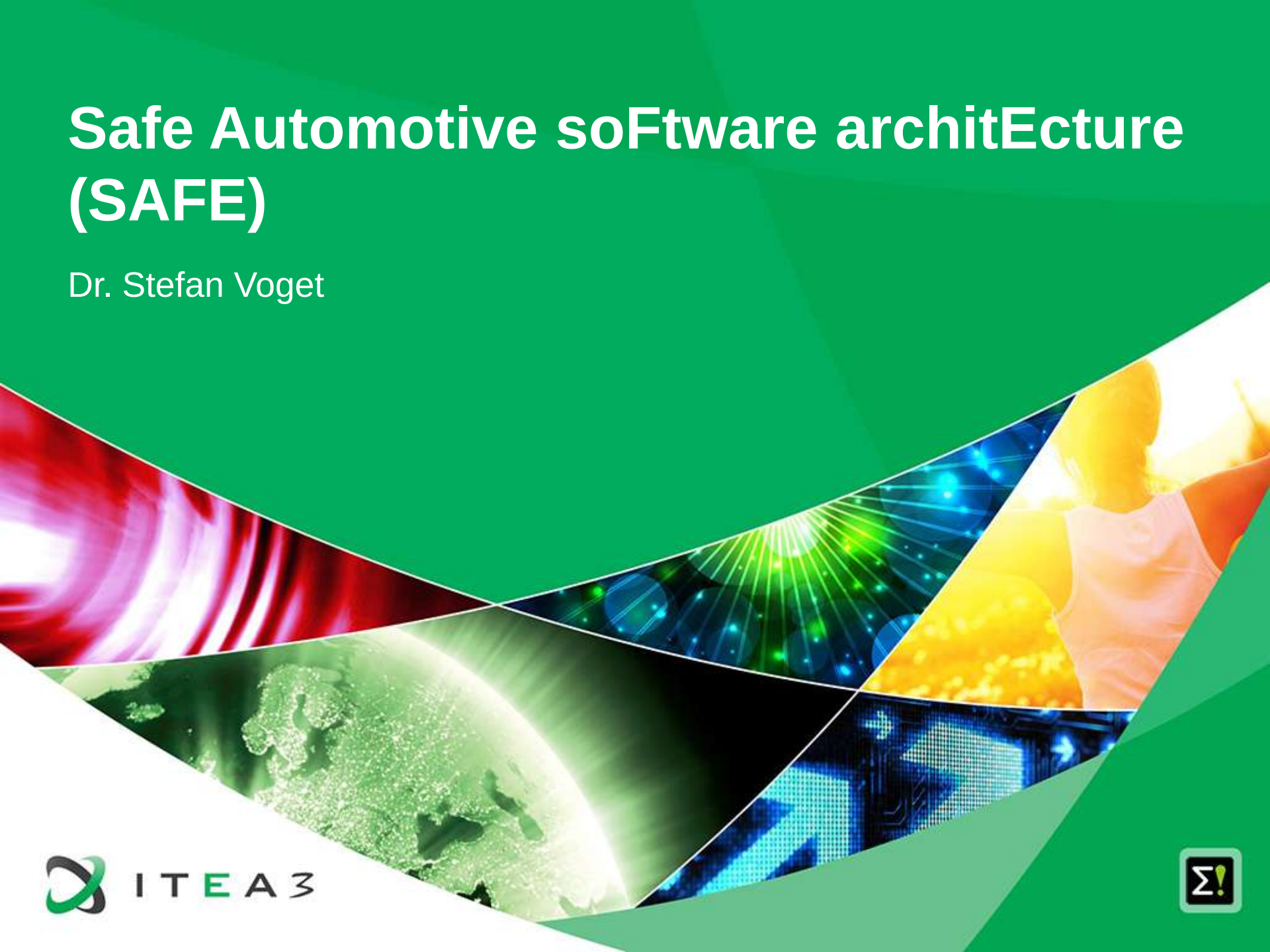
Safe Automotive soFtware architEcture (SAFE)

Dr. Stefan Voget



Agenda

SAFE

