Safe Automotive software architecture (SAFE) Project Presentation

SAFE project partners
Content

• Motivation

• Concept Level

• Implementation Level

• Organization
SAFE – Motivation

Issues in Safety Analysis*

The coherency issue
- How do safety analysis results relate to the actual design?
- How can safety engineers keep track with ongoing evolutions 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?

*) Model-Based Safety Analysis - OFFIS 2006
PART 1 – The Project
Challenges

We base the entire development cycle around the model!

How to keep safety related aspects consistent?

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

Why not the safety analysis?

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
<table>
<thead>
<tr>
<th>Requirement</th>
<th>Function</th>
<th>Variability</th>
<th>Environment</th>
<th>Logical</th>
<th>Technical</th>
<th>Geometrical</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image1.png" alt="Image" /></td>
<td><img src="image2.png" alt="Image" /></td>
<td><img src="image3.png" alt="Image" /></td>
<td><img src="image4.png" alt="Image" /></td>
<td><img src="image5.png" alt="Image" /></td>
<td><img src="image6.png" alt="Image" /></td>
<td><img src="image7.png" alt="Image" /></td>
</tr>
<tr>
<td><img src="image8.png" alt="Image" /></td>
<td><img src="image9.png" alt="Image" /></td>
<td><img src="image10.png" alt="Image" /></td>
<td><img src="image11.png" alt="Image" /></td>
<td><img src="image12.png" alt="Image" /></td>
<td><img src="image13.png" alt="Image" /></td>
<td><img src="image14.png" alt="Image" /></td>
</tr>
<tr>
<td><img src="image15.png" alt="Image" /></td>
<td><img src="image16.png" alt="Image" /></td>
<td><img src="image17.png" alt="Image" /></td>
<td><img src="image18.png" alt="Image" /></td>
<td><img src="image19.png" alt="Image" /></td>
<td><img src="image20.png" alt="Image" /></td>
<td><img src="image21.png" alt="Image" /></td>
</tr>
<tr>
<td><img src="image22.png" alt="Image" /></td>
<td><img src="image23.png" alt="Image" /></td>
<td><img src="image24.png" alt="Image" /></td>
<td><img src="image25.png" alt="Image" /></td>
<td><img src="image26.png" alt="Image" /></td>
<td><img src="image27.png" alt="Image" /></td>
<td><img src="image28.png" alt="Image" /></td>
</tr>
</tbody>
</table>

**SAFE – Motivation**
**Model Based Development**
**Safety Analysis**
SAFE – Motivation
Additional perspective - ISO26262

Vehicle Development
System Development
Component Development

3-7 Hazard analysis and risk assessment
Hazard analysis and risk assessment

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
Hardware safety requirements

6-6 Specification of software safety requirements
Software safety requirements

Vehicle Level (Features)
System Level (Functional Blocks)
System Level (Architectural Blocks)
Component Level 1-2 (components)
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

<table>
<thead>
<tr>
<th>1. Vocabulary</th>
</tr>
</thead>
<tbody>
<tr>
<td>2-5 Overall safety management</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>2. Management of functional safety</th>
</tr>
</thead>
<tbody>
<tr>
<td>2-6 Safety management during item development</td>
</tr>
<tr>
<td>2-7 Safety management after release for production</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>3. Concept phase</th>
</tr>
</thead>
<tbody>
<tr>
<td>3-5 Initiation of product development at the software level</td>
</tr>
<tr>
<td>3-6 Specification of the technical safety requirements</td>
</tr>
<tr>
<td>3-7 Specification of the hardware safety requirements</td>
</tr>
<tr>
<td>3-8 System design</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>4. Product development: system level</th>
</tr>
</thead>
<tbody>
<tr>
<td>4-5 Initiation of product development at the system level</td>
</tr>
<tr>
<td>4-6 Specification of the technical safety requirements</td>
</tr>
<tr>
<td>4-7 System design</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>5. Product development: hardware level</th>
</tr>
</thead>
<tbody>
<tr>
<td>5-5 Initiation of product development at the hardware level</td>
</tr>
<tr>
<td>5-6 Specification of hardware safety requirements</td>
</tr>
<tr>
<td>5-7 Hardware design</td>
</tr>
<tr>
<td>5-8 Hardware architectural metrics</td>
</tr>
<tr>
<td>5-9 Evaluation of violation of the safety goal due to random HW failures</td>
</tr>
<tr>
<td>5-10 Hardware integration and testing</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>6. Product development: software level</th>
</tr>
</thead>
<tbody>
<tr>
<td>6-5 Initiation of product development at the software level</td>
</tr>
<tr>
<td>6-6 Specification of software safety requirements</td>
</tr>
<tr>
<td>6-7 Software architectural design</td>
</tr>
<tr>
<td>6-8 Software unit design and implementation</td>
</tr>
<tr>
<td>6-9 Software unit testing</td>
</tr>
<tr>
<td>6-10 Software integration and testing</td>
</tr>
<tr>
<td>6-11 Software verification</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>7. Production and operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>7-5 Production</td>
</tr>
<tr>
<td>7-6 Operation, service and decommissioning</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>8. Supporting processes</th>
</tr>
</thead>
<tbody>
<tr>
<td>8-5 Interfaces within distributed developments</td>
</tr>
<tr>
<td>8-6 Overall management of safety requirements</td>
</tr>
<tr>
<td>8-7 Configuration management</td>
</tr>
<tr>
<td>8-8 Change management</td>
</tr>
<tr>
<td>8-9 Verification</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>9. ASIL-oriented and safety-oriented analyses</th>
</tr>
</thead>
<tbody>
<tr>
<td>9-5 Requirements decomposition with respect to ASIL tailoring</td>
</tr>
<tr>
<td>9-6 Criteria for coexistence of</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>10. (Informative) Guidelines on ISO 26262</th>
</tr>
</thead>
</table>
SAFE – Motivation

