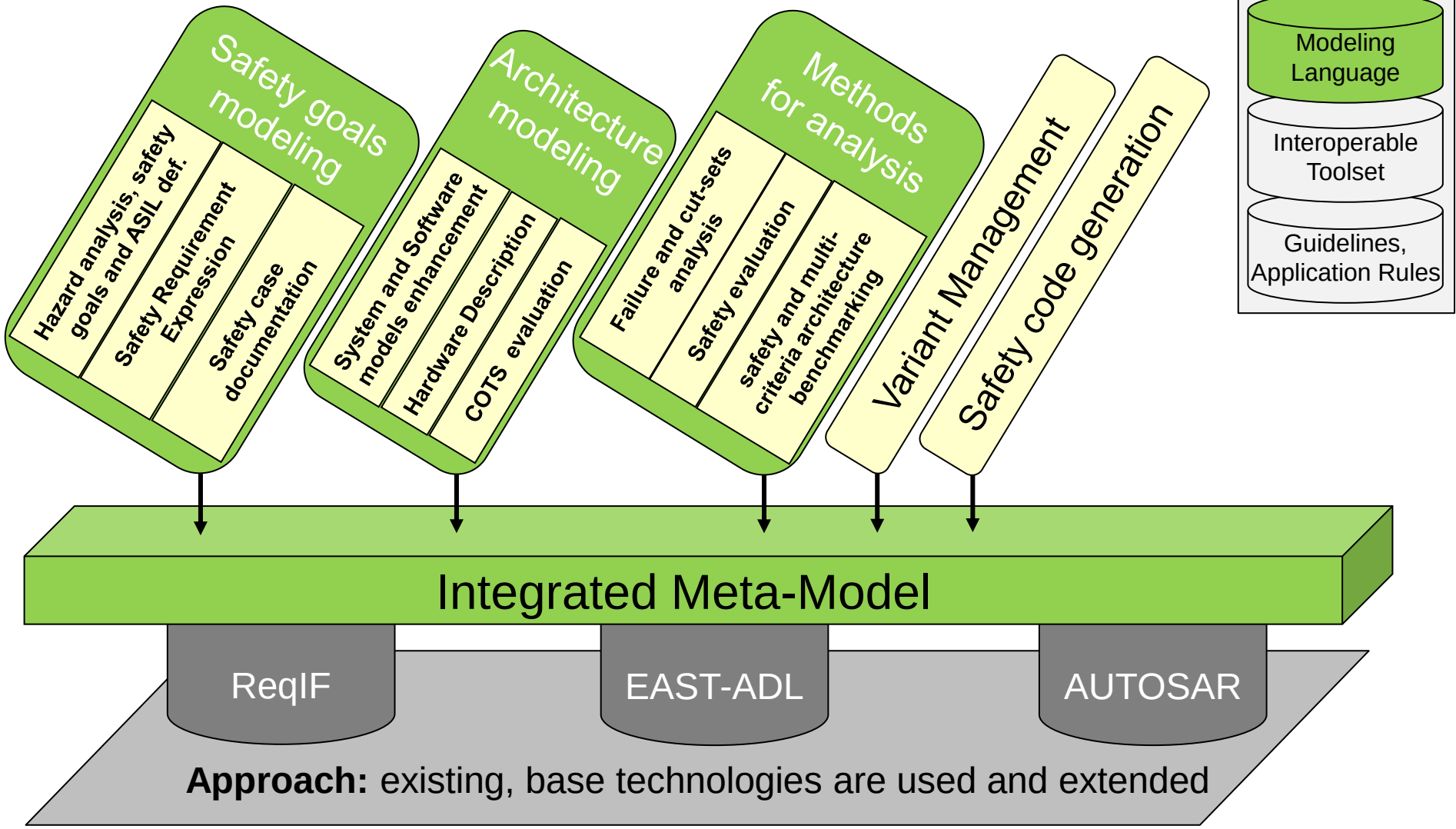
Completive Material

- Training Material
- Recommendation and Guidelines

Content

- Motivation
- **Concept Level**
  - **Open Meta-model**
  - Assessment Methodology
- Implementation Level
- Organization

