Safe Automotive software architecture (SAFE)

Co-summit 2015, 10-11 March 2015, Berlin - Germany
Dr. Stefan Vogt
Agenda

SAFE makes Functional safety safe

SAFE in the project landscape
SAFE and standardization
SAFE Motivation
Recalls for safety-related components

October 2013

- Toyota recalls 900,000 vehicles
- Constructional flaw

Water can leak from the air conditioning and drip on control modules for airbags, which can cause airbags to set off or lose their function.

October 2013

November 2013

July 2014

(Source: Vice Media Inc. 2014)
SAFE Motivation
Recalls for safety-related components

Fuse can melt, causing both lighting circuits to malfunction, leaving the car unlighted.

- November 2013
  - VW recalls 800.000 Tiguans
  - Possible dangerous safety fuse

October 2013    November 2013    July 2014

(Source: Vice Media Inc. 2014)
SAFE Motivation
Recalls for safety-related components

Danger of suddenly turning off, resulting in loosing most safety features while driving

- October 2013
- November 2013
- July 2014

- GM recalls 8.4 Mill. vehicles
- Faulty ignition switch

(Source: Vice Media Inc. 2014)
SAFE Motivation
Scope of SAFE - ISO26262 Development Lifecycle

Starting situation 2011

- Automotive Functional Safety norm published November 2011
- 1st mandatory interpretation of general standard IEC61508 for automotive industry
SAFE Motivation
Scope of SAFE - ISO26262 Development Lifecycle

Management and supporting processes

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

- Functional analysis
- System architecture
- Component architecture
- Hardware / Software

- Hazard & Risk Analysis
- Functional safety concept
- Technical safety concept
- HW/SW safety reqs.

- System Safety Analyses
- Component Safety Analyses
- HW/SW Safety Analyses
SAFE Motivation
Scope of SAFE - ISO26262 Development Lifecycle

- 900,000 vehicles
- Water can drip on control modules for airbags, which can cause airbags to set off

- 800,000 vehicles
- Fuse can melt, causing both lighting circuits to malfunction, leaving the car unlighted

- 8.4 Mill. vehicles
- Danger of suddenly turning off, resulting in loosing most safety features while driving

Concept: Hazard and risk analysis
Concept: Influence from other technologies
Concept: Failure propagation
SAFE Motivation
Scope of SAFE - ISO26262 Development Lifecycle

Challenge
- ISO26262 defines more than 1000 requirements
- Challenge for automotive industry:
  - Reach acceptable risk level by ensuring process compliance with ISO26262

Approach
- Provide model based development process that integrates functional-safety

Solution of SAFE
- Architecture description language
- Tools
- Methods and application Rules
SAFE Motivation
Scope of SAFE - ISO26262 Development Lifecycle

Challenge
- ISO26262 defines more than 1000 requirements
- Challenge for automotive industry:
  - Reach acceptable risk level by ensuring process compliance with ISO26262

Approach
- Provide model based development process that integrates functional-safety

Solution of SAFE
- Architecture description language
- Tools
- Methods and and application Rules
SAFE makes Functional safety safe

Agenda

SAFE motivation

SAFE in the project landscape

SAFE and standardization
SAFE in the project landscape
Who did it?

Start: 01.07.2011

France
Austria
Germany
SAFE in the project landscape
How did we work with others?

SAFE

Input from
Align with
Output to

Products & Standards
SAFE in the project landscape
How did we work with others?

Tooling
- EDONA
- CESAR

Safety
- SAFE

Timing
- TIMMO
- TIMMO2

ADL
- EAST-EEA
- ATESTT
- ATESTT2
- MAENAD

Industry Consortia
- AUTOSAR
- JASPAR

EAST-ADL Association

2001 2005 2010 2015

EAST-ADL EAST-ADL2 EAST-ADL 2.1 EAST-ADL 2.x
SAFE in the project landscape
How did we work with others?

* Source: SafeTRANS News (news.safetrans-de.org)
SAFE in the project landscape
How did we work with others?

Products
&
STANDARDS
SAFE makes Functional safety safe

SAFE in the project landscape

SAFE motivation

SAFE and standardization
SAFE and standardization
Influence of SAFE

Architecture Description Language
- AUTOSAR
  Industry standard for SW configuration
- EAST-ADL
  Industry standard for functional architecture

Tools
- ARTEMIS innovation Cluster on transportation

Requirements
- ISO
  ISO26262

Methodologies and application rules
- OMG
  Standardization group for SW engineering
SAFE and standardization
Summary

SAFE
Made first implementation of the standard
ISO 26262 published in 2011 → we started in 2011

SAFE
All partners had the same goal to ensure safety
Not only for Europe but for whole world

SAFE
Provided commercial tools and trainings to the market
Set standards

SAFE
Exploitation from a 1st Tier point of view

OEM
Supplier
Developer
Safety Expert
Thank you for your attention