Safe Automotive software architecture (SAFE) Project Presentation

SAFE project partners
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
<table>
<thead>
<tr>
<th>SAFE – Motivation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scope and Goals</td>
</tr>
</tbody>
</table>

### 1. Vocabulary
- Overall safety management
- Safety management during item development
- Safety management after release for production

### 2. Management of functional safety
- Initiation of product development at the system level
- Specification of the technical safety requirements
- System design
- Item integration and testing
- Release for production
- Functional safety assessment
- Safety validation

### 3. Concept phase
- Item definition
- Initiation of the safety lifecycle
- Hazard analysis and risk assessment
- Functional safety concept

### 4. Product development: system level
- Initiation of product development at the hardware level
- Specification of hardware safety requirements
- Hardware design
- Hardware architectural metrics
- Evaluation of violation of the safety goal due to random HW failures
- Hardware integration and testing
- Release for production
- Software verification

### 5. Product development: hardware level
- Initiation of product development at the hardware level
- Specification of hardware safety requirements
- Hardware design
- Hardware architectural metrics
- Evaluation of violation of the safety goal due to random HW failures
- Hardware integration and testing

### 6. Product development: software level
- Initiation of product development at the software level
- Specification of software safety requirements
- Software architectural design
- Software unit design and implementation
- Software unit testing
- Software integration and testing
- Software verification

### 7. Production and operation
- Production
- Operation, service and decommissioning

### 8. Supporting processes
- Interfaces within distributed developments
- Overall management of safety requirements
- Configuration management
- Change management
- Verification
- Documentation
- Qualification of software tools
- Qualification of software components
- Qualification of hardware components
- Proven in use argument

### 9. ASIL-oriented and safety-oriented analyses
- Requirements decomposition with respect to ASIL tailoring
- Criteria for coexistence of ASIL
- Analysis of dependent failures
- Safety analyses

### 10. (Informative) Guidelines on ISO 26262
SAFE – Motivation
Project Vision

ISO26262

SAFE

Developer

Requirements
Seamless tool-supported development

Modelling Language

Interoperable Toolset

Guidelines, Application Rules

3-7 Hazard analysis and risk assessment
3-7 Hazard analysis and risk assessment
Specification of safety goals
3-8 Functional safety concept
Specification of functional safety requirements
4-6 Specification of technical safety requirements
Specification of technical safety requirements
5-6 Specification of hardware safety requirements
6-6 Specification of software safety requirements

ITEA 2 ~ 10039
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
- **Integrated 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

<table>
<thead>
<tr>
<th>OEMs</th>
<th>Engineering Partner</th>
<th>Accreditation body</th>
</tr>
</thead>
<tbody>
<tr>
<td>BMW-CarIT (G)</td>
<td>AVL Software &amp; Function (G)</td>
<td>TÜV NORD Mobilität (G)</td>
</tr>
</tbody>
</table>

### Tiers 1

<table>
<thead>
<tr>
<th></th>
<th>Silicon Supplier</th>
<th>Academia</th>
</tr>
</thead>
<tbody>
<tr>
<td>Continental Automotive (G)</td>
<td>Infineon Technologies (G)</td>
<td>Fortiss (G)</td>
</tr>
<tr>
<td>Continental Automotive (Fr)</td>
<td></td>
<td>FZI, Karlsruhe University (Ge)</td>
</tr>
<tr>
<td>Continental Teves (G)</td>
<td></td>
<td>OFFIS (Ge)</td>
</tr>
<tr>
<td>Valeo EEM (Fr)</td>
<td></td>
<td>LaBRi, Bordeaux University (Fr)</td>
</tr>
<tr>
<td>ZF (G)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Tool suppliers & SME

- Aquintos (G)
- Dassault Systemes (Fr)
- ITEMIS France (Fr)
- Pure Systems (G)
- TTTEch (Aut)
SAFE – Project Organization
Work-Package Structure