SAFE – Concept Level
Meta-model for Model based Safety Analysis



SAFE – Concept Level
Hazard analysis and risk assessment

ISO26262

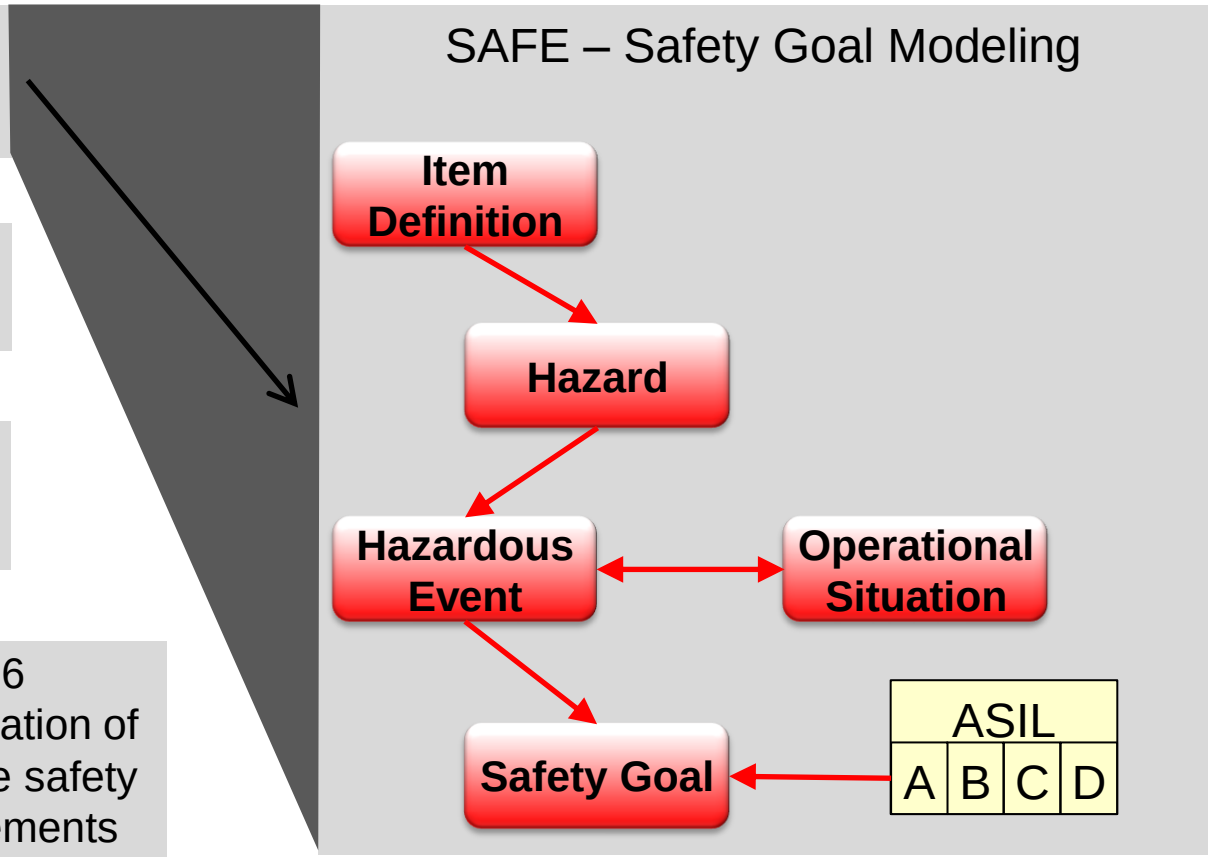
3-7 Hazard analysis and risk assessment

3-8 Functional safety concept

4-6 Specification of technical safety requirements

5-6 Specification of hardware safety requirements

6-6 Specification of software safety requirements



SAFE – Concept Level
Functional safety concept

ISO26262

3-7 Hazard analysis and risk assessment

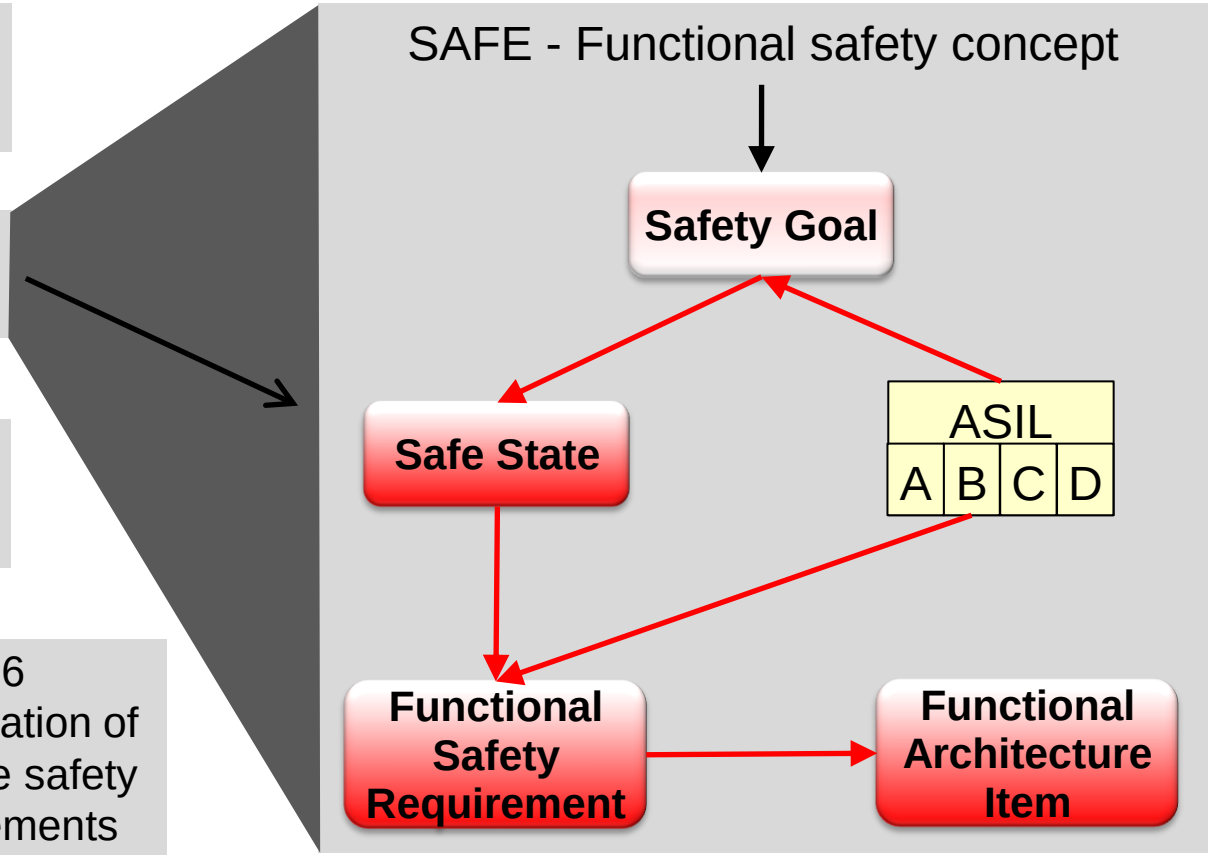
3-8 Functional safety concept

4-6 Specification of technical safety requirements

5-6 Specification of hardware safety requirements

6-6 Specification of software safety requirements

Specification of the functional safety requirements … and their interaction necessary to achieve the safety goals.



SAFE – Concept Level
Technical safety concept

ISO26262

Specification of the technical safety requirements and their allocation to system elements for implementation by the system design.

