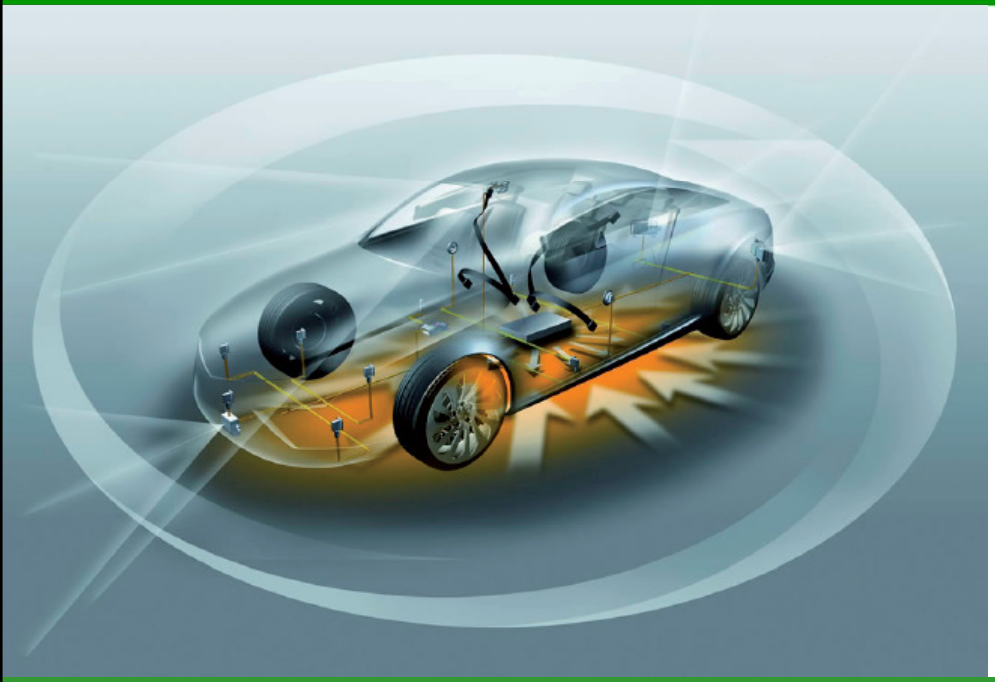
ITEA 2

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
MINISTÈRE DE L'ÉCONOMIE DES FINANCES ET DE L'INDUSTRIE

dgcis
direction générale de la compétitivité de l'industrie et des services

EUREKA

Content

- **Motivation**
- Project Organization
- Work Packages
- Miscellaneous

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 and Goals

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

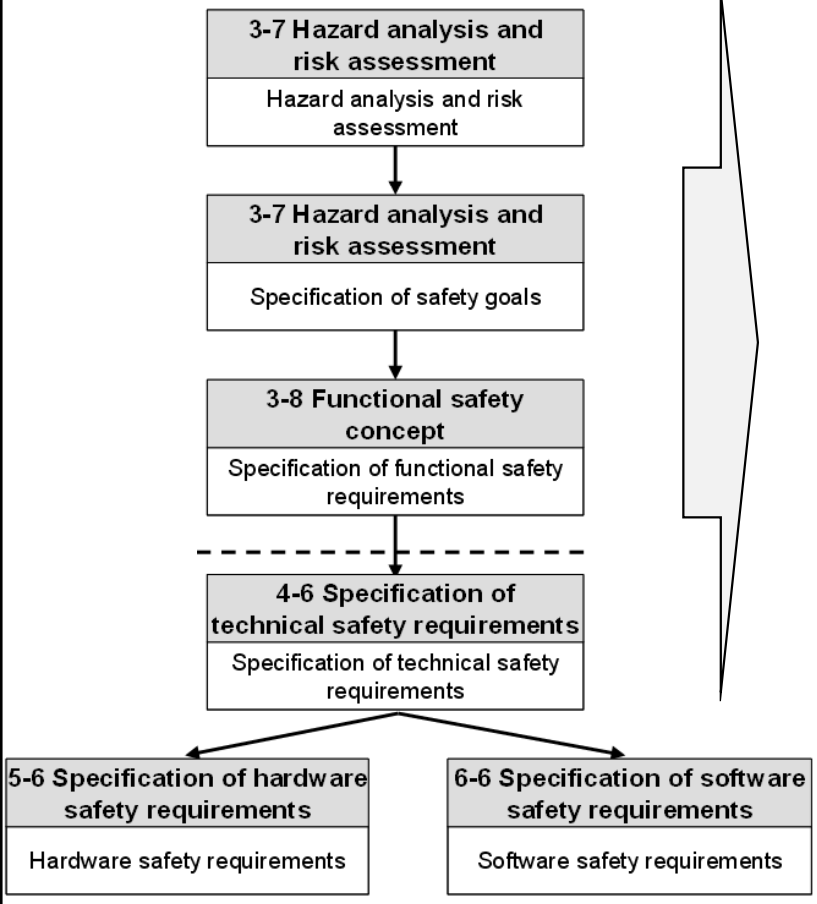
9. ASIL-oriented and safety-oriented analyses

- **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

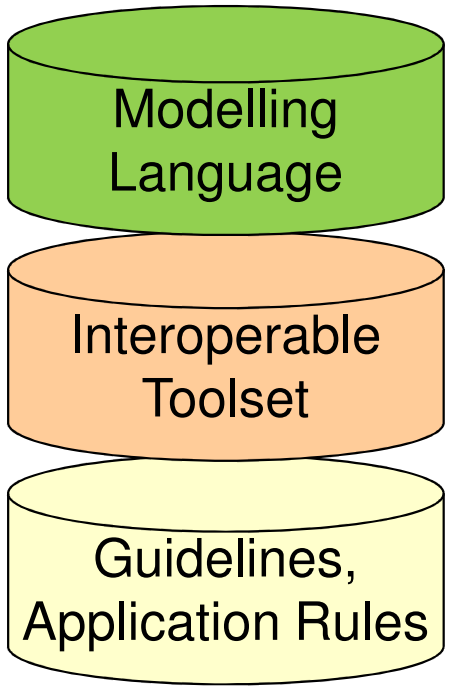
10. (Informative) Guidelines on ISO 26262