**WP1**: Project Management, Exploitation

**WP2**: Requirement Elicitation

**WP3**: Model Based Development for Functional Safety
   - Modelling Language

**WP4**: Technology Platform
   - Interoperable Toolset

**WP6**: Methodology & Application Rules
   - Guidelines, Application Rules

**WP5**: Evaluation Scenarios

**WP7**: Training, Dissemination
SAFE – Project Organization

Milestones

Requirements

MS1 (04.12)

Meta model and method definition

MS2 (06.12)

Development of tool

M3 (09.12)

Evaluation

MS4 (12.12)

Meta model and method definition

MS5 (02.13)

Development of tool support

MS6 (07.13)

Evaluation

MS7 (12.13)

Development of tool

MS8 (02.14)

Evaluation

MS9 (04.14)

Development of tool

MS10 (06.14)

Platforms

Platform v1

Platform v2

Platform v3

ITEA 2 ~ 10039
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

- **WP2 – Requirements Elicitation**
- **WP3 – Model Based Development for Functional Safety**
- **WP4 – Technology Platform**
- **WP5 – Evaluation Scenarios**
- **WP6 – Methodology & Application Rules**
- **WP7: Training, Dissemination**
SAFE – WP 2
Requirements Elicitation

ISO26262
Requirements on model based development

State of the art
Parallel projects to cooperate with

Use Cases
Exemplarily industrial use cases

Filter: Project Targets

SAFE Project Requirements

> 500 requirements

> 60 requirements
Content

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

WP1: Project Management, Exploitation
- WP3: Model Based Development for Functional Safety
  - Modelling Language
- WP4: Technology Platform
  - Interoperable Toolset
- WP6: Methodology & Application Rules
  - Guidelines, Application Rules

WP7: Training, Dissemination
SAFE – WP 3
Model based dev. for Functional Safety

Safety goals modelling
- Hazard analysis, safety goals and ASIL def.
- Safety Requirement Expression
- Safety case documentation

Architecture modelling
- System and Software models enhancement
- Hardware Description
- COTS evaluation

Methods for analysis
- Failure and cut-sets analysis
- Safety evaluation
- Safety and multi-criteria architecture benchmarking

Variant Management

Safety code generation

Implemented in Meta Model Definition

Approach: base technologies are used and extended
- ReqIF
- EAST-ADL
- AUTOSAR
- IP-XACT

Modelling Language
Interoperable Toolset
Guidelines, Application Rules
SAFE – WP 3
Meta-model integration approach

- Process
- Requirements
- Hazards
- Analysis

- Validation
- Dysfunctional

- System
- Hardware
- References

- Configuration
- Software

- Initial release
- Intermediary release
- Final release
SAFE – WP 3
Use meta-model backbone for SAFE

SAFE Technology Platform

- MM: SAFE project
- Toolplatform: SAFE project & Eclipse A-IWG

USES

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

USES
• Work Packages
  – WP2 – Requirements Elicitation
  – WP3 – Model Based Development for Functional Safety
  – **WP4 – Technology Platform**
  – WP5 – Evaluation Scenarios
  – WP6 – Methodology & Application Rules
  – WP7: Training, Dissemination
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

Metamodelling implementation
SAFE – WP 4
Technology Platform – Architectural View

SAFE Technology Platform

RMF (Req IF)
- Validation
- EAST-ADL Explorer
- EAST-ADL Meta Model Implementation
- Serialization
- Abstraction level M2M
- EAST-ADL Editor
- Tool Adapters

EATOP (EAST-ADL)

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

DSDP (IP-XACT)

SPHINX
- Navigator & Editor Sockets
- Validation Runtime Extensions
- Compare & Merge Integration
- M2x Integration

Eclipse
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

Project Targets

SAFE Requirements (WP2)

Requirements on WP 3/4/6

WP 3/4/6 results

Evaluated Scenarios (WP5)

Tier 1’s perspective (eGas & Electrical Brake)

Mixed criticality software layer

Definition of assessment criteria

Safety analysis of a system with MCU and MCAL

Loop safety analysis at high level

Safety code generation
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
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.