3-7 Hazard analysis and risk assessment

↓

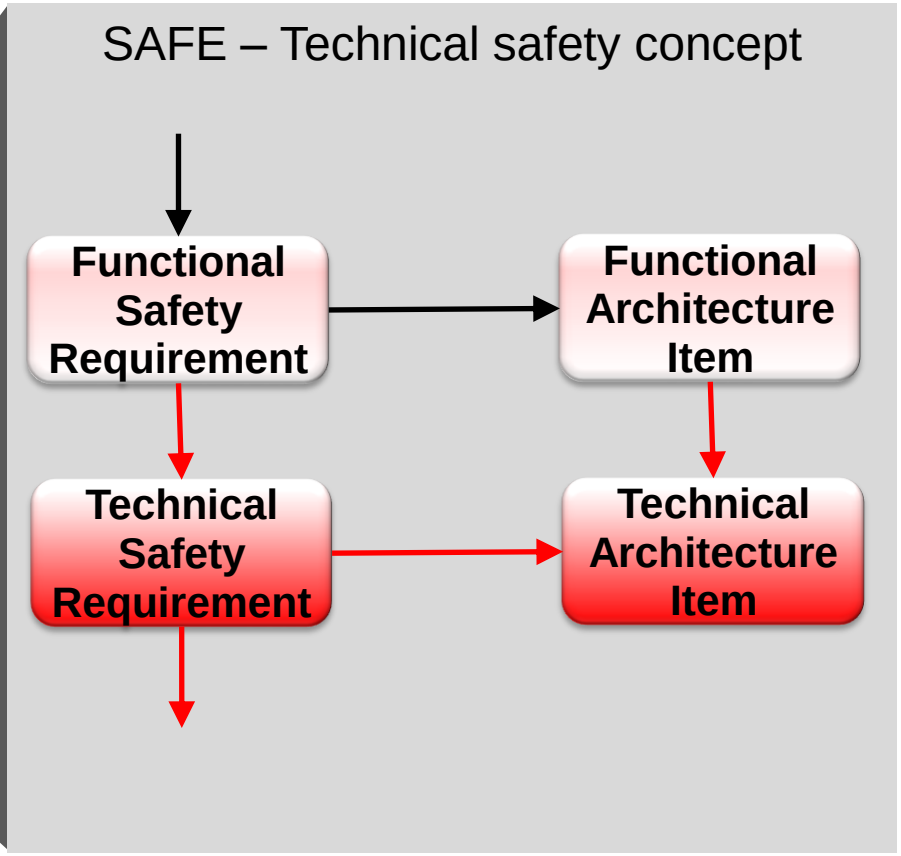
3-8 Functional safety concept

↓

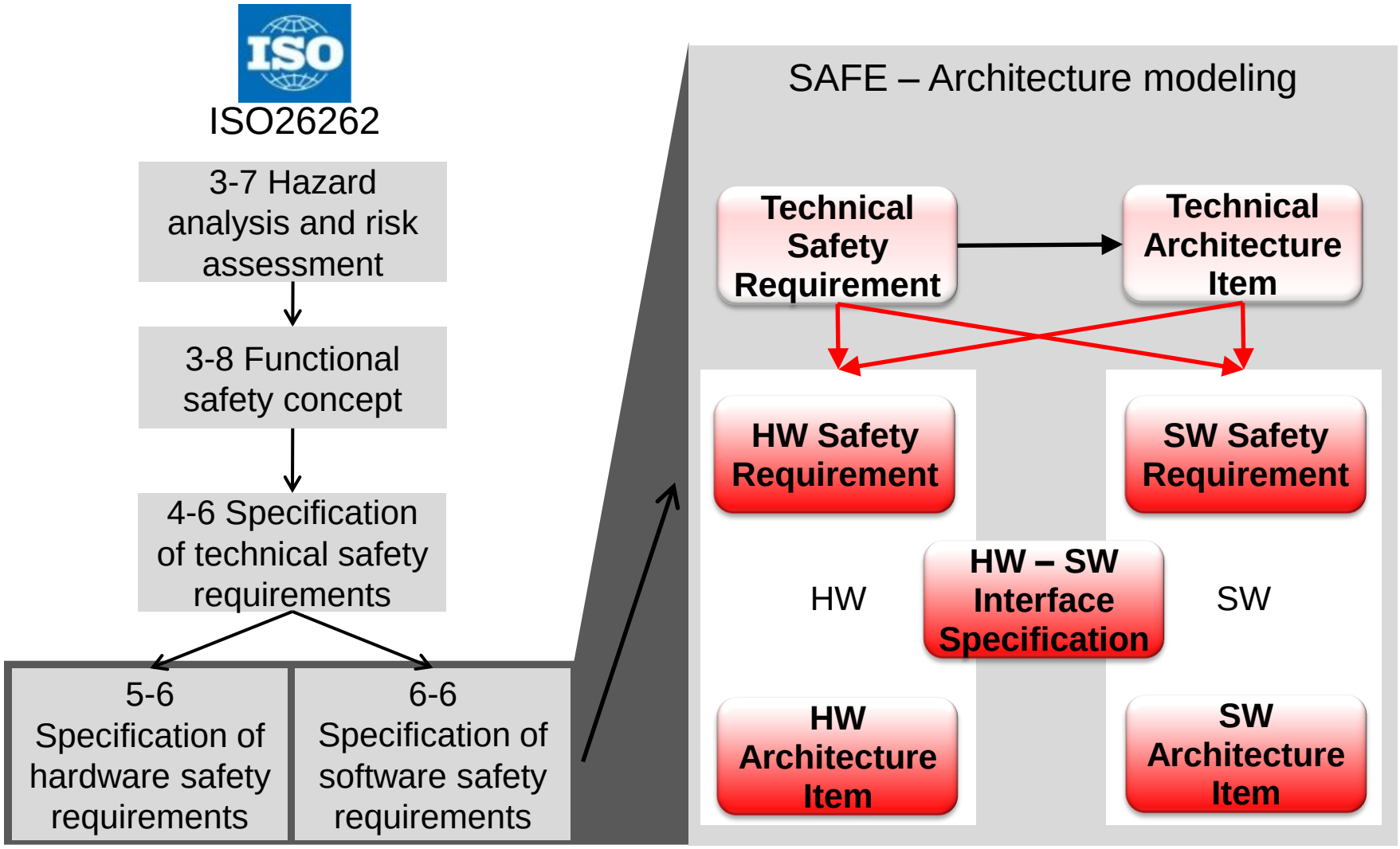
4-6 Specification of technical safety requirements

5-6 Specification of hardware safety requirements

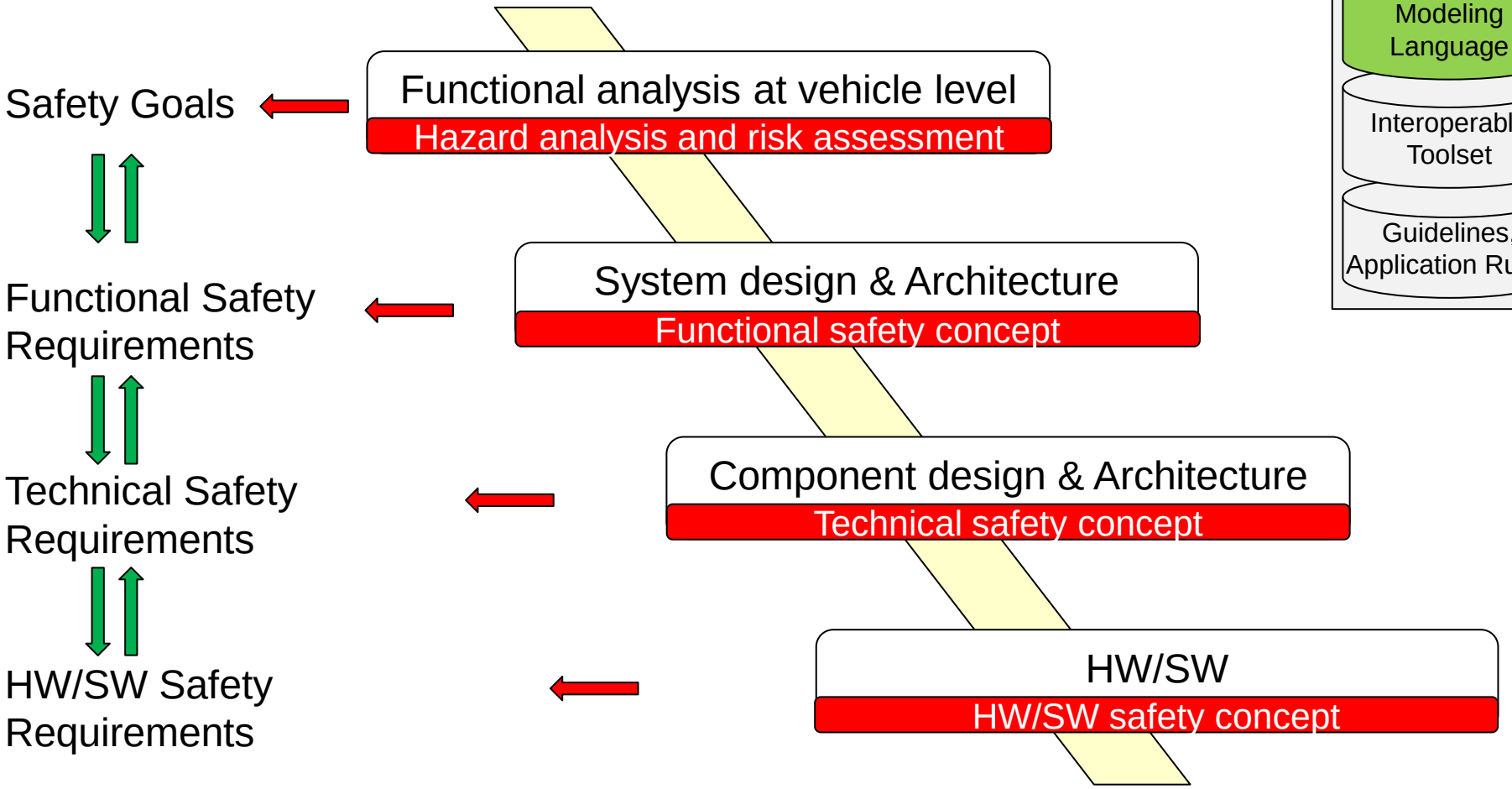
6-6 Specification of software safety requirements