SAFE – Motivation
Project Vision

ISO26262

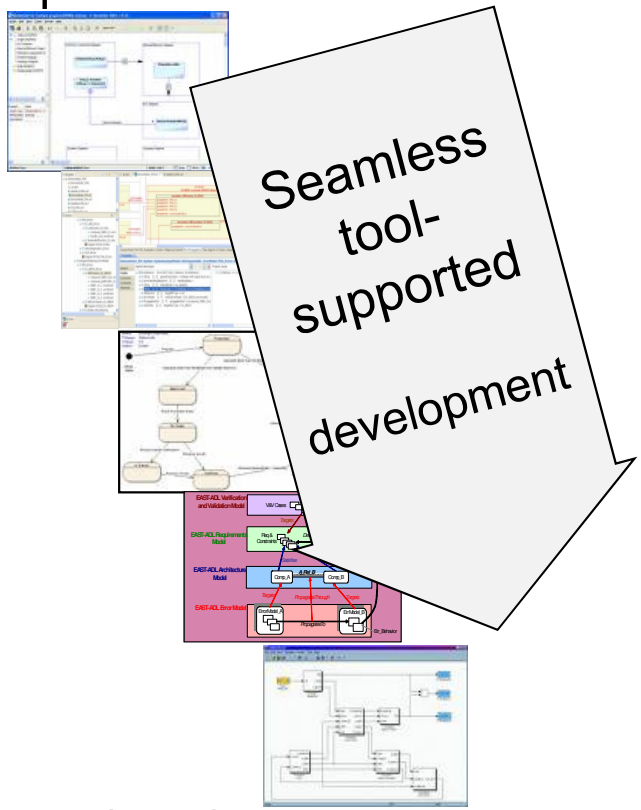


SAFE



Developer

Requirements



HW-SW Component Models

SAFE – Motivation
Approaches

To achieve the goals, SAFE will bring a new approach based on:

- **Model based technology** to anticipate safety evaluation
- **Process assessment** to demonstrate conformance to the standard
- I**ntegrated workflow including design and safety analysis** in a fully traceable and automated tool chain
- **Concurrent engineering experience** on new technology to ensure interoperability of processes within the supply chain
- **Optimization of verification process**, using new technology for assessment (automated FTA, architecture benchmark, ...)
- **Guidance and design guidelines to define safety patterns**
  - architecture, AUTOSAR platform configuration, product line management, independence and non interference of functions and components, code generator ...

SAFE – Motivation
Expected Results

- **Open meta model** for description of system, software, hardware
- **Technology Platform**
- **Training Material**
- **Industrial use cases** demonstrating methods and tools
- **Assessment process** to demonstrate compliance to ISO26262
- **Recommendation and Guidelines** for
  - System decomposition for effective design of safety mechanism
  - Compliance with architecture constraints and safety mechanism
  - AUTOSAR platform configuration for safety
  - Inclusion of COTS in a safety system

SAFE – Motivation
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

- Motivation
- **Project Organization**
- Work Packages
- Miscellaneous

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
Consortium

OEMs

- BMW-CarIT (G)

Tiers1

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

Engineering Partner

- AVL Software & Function (G)

Silicon Supplier

- Infineon Technologies (G)

Tool suppliers & SME

- Aquintos (G)
- Dassault Systemes (Fr)
- ITEMIS France (Fr)
- Pure Systems (G)
- TTTEch (Aut)

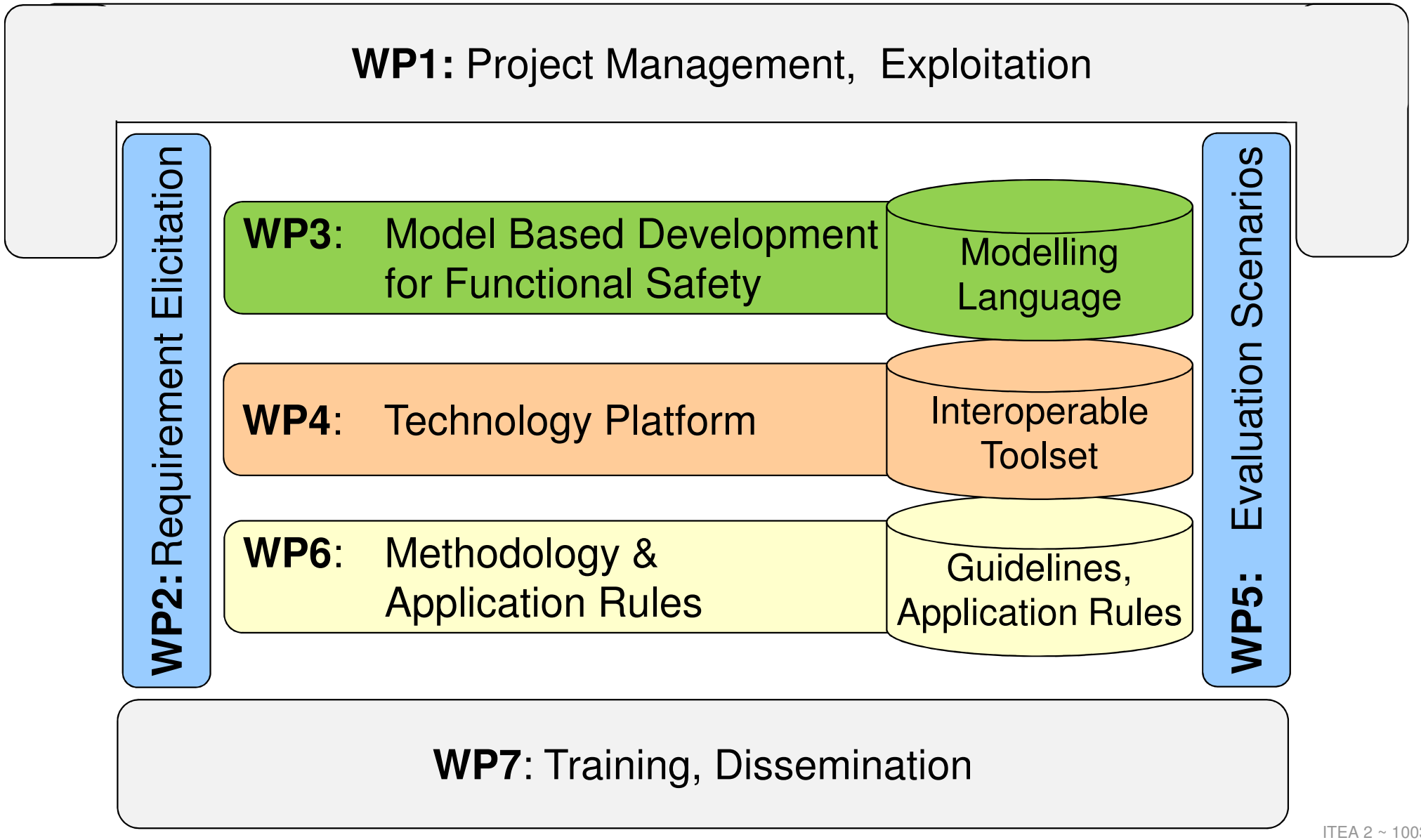
Accreditation body

- TÜV NORD Mobilität (G)