Approach

ISO26262

3-7 Hazard analysis and risk assessment

3-8 Functional safety concept

4-6 Specification of technical safety requirements

Modeling Language

Interoperable Toolset

Guidelines, Application Rules

Requirements

Seamless tool-supported development

HW-SW Component Models

ISO

SAFE

Developer

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

Hazard analysis and risk assessment

Functional safety concept

Specification of technical safety requirements

Specification of hardware safety requirements

Specification of software safety requirements
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

Competitive 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

**Approach:** existing, base technologies are used and extended
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 – Safety Goal Modeling

Item Definition

Hazard

Hazardous Event

Operational Situation

Safety Goal

ASIL
A B C D
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 - Functional safety concept
Safety Goal
ASIL
A B C D
Safe State
Functional Safety Requirement
Functional Architecture Item
SAFE – Concept Level
Technical 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 technical safety requirements and their allocation to system elements for implementation by the system design.
SAFE – Concept Level
HW-SW Safety concept

ISO26262

3-7 Hazard analysis and risk assessment

3-8 Functional safety concept

4-6 Specification of technical safety requirements

SAFE – Architecture modeling

Technical Safety Requirement → Technical Architecture Item

HW Safety Requirement → HW – SW Interface Specification

HW Architecture Item

SW Safety Requirement → SW Architecture Item

HW

SW
SAFE – Concept Level

Summary: Safety Requirement Expression

- Safety Goals
- Functional Safety Requirements
- Technical Safety Requirements
- HW/SW Safety Requirements

- Functional analysis at vehicle level
  - Hazard analysis and risk assessment

- System design & Architecture
  - Functional safety concept

- Component design & Architecture
  - Technical safety concept

- HW/SW
  - HW/SW safety concept

Modeling Language
Interoperable Toolset
Guidelines, Application Rules
SAFE – Concept Level
Meta-model integration approach

- Process
  - Validation
    - Requirements
    - Hazards
    - Dysfunctional
    - Analysis
  - References

- System
  - Hardware
  - Software
  - Configuration

- References

- Initial release
  - 30.06.2012
- Intermediary release
  - 30.04.2013
- Final release
  - 28.02.2014
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

SAFE Meta-Model Implementation

Tool Interfacing
- Autofocus (Fortiss)
- CATIA V6 (Dassault Systèmes)
- HeRaClea (OFFIS)
- PREEvision (Vector)
- pure::variants (pure-systems)

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

Platform
- Software platform for mixed criticality

Software platform for mixed criticality

RMF (ReqIF modeling framework)

EATOP (EAST-ADL tool platform)

ARTOP (AUTOSAR tool platform)

Sphinx

Eclipse

Guidelines, Application Rules

Modelling Language

Interoperable Toolset

PREEvision (Vector)

Autofocus (Fortiss)

CATIA V6 (Dassault Systèmes)

HeRaClea (OFFIS)

pure::variants (pure-systems)
Content

• Motivation

• Concept Level

• Implementation Level
  – Technology Platform
  – Industrial use cases

• Organization
SAFE – Implementation Level
Evaluation Scenarios

- Project Targets
- SAFE Requirements (WP2)
- SAFE Requirements (WP2)
- Requirements on WP 3/4/6
- Evaluation Scenarios (WP5)
- WP 3/4/6 results
- 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