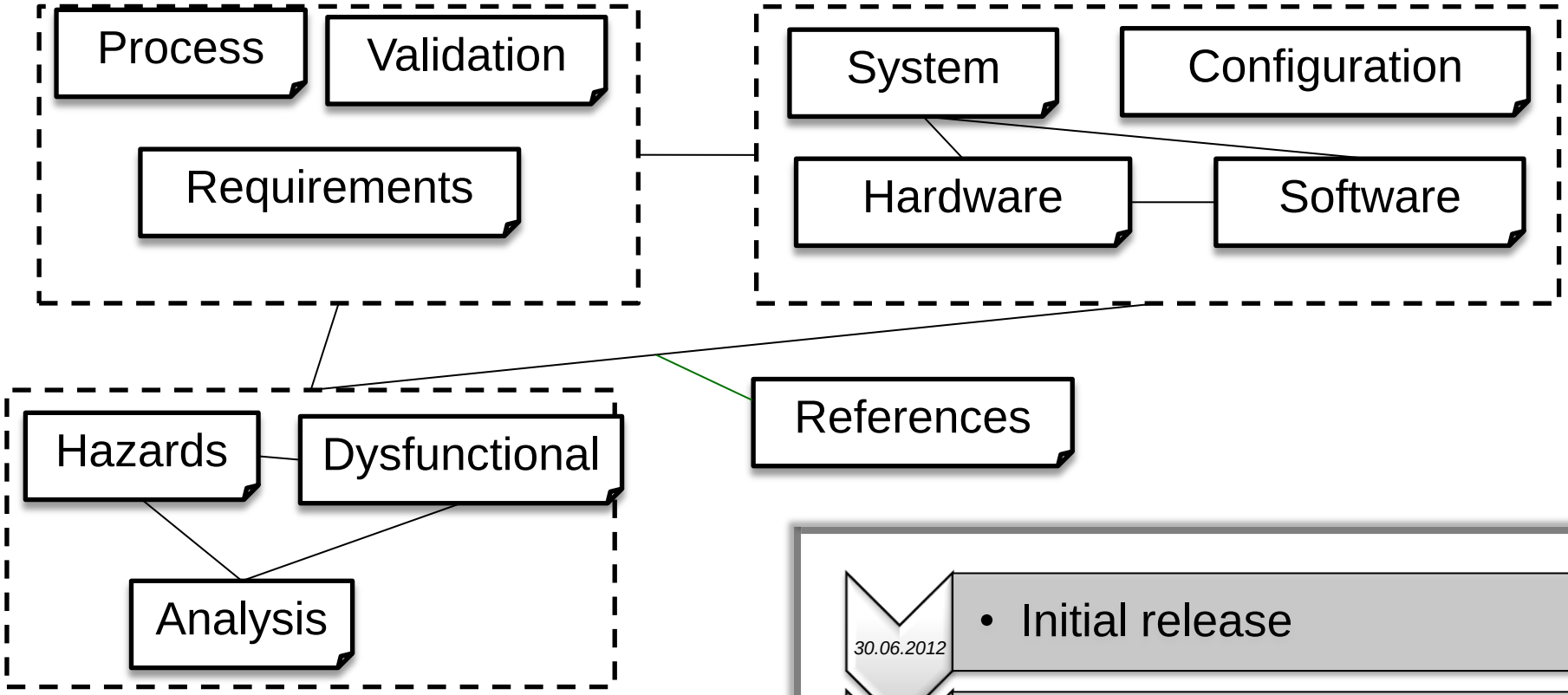
SAFE – Concept Level
HW-SW Safety concept



SAFE – Concept Level
Summary: Safety Requirement Expression



SAFE – Concept Level
Meta-model integration approach



30.06.2012
- Initial release

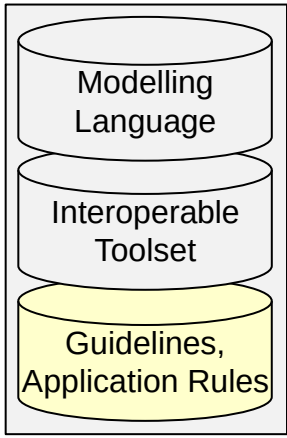
30.04.2013
- Intermediary release

28.02.2014
- Final release

Content

- Motivation
- **Concept Level**
  - Open Meta-model
  - **Assessment Methodology**
- Implementation Level
- Organization