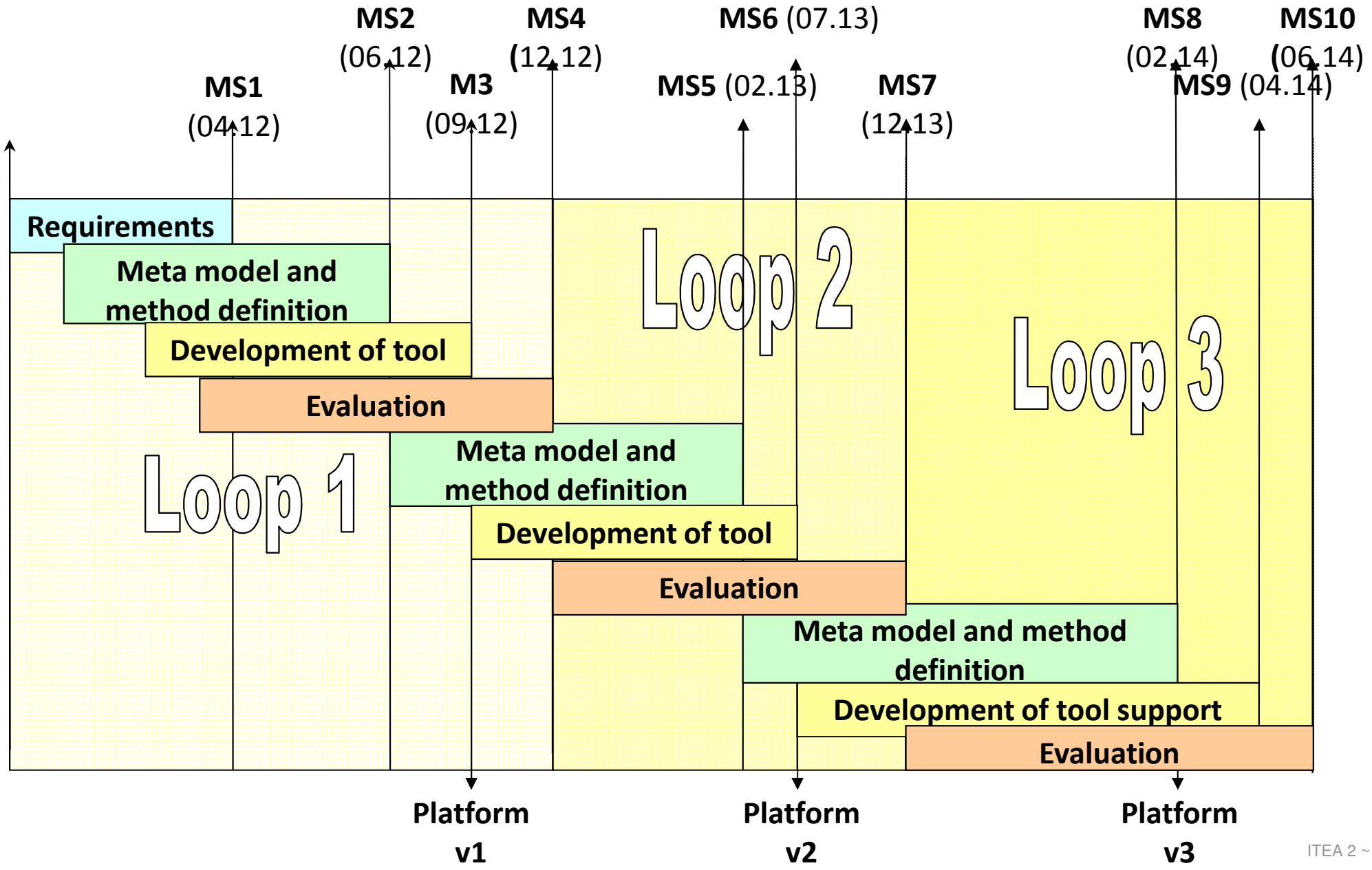
Academia

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

SAFE – Project Organization
Work-Package Structure



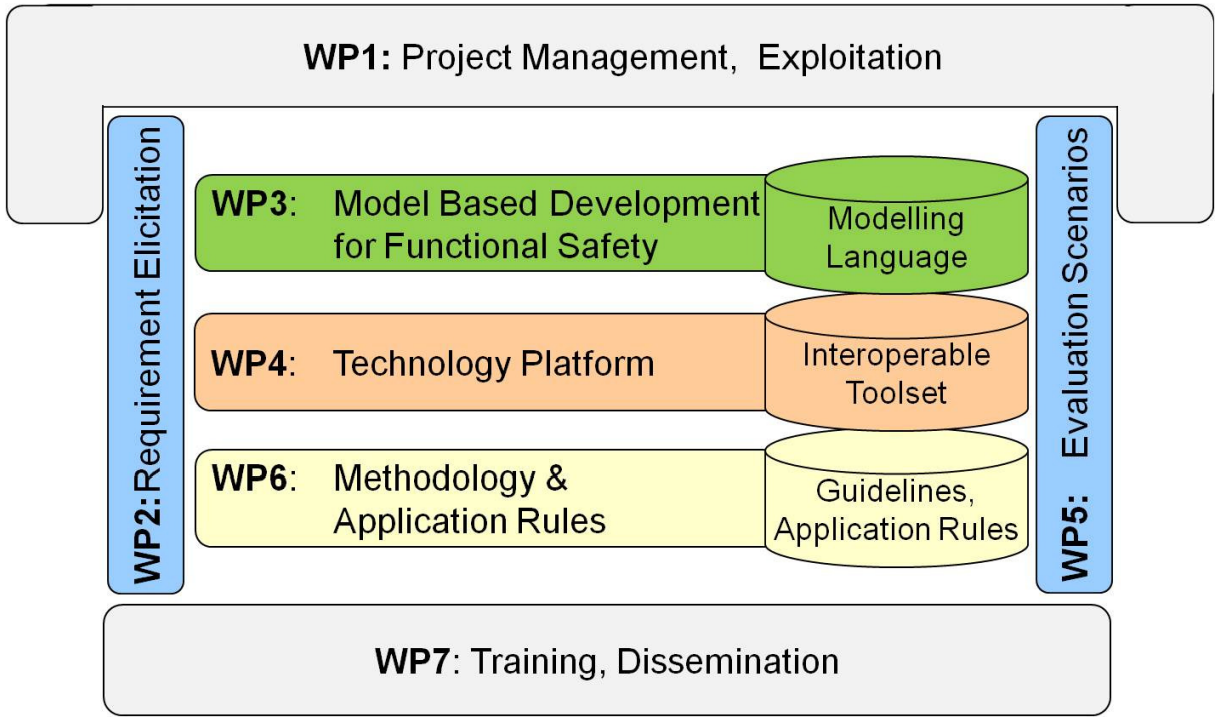
SAFE – Project Organization
Milestones



Content

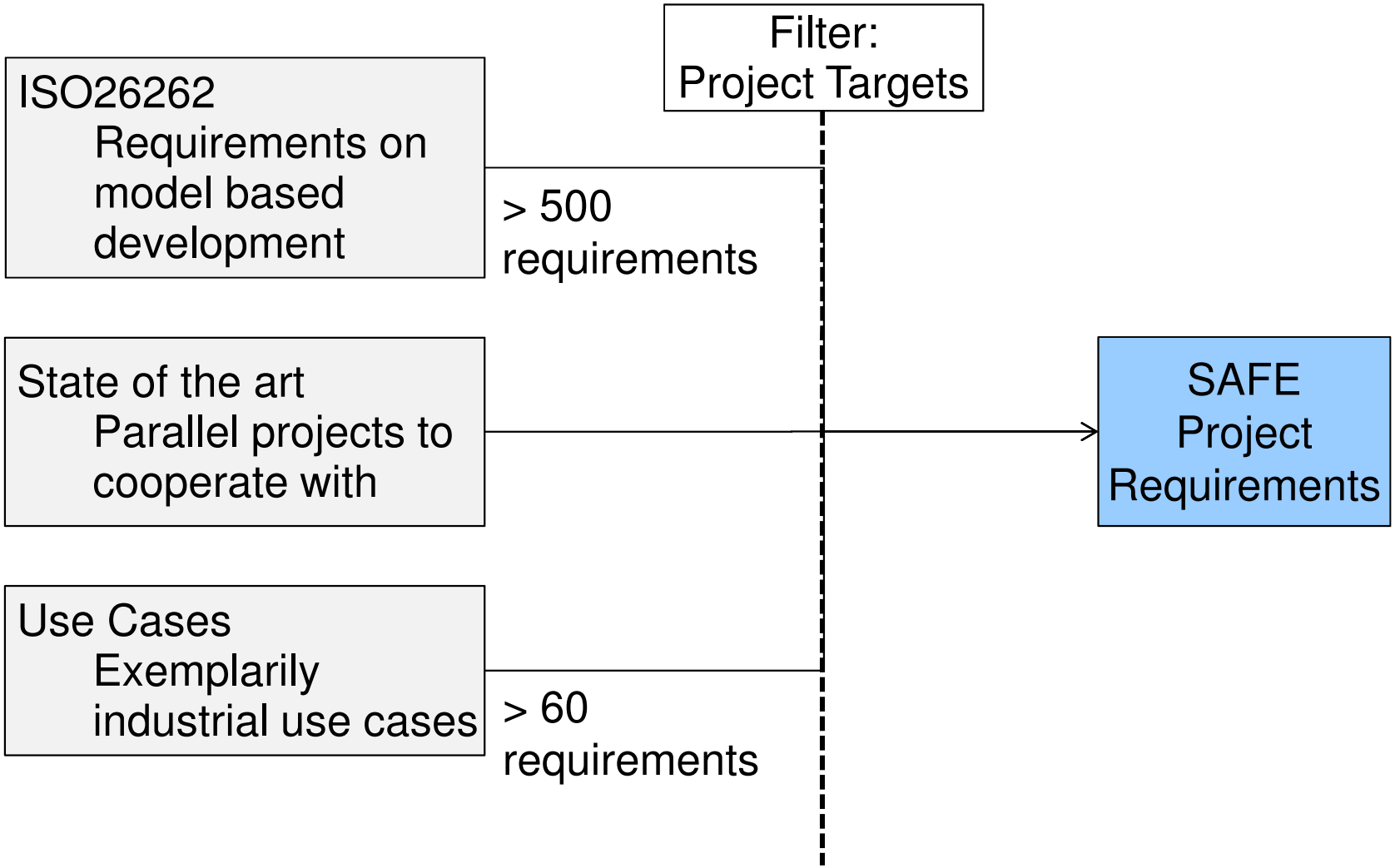
- Motivation
- Project Organization
- **Work Packages**
  - WP2 – Requirements Elicitation
  - WP3 – Model Based Development for Functional Safety