Requirements on WP 3/4/6

WP 3/4/6 results
Content

• Motivation

• Concept Level

• Implementation Level

• Organization
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

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

**WP1:** Project Management, Exploitation

**WP2:** Requirement Elicitation

**WP3:** Model Based Development for Functional Safety

**WP4:** Technology Platform

**WP5:** Evaluation Scenarios

**WP6:** Methodology & Application Rules

**WP7:** Training, Dissemination
## PART 1 – The Project

### Results

<table>
<thead>
<tr>
<th>Concept Level</th>
<th>WP1</th>
<th>WP2</th>
<th>WP3</th>
<th>WP4</th>
<th>WP5</th>
<th>WP6</th>
<th>WP7</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Analysis ISO26262 requirements</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>▶️</td>
</tr>
<tr>
<td>Open meta-model</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>▶️</td>
</tr>
<tr>
<td>Assessment process</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>▶️</td>
</tr>
</tbody>
</table>

### Implementation Level

<table>
<thead>
<tr>
<th>Implementation Level</th>
<th>WP1</th>
<th>WP2</th>
<th>WP3</th>
<th>WP4</th>
<th>WP5</th>
<th>WP6</th>
<th>WP7</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Technology Platform</td>
<td></td>
<td></td>
<td></td>
<td>▶️</td>
<td></td>
<td></td>
<td></td>
<td>▶️</td>
</tr>
<tr>
<td>Industrial Use Case Evaluation</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>▶️</td>
<td></td>
<td></td>
<td>▶️</td>
</tr>
</tbody>
</table>

### Completive Material

<table>
<thead>
<tr>
<th>Completive Material</th>
<th>WP1</th>
<th>WP2</th>
<th>WP3</th>
<th>WP4</th>
<th>WP5</th>
<th>WP6</th>
<th>WP7</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Training Material</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>▶️</td>
<td></td>
<td>▶️</td>
</tr>
<tr>
<td>Recommendation and Guidelines</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>▶️</td>
<td>▶️</td>
</tr>
</tbody>
</table>
SAFE – Project Organization

**Milestones**

**Requirements**
- Meta model and method definition
  - Development of tool
  - Evaluation

**Loop 1**
- Platform v1
  - Meta model and method definition
  - Development of tool
  - Evaluation

**Loop 2**
- Platform v2
  - Meta model and method definition
  - Development of tool support

**Loop 3**
- Platform v3
  - Evaluation

**Milestones (Dates)**
- MS1 (04.12)
- MS2 (06.12)
- MS3 (09.12)
- MS4 (12.12)
- MS5 (02.13)
- MS6 (07.13)
- MS7 (12.13)
- MS8 (02.14)
- MS9 (04.14)
- MS10 (06.14)
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

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

SAFE – Safety Analysis

Model-Based Development

Software Architecture & Implementation

System Architecture

Functional Architecture

Feature Model

Hazard Analysis

Technical Safety Concept

Refined Technical Safety Concept

Satisfy authorities
satisfy customer

Customer Functions

- be cheap
- be available
- be comfortable
- do not pollute

BrakeActivated

Environment Situation

- hazardous event S
- hazard S = E
- derived from S

- HIGHWAY DRIVING
- Sudden Loss of Braking in Slope

- ASIL C
- exposure
- severity
- controllability

Vehicle Functions

- transport people
- ensure good feeling
- ensure low vibrations
- ensure low noise

- provide entertainment
- allow vehicle personalization

- provide navigation system

- provide air conditioning

Development Model

- provide interior place
- provide vehicle access

- authorize vehicle access
- provide practical access

- provide glass holder
- provide refrigerator

- emit visual signals
- emit acoustic signals

Safety Concept

- provide interior-exterior interfacing...
- emit signals to exterior

- ensure vehicle stability
- coordinate energy forms
- transmit energy

- ensure visibility

Function Flaw

- Brake Pedal shall not request below 40% of driver feeling
- Brake Pedal Sensors shall be independent
- Requirement Interval shall be at least 40ms

Technical Safety Concept

- Service Brake
- Safety Goal

- technical safety requirement

- derive req
- mechanism and includes safety

- derived from - based

- ASIL
- controllability

- architectural SW

- provision for certification

- ensure low lateral forces
- provide air conditioning
- ensure interior quality

- provide vehicle motion
- drive vehicle
- provide interior place
- provide vehicle access

- authorize vehicle access
- provide practical access

- provide glass holder
- provide refrigerator

- emit visual signals
- emit acoustic signals

- ensure visibility

- enhance visibility

- passively enhance driving
- actively enhance driving

- enhance visibility

- provide night vision

- provide blind corner view

- detect objects

- provide navigation system

- detect collision risk

- assist vehicle parking

- assist lane change

- detect lane departure

- detect crossing vehicle

- provide blind corner view

- detect objects

- provide night vision
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

ISO26262
- Requirements on model based development

State of the art
- Parallel projects to cooperate with

Use Cases
- Exemplarily industrial use cases

Filter: Project Targets
- > 500 requirements
- > 60 requirements

SAFE Project Requirements
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.