SAFE – Concept Level
Assessment Methodology



Objectives

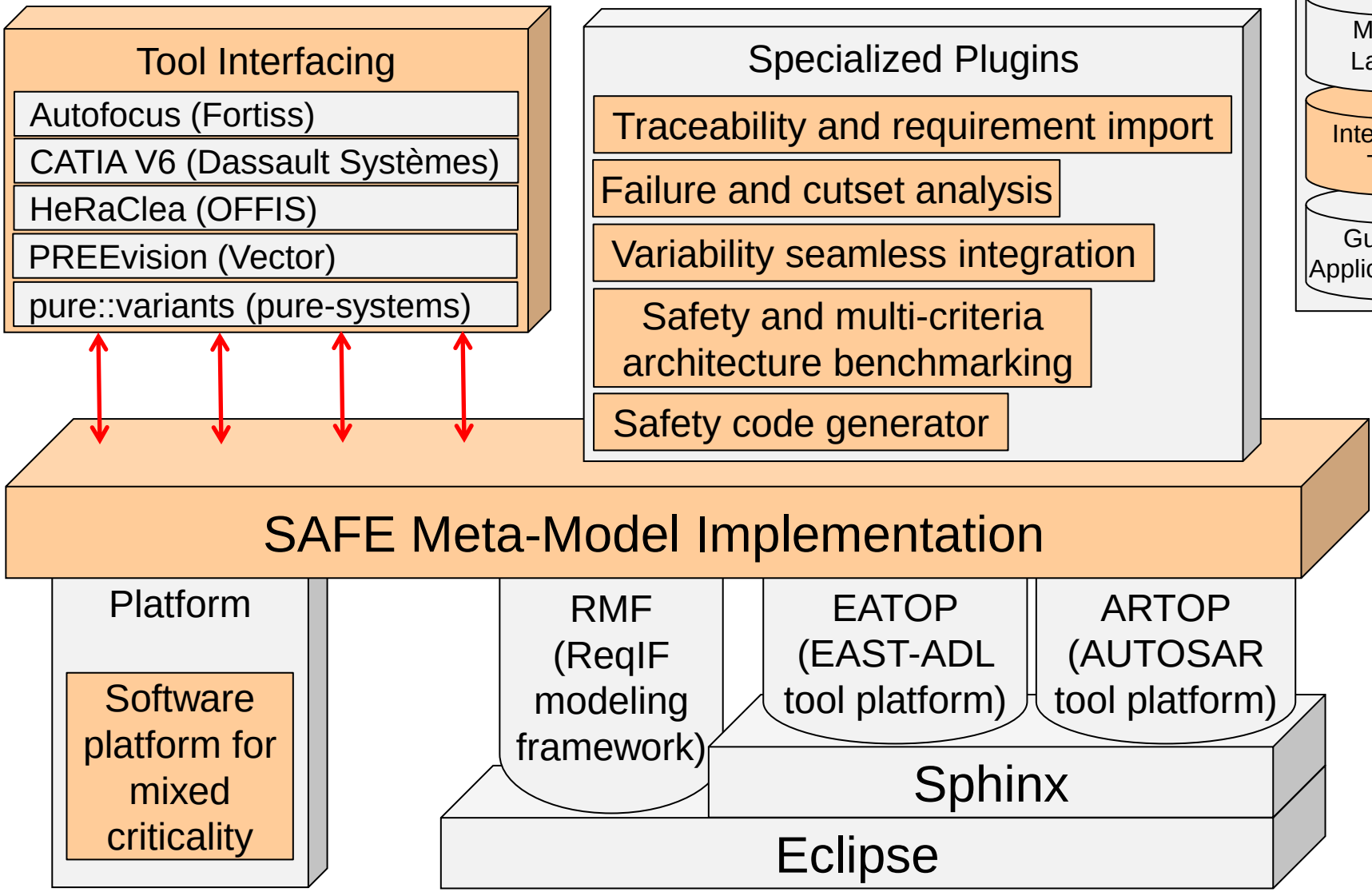
- Tackle the introduction of a comprehensive functional safety process according to ISO26262 to a real engineering team
- Assessment procedure for functional safety
- Process step and adequate measures to allow seamless implementation in the different engineering disciplines

Content

- Motivation
- Concept Level
- **Implementation Level**
  - **Technology Platform**
  - Industrial use cases
- Organization

SAFE – Implementation Level

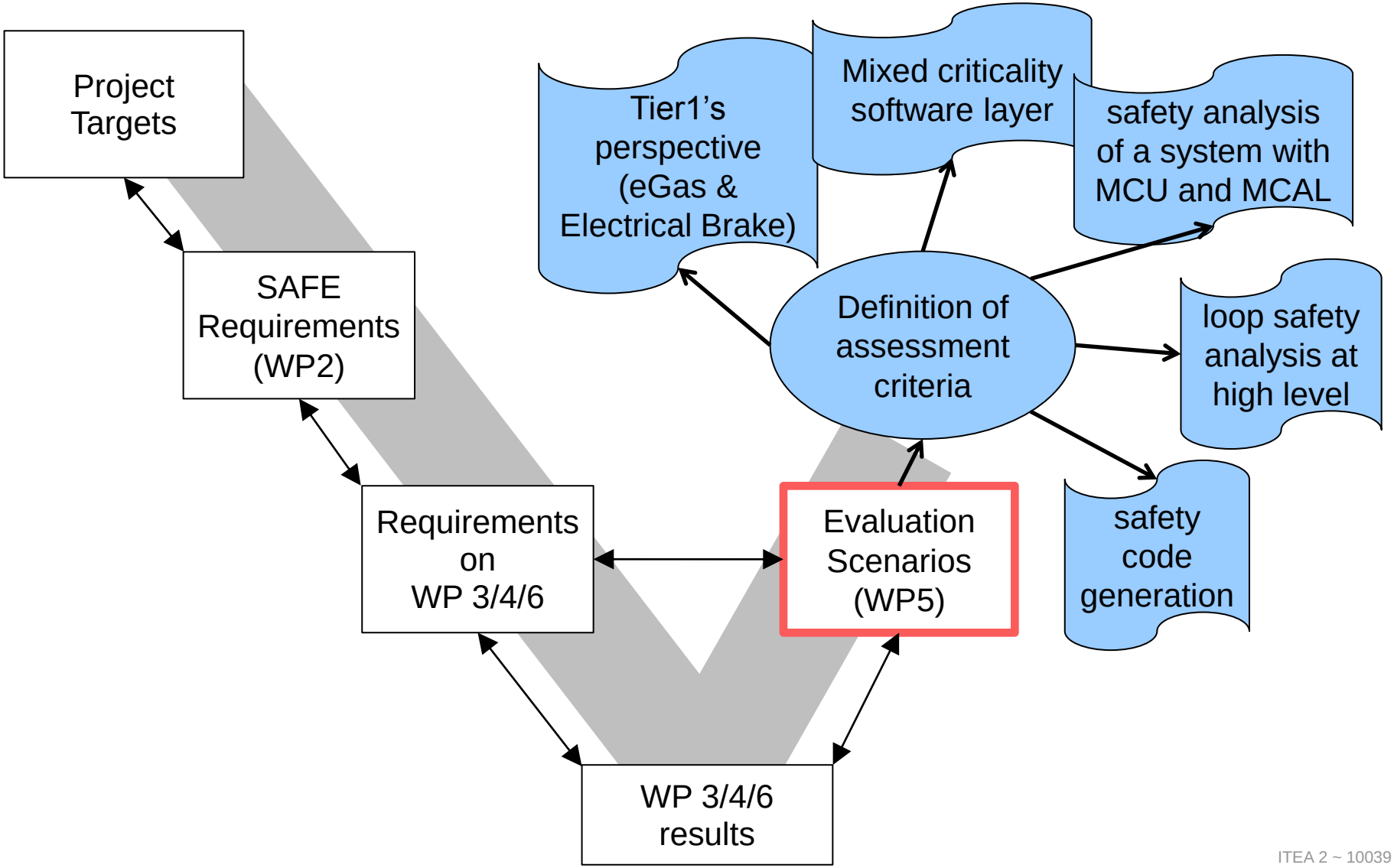
Meta-model for Model based Safety Analysis