  - WP4 – Technology Platform
  - WP5 – Evaluation Scenarios
  - WP6 – Methodology & Application Rules
- Miscellaneous

Content

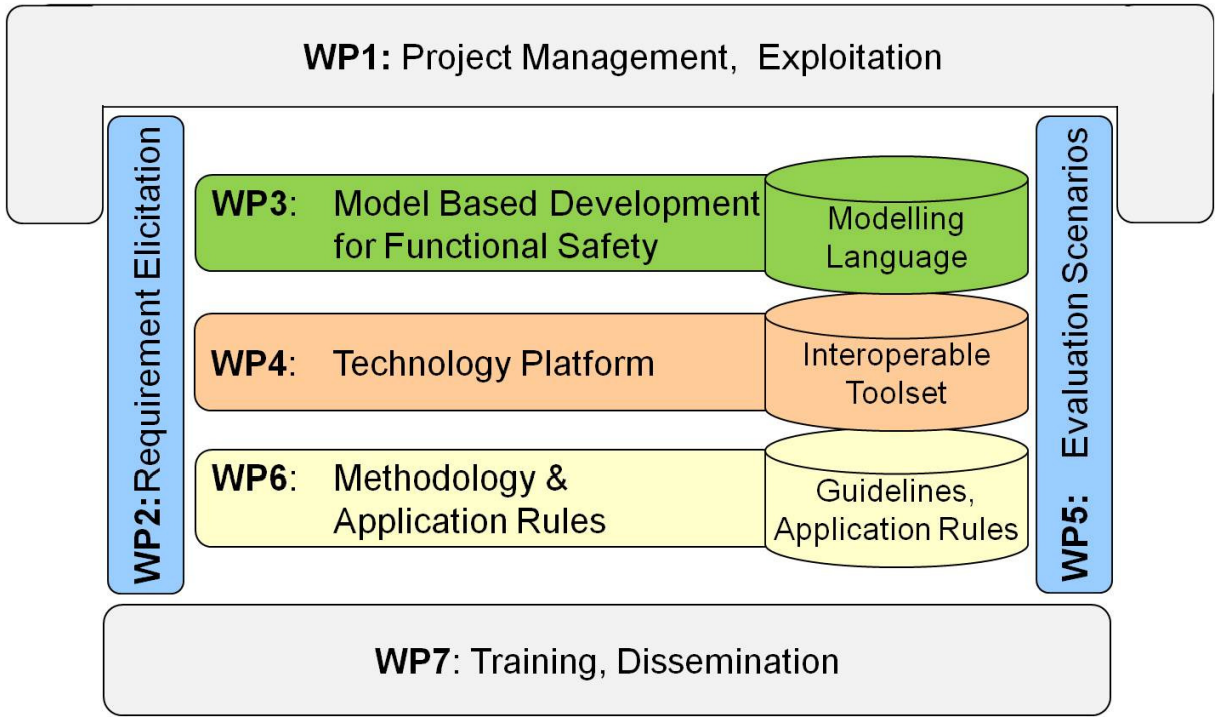


- Work Packages
  - **WP2 – Requirements Elicitation**
  - WP3 – Model Based Development for Functional Safety
  - WP4 – Technology Platform
  - WP5 – Evaluation Scenarios
  - WP6 – Methodology & Application Rules

SAFE – WP 2
Requirements Elicitation

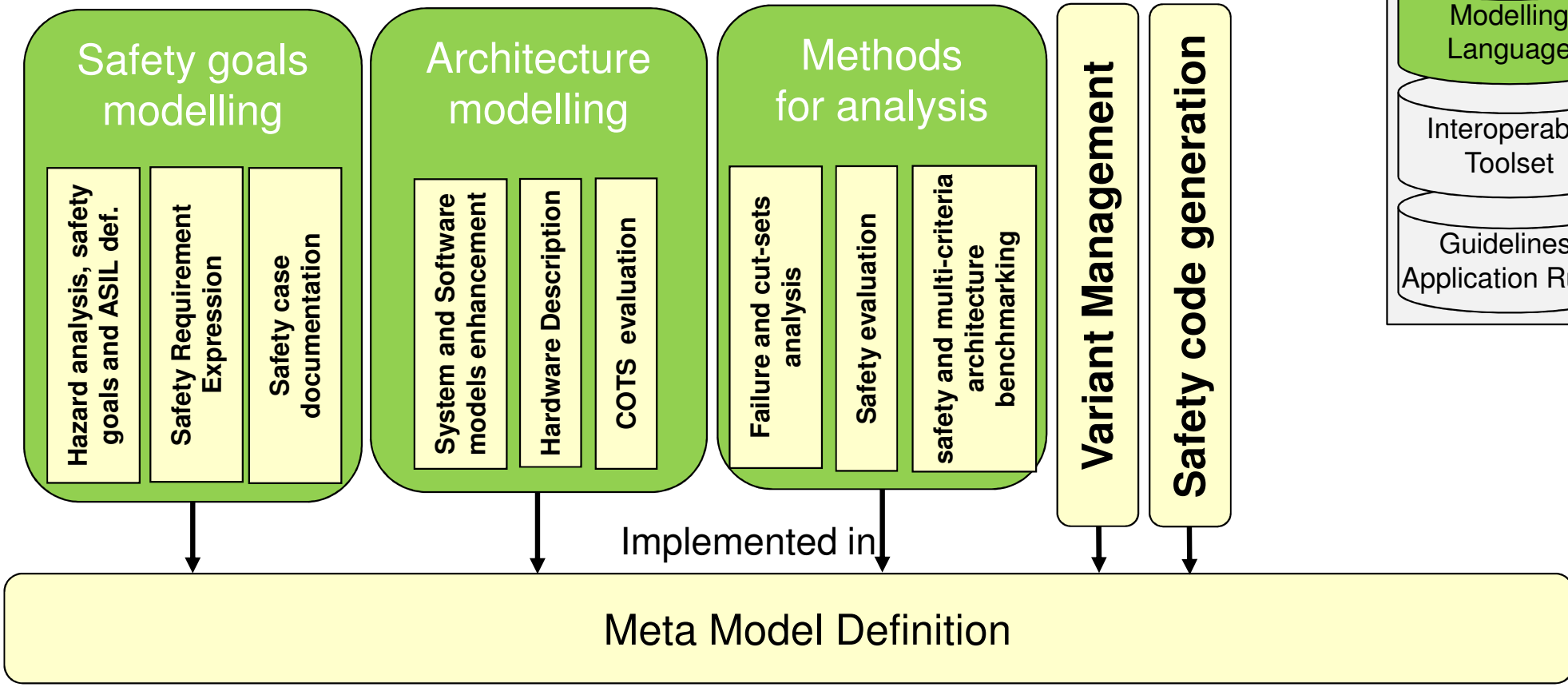


Content



- Work Packages
  - WP2 – Requirements Elicitation
  - **WP3 – Model Based Development for Functional Safety**
  - WP4 – Technology Platform
  - WP5 – Evaluation Scenarios
  - WP6 – Methodology & Application Rules

SAFE – WP 3
Model based dev. for Functional Safety



Approach: base technologies are used and extended

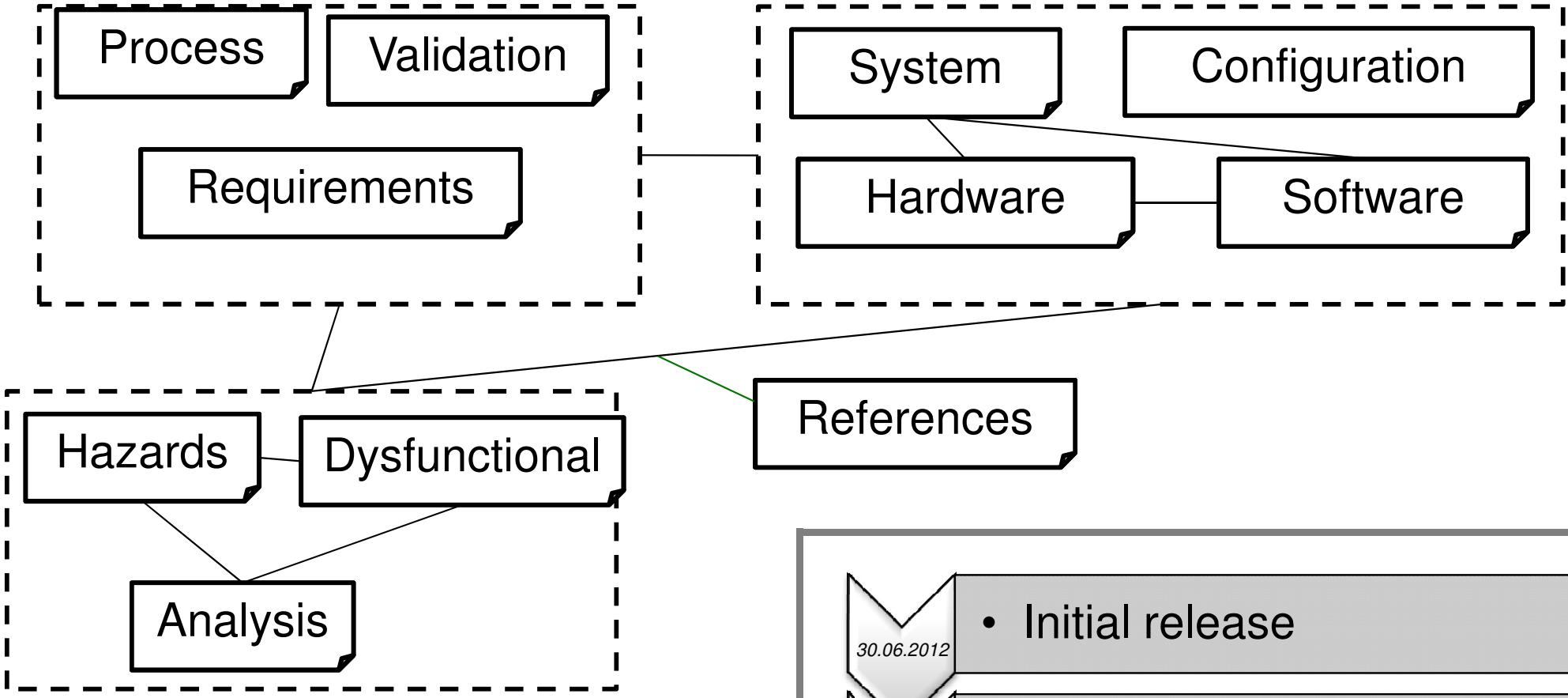
ReqIF

EAST-ADL

AUTOSAR

IP-XACT

SAFE – WP 3
Meta-model integration approach



30.06.2012
- Initial release

30.04.2013
- Intermediary release

28.02.2014
- Final release

SAFE – WP 3
Use meta-model backbone for SAFE

SAFE Technology Platform

MM:
SAFE project

Toolplatform:
SAFE project
&
Eclipse A-IWG

USES

Req-IF
MM: OMG
Toolplatform: Eclipse RMF project

USES

EAST-ADL
MM: EAST-ADL Association
Toolplatform: EATOP (In creation phase)