Content

- Motivation
- Concept Level
- **Implementation Level**
  - Technology Platform
  - **Industrial use cases**
- Organization

SAFE – Implementation Level
Evaluation Scenarios



Content

- Motivation
- Concept Level
- Implementation Level
- **Organization**

SAFE – Project Organization
Consortium

OEMs
- BMW-CarIT (G)

Engineering Partner
- AVL Software & Function (G)

Accreditation body
- TÜV NORD Mobilität (G)

Tiers1
- Continental Automotive (G)
- Continental Automotive (Fr)
- Continental Teves (G)
- Valeo EEM(Fr)
- ZF (G)

Silicon Supplier
- Infineon Technologies (G)

Tool suppliers & SME
- Aquintos (G)
- Dassault Systemes (Fr)
- ITEMIS France (Fr)
- Pure Systems (G)
- TTTEch (Aut)

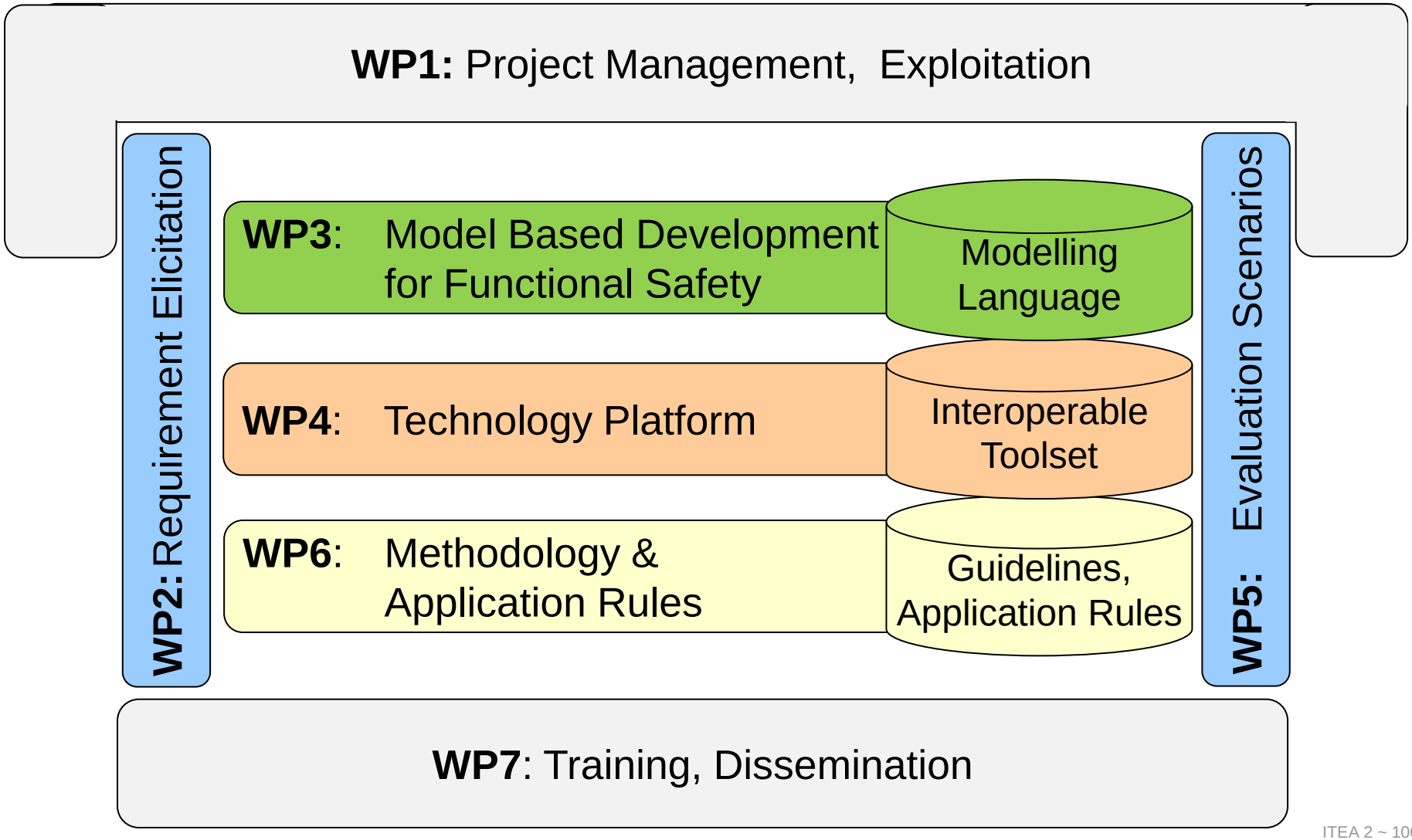
Academia
- Fortiss (G)
- FZI, Karlsruhe University (Ge)
- OFFIS (Ge)
- LaBRi, Bordeaux University (Fr)