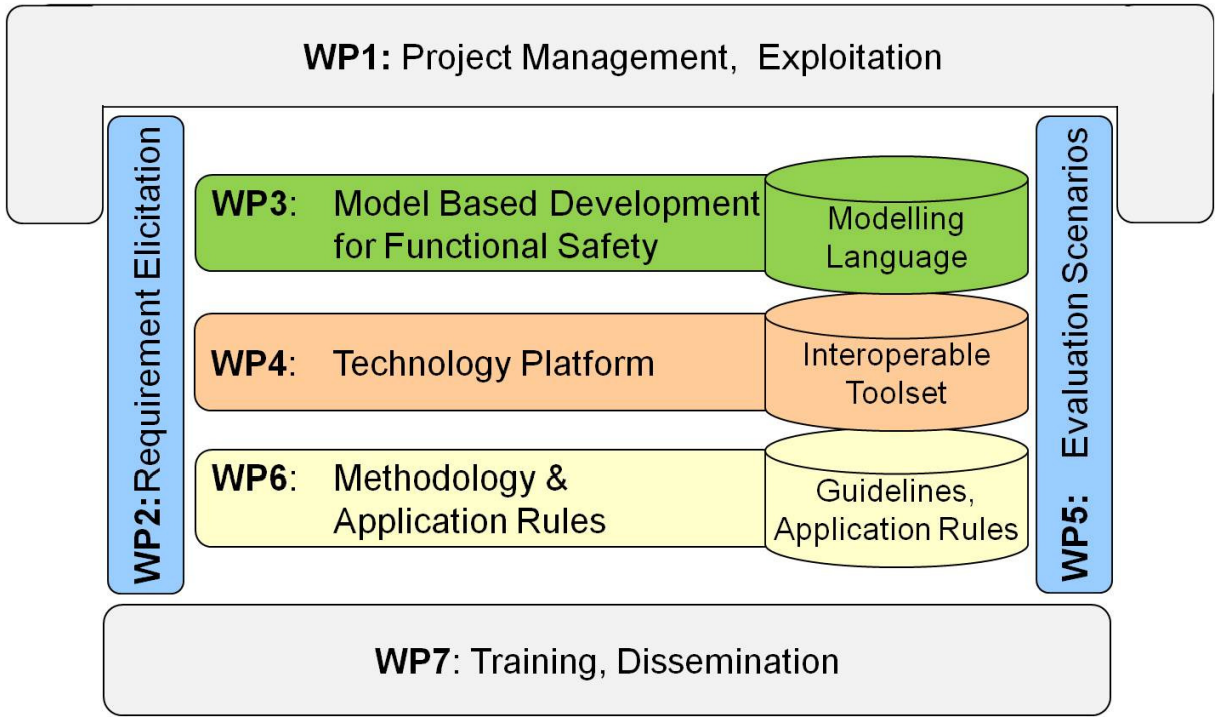
USES

AUTOSAR
MM: AUTOSAR
Toolplatform: ARTOP

USES

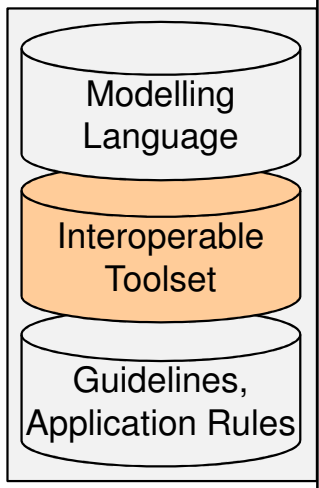
IP-XACT
MM: IEEE 1685-2009
Toolplatform: XMLSchema, Eclipse Editor

Content



- Work Packages
  - WP2 – Requirements Elicitation
  - WP3 – Model Based Development for Functional Safety
  - **WP4 – Technology Platform**
  - WP5 – Evaluation Scenarios
  - WP6 – Methodology & Application Rules

SAFE – WP 4
Technology Platform – Functional View



Specialized Plugins

- Traceability and requirement import
- Behavioural translator
- Failure and cutset analysis
- Variability seamless integration
- Safety and multi-criteria architecture benchmarking
- Safety code generator

Platform

Software platform for mixed criticality

Tool Interfacing

PREEVISION extension

Metamodel implementation

SAFE – WP 4
Technology Platform – Architectural View

SAFE Plugin | SAFE Plugin | SAFE Plugin | SAFE Plugin

SAFE Technology Platform

RMF (Req IF)

EATOP (EAST-ADL)

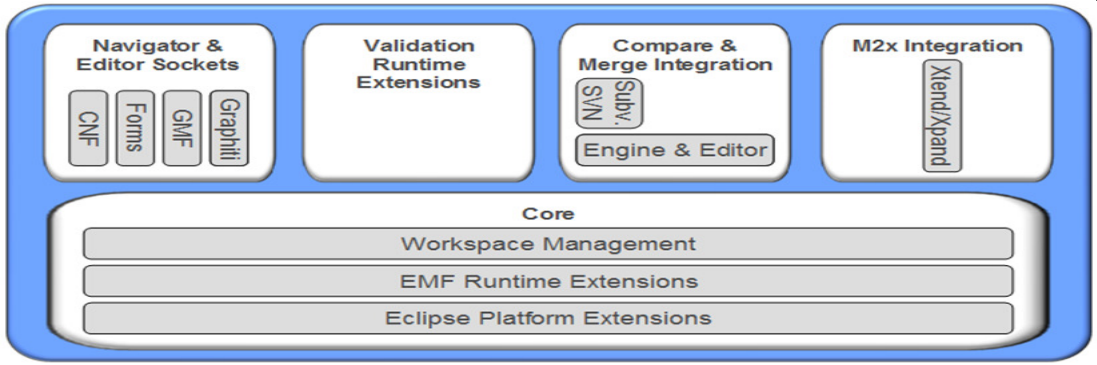
- Validation
- EAST-ADL Explorer
- EAST-ADL Meta Model Implementation
- Serialization
- Abstraction level M2M
- EAST-ADL Editor
- Tool Adapters

ARTOP (AUTOSAR)

User Group that implements the AUTOSAR meta-model in an Eclipse based platform.

DSDP (IP-XACT)

SPHINX



Eclipse

SAFE WP4 - technology platform
Meta Model Implementation

Goals & expected results

- Based on existing meta-models (EAST-ADL2/SysML, AUTOSAR, Matlab/ Simulink, SystemC, IP-XACT)
- Enrich them with new concepts to support
  - failure description, failure mode analysis, and other information necessary to perform safety analysis
- Definition in EMF/Ecore, generation of corresponding model and edit plug-ins in Java
- Integration in to Artop/Sphinx platform
- Model-to-model transformations from existing meta-models to SAFE meta-model
- Model-to-model transformation from SAFE meta-model to UML2

SAFE WP4 - technology platform
Specialized plug-in realization

- Traceability and requirement import
  - Requirement import from Doors and Requirement Interchange format
  - Traceability between artifacts allowing linkage of SAFE meta-model with already existing modeling concepts (IP-XACT, AUTOSAR)

- Behavioural Translator
  - Dependency analysis on behavioural Simulink/ StateFlow models (optional SystemC, UML2 state chart diagrams)
  - Graphs capturing failure propagation from initial errors to resulting hazardous events
- Model Based Failure and Cut-set Analysis
- Variant seamless integration
- Safety and multi criteria architecture modelling and benchmarking
- Safety code generation

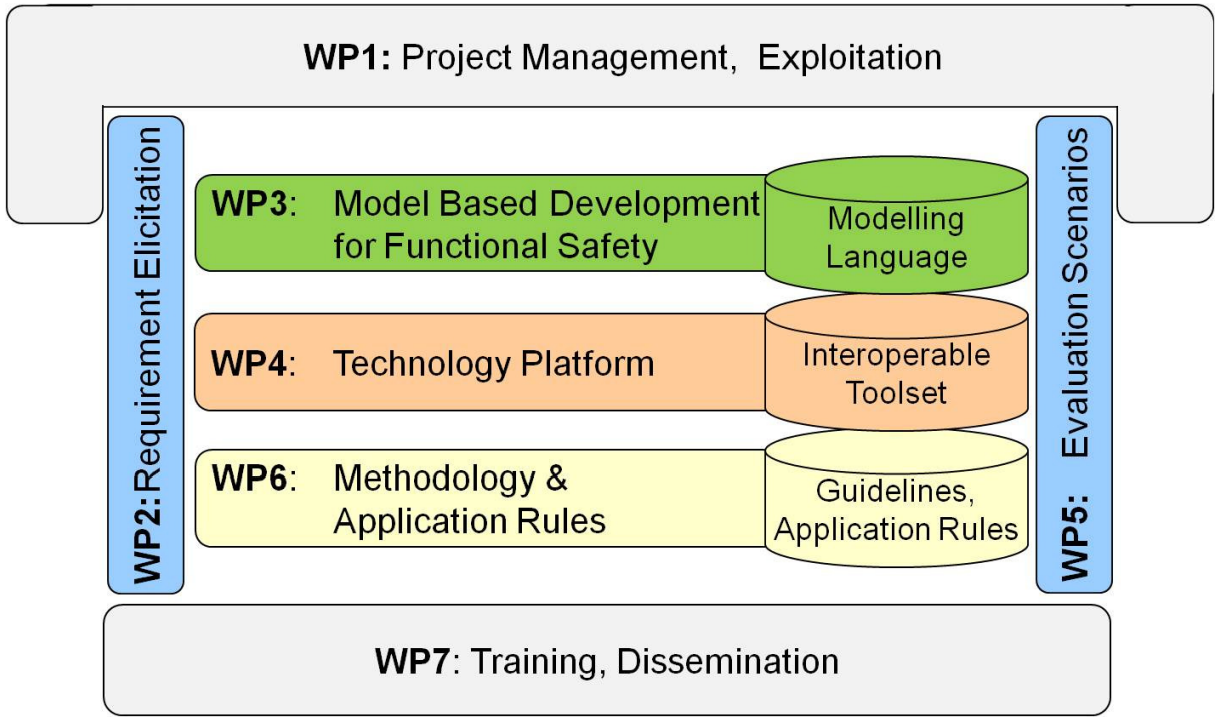
SAFE WP4 - technology platform
Specialized plug-in realization

- Traceability and requirement import
- Behavioural Translator
- Model Based Failure and Cut-set Analysis
  - Analysis of quantitative failure propagation mechanism and model based failure propagation (FMEA, FTA) including backward annotation on the initial models
  - Generate Altarica code from the model that will generate analysis results (FTA)
  - XML connector to the FTA/FMEA generator adopted from SPEEDS project results, built from fault injection and analysis of propagation
- Variant seamless integration
- Safety and multi criteria architecture modelling and benchmarking
- Safety code generation