SAFE – Project Organization
Basic Data

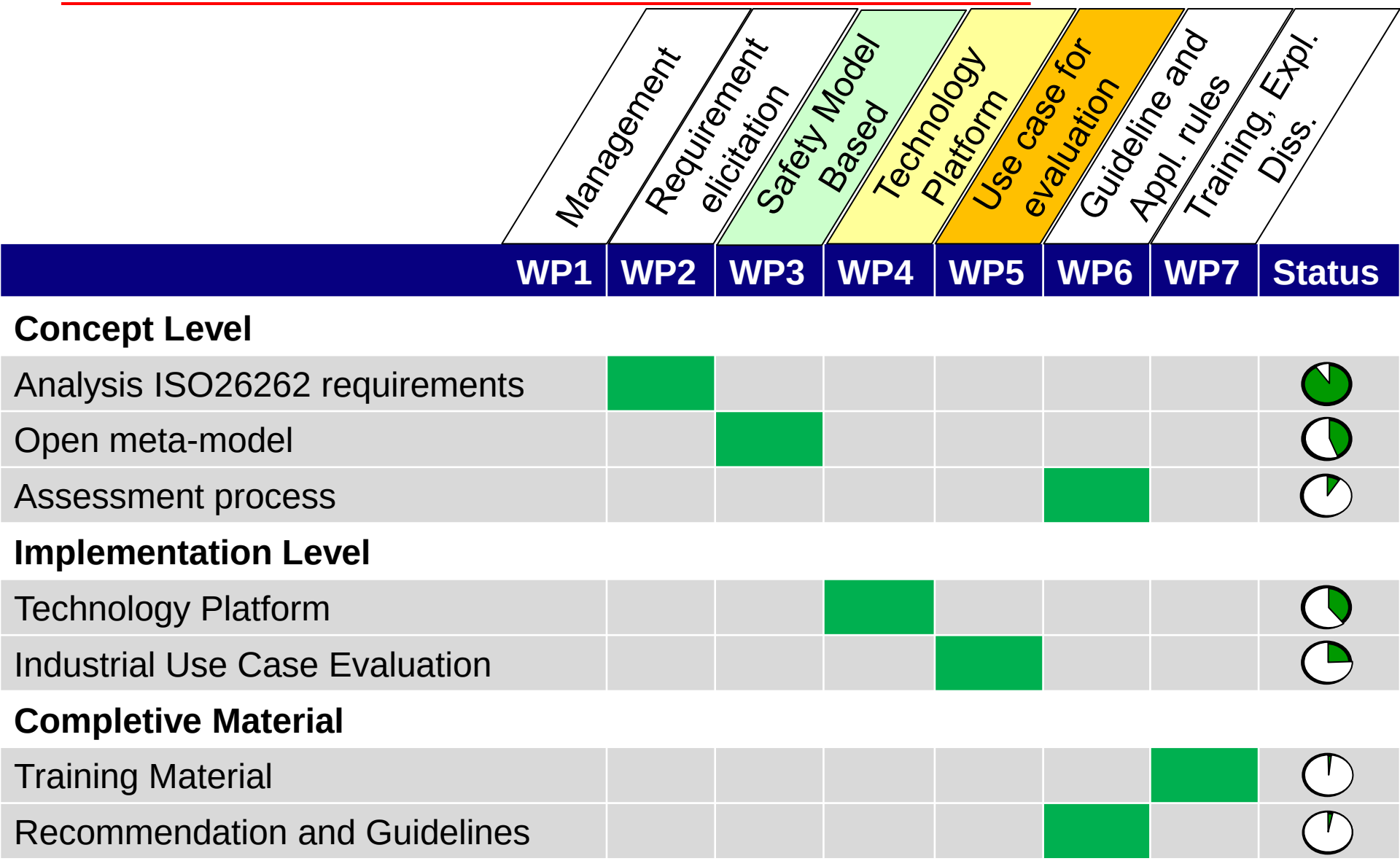
- Duration: 36 months
- Timing: 01.07.2011 – 30.06.2014
- Partners: 18
- Countries: Austria, France, Germany
- Budget: 12 M€
- Coordinator: Dr. Stefan Voget, Continental Automotive (G)

- OEM Advisory Board
  - Audi (G)
  - Daimler (G)
  - Fiat (It)
  - Renault (Fr)
  - Volvo Technology (Swe)

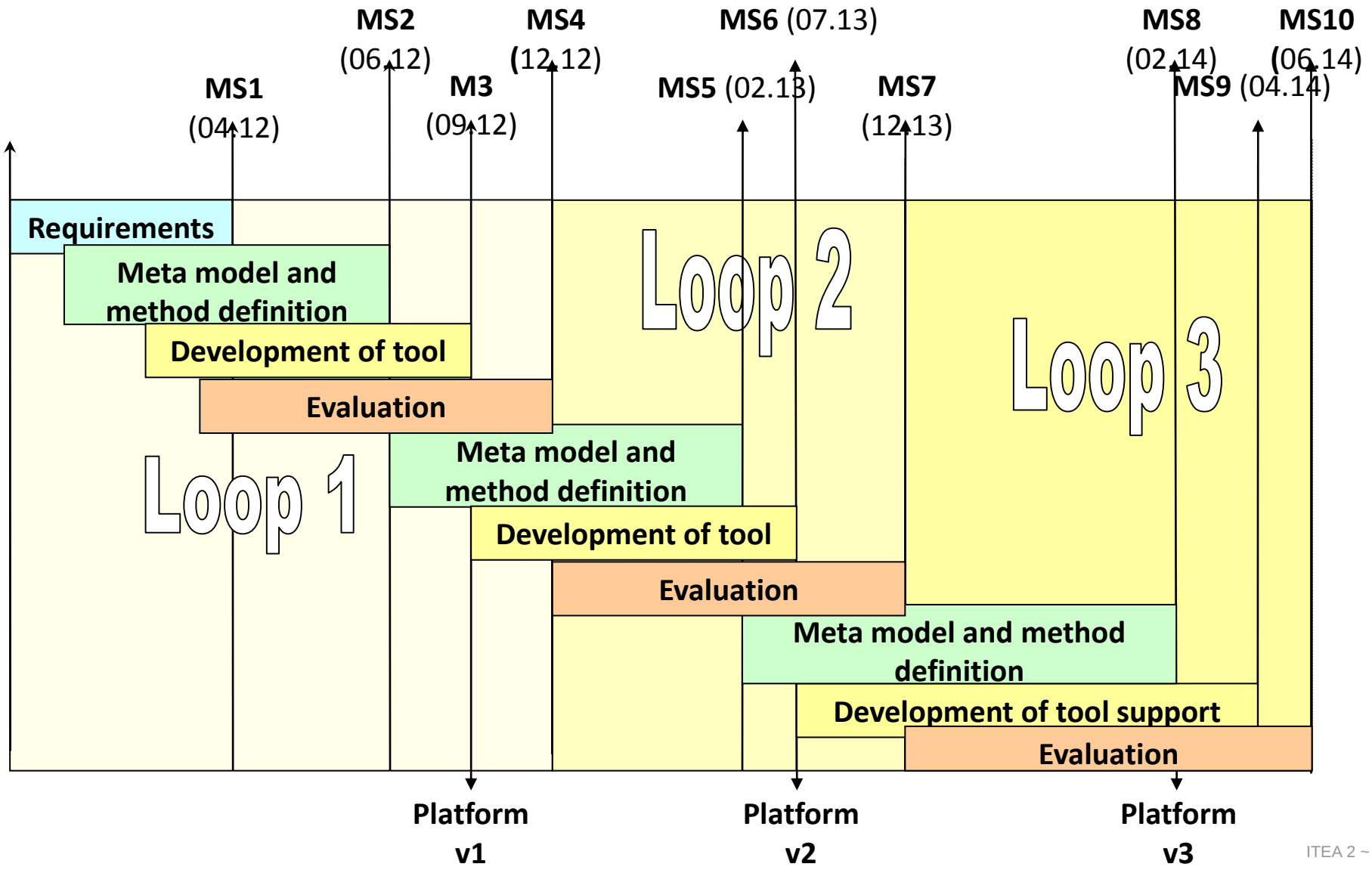
SAFE – Project Organization
Work-Package Structure