SAFE WP4 - technology platform
Specialized plug-in realization

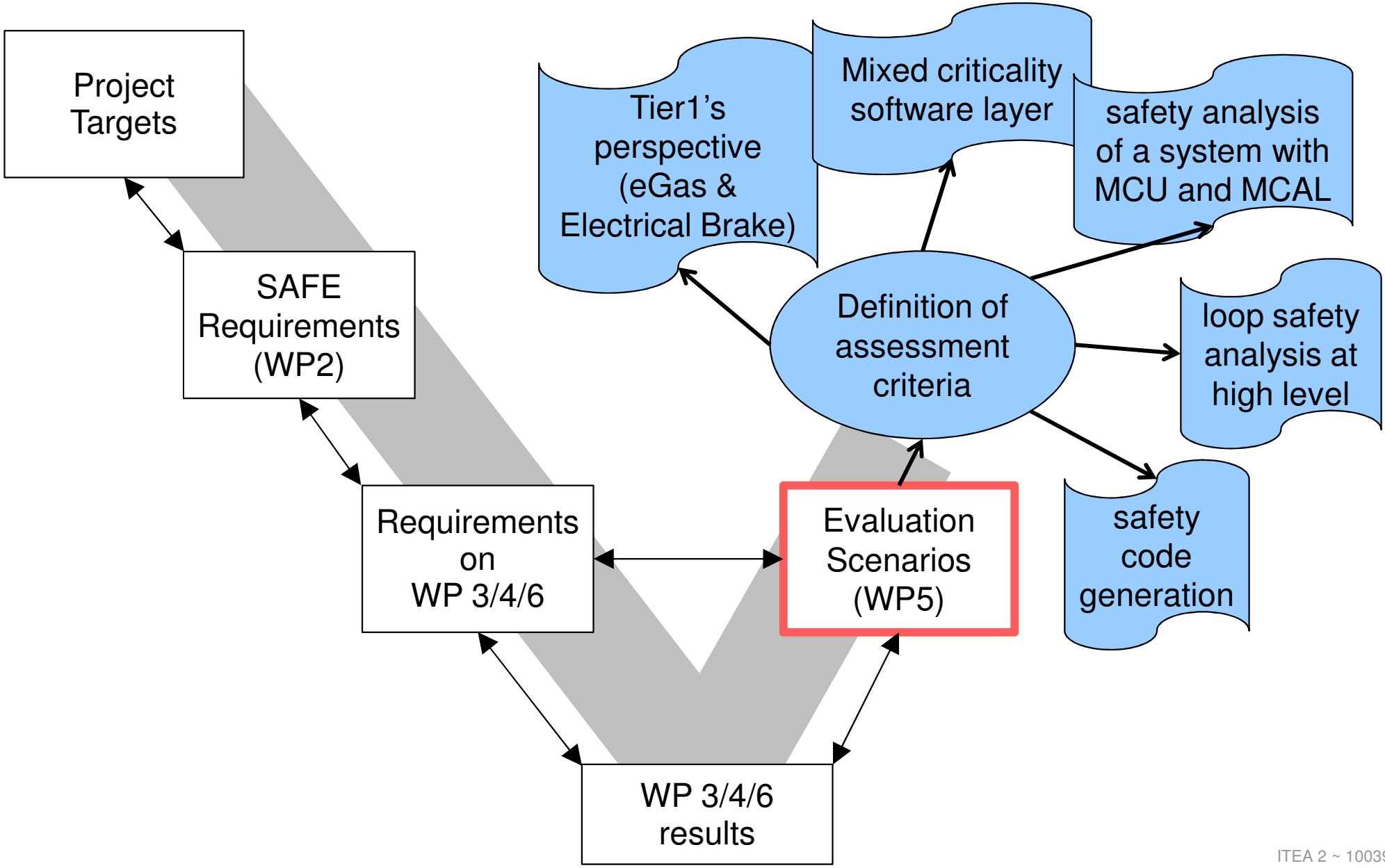
- Traceability and requirement import
- Behavioural Translator
- Model Based Failure and Cut-set Analysis
- Variant seamless integration
  - Interaction of SAFE meta-model implementation with pure::variants
- Safety and multi criteria architecture modelling and benchmarking
  - Enables model-based development of metrics to calculate properties for assessment of architecture and components (quantitative and potentially qualitative)
- Safety code generation
  - Enables generation of software assets for integrating software components according to their safety requirements

Content

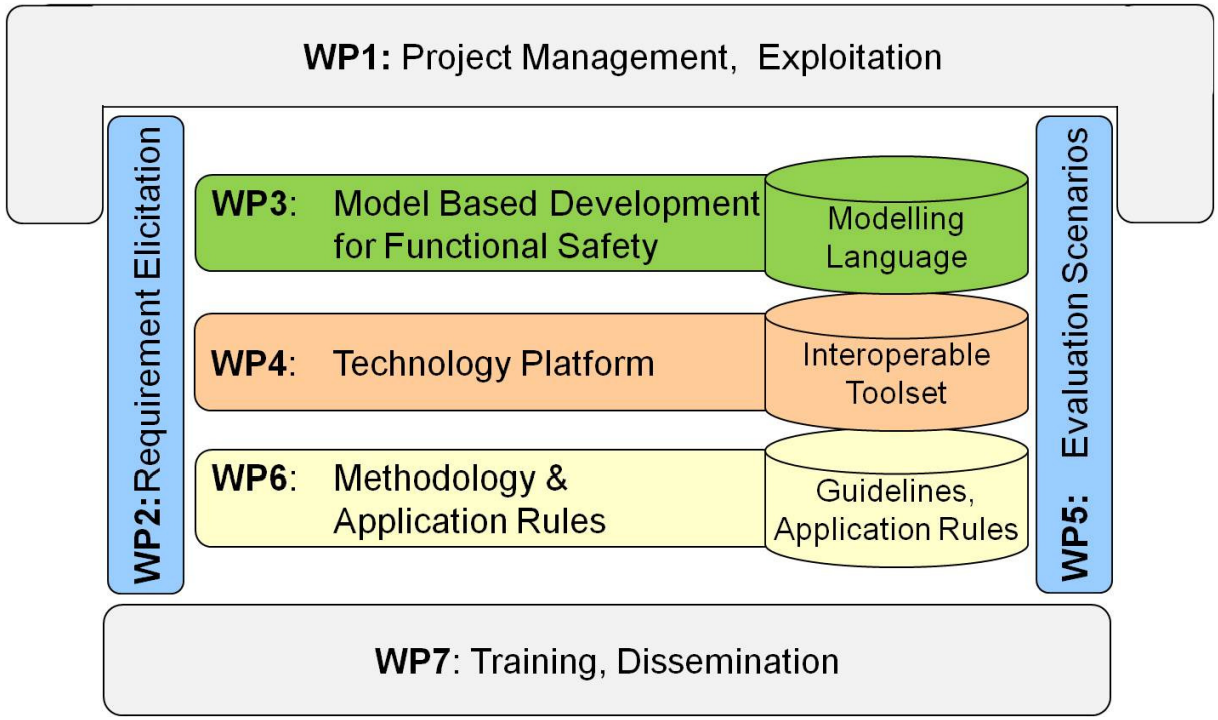


- Work Packages
  - WP2 – Requirements Elicitation
  - WP3 – Model Based Development for Functional Safety
  - WP4 – Technology Platform
  - **WP5 – Evaluation Scenarios**
  - WP6 – Methodology & Application Rules

SAFE – WP 5
Evaluation Scenarios

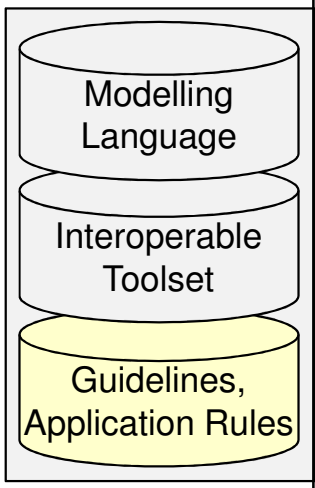


Content



- Work Packages
  - WP2 – Requirements Elicitation
  - WP3 – Model Based Development for Functional Safety
  - WP4 – Technology Platform
  - WP5 – Evaluation Scenarios
  - **WP6 – Methodology & Application Rules**

SAFE – WP 6
Methodology & Application Rules



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
- Project Organization
- Work Packages
- **Miscellaneous**

SAFE – Miscellaneous
Link to AUTOSAR

- AUTOSAR R4.0 includes safety mechanism and documentation report
- ISO26262 automotive functional safety published 2011

- SAFE provides to AUTOSAR
  - Set up **link to ISO26262** and engineering processes
  - Provide complete **overview on system level**
  - Complement **hardware description**

- SAFE evaluates AUTOSAR results for
  - **AUTOSAR platform configuration** for safety application
  - Safety test **conformance** for component
  - **Process** compliance with safety standard

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.