PART 1 – The Project
Results



SAFE – Project Organization
Milestones



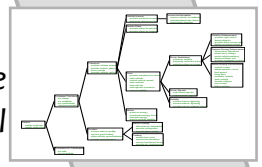
SAFE – Miscellaneous

Link to AUTOSAR

AUTOSAR standardizes

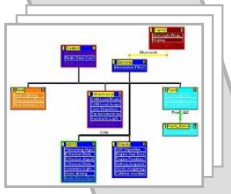
- ECU SW architecture
- Basic SW
- Application Interfaces
- Methodology
- Templates – Representation
- AUTOSAR R4.0 includes safety mechanism and documentation report

Feature Model

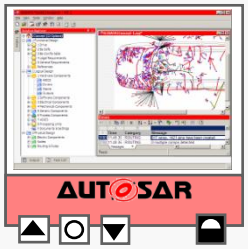


Functional architecture

System architecture



Softwrare Architecture & Implementation

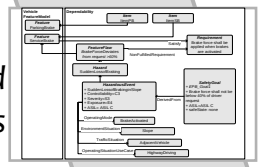


Model-Based Development

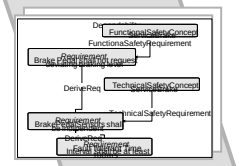
SAFE provides to AUTOSAR

- Set up link to ISO26262 and engineering processes
  - Complete overview on system level
  - Complement hardware description
    - Mechanisms for safety code generation

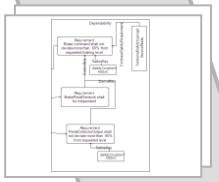
Hazard Analysis



Functional Safety Concept



Technical Safety Concept



Refined Technical Safety Concept

Model-Based Safety Analysis

SAFE – Miscellaneous
Market Impact

OEMs

- Methods and tools that will give the flexibility to develop new architectures with a Safety In the Loop approach
- Possibility to deploy new architectures with a *shorter time to market*.

First Tiers

- Possibility to demonstrate safety conformity of developed ECUs and automotive subsystems
- Optimize the cost of the development
- Allow reduction of re-certification due to late changes

Semiconductor manufacturers and IP hardware providers

- Help to develop and focus on new component architectures capable to support ISO26262.

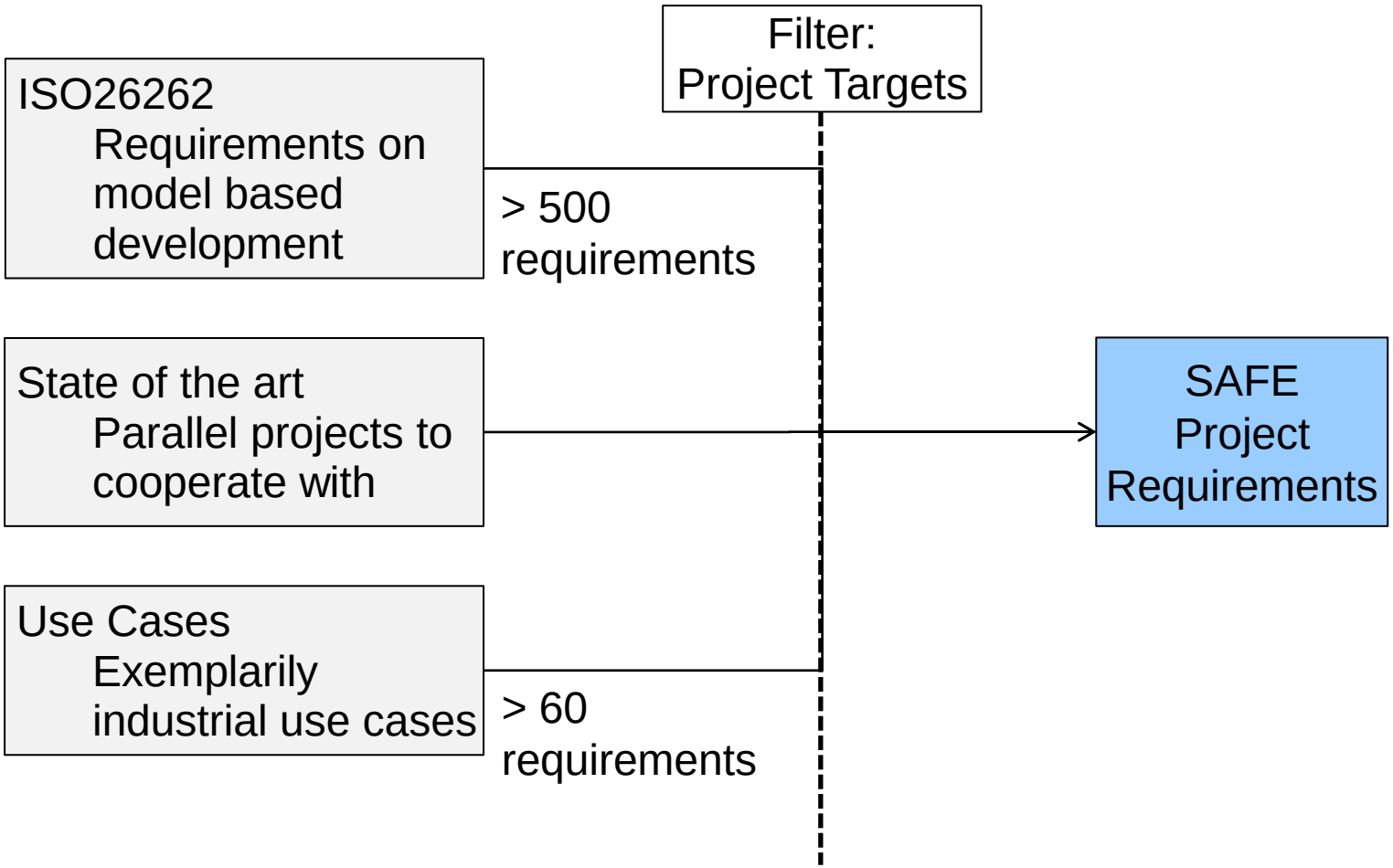
Tool vendors

- Opportunity to develop an integrated tool-chain, including design and safety analysis in a single process
- Easy to adapt the tools to other embedded domains with strong concerns in Safety like Aerospace and Train.

Content

- **BACKUP**

SAFE – WP 2
Requirements Elicitation



ITEA 2

INFORMATION TECHNOLOGY FOR EUROPEAN ADVANCEMENT

SAFE

Thank you for your attention

This document is based on the SAFE project in the framework of the ITEA2, EUREKA cluster program Σ! 3674. The work has been funded by the German Ministry for Education and Research (BMBF) under the funding ID 01IS11019, and by the French Ministry of the Economy and Finance (DGCIS). The responsibility for the content rests with the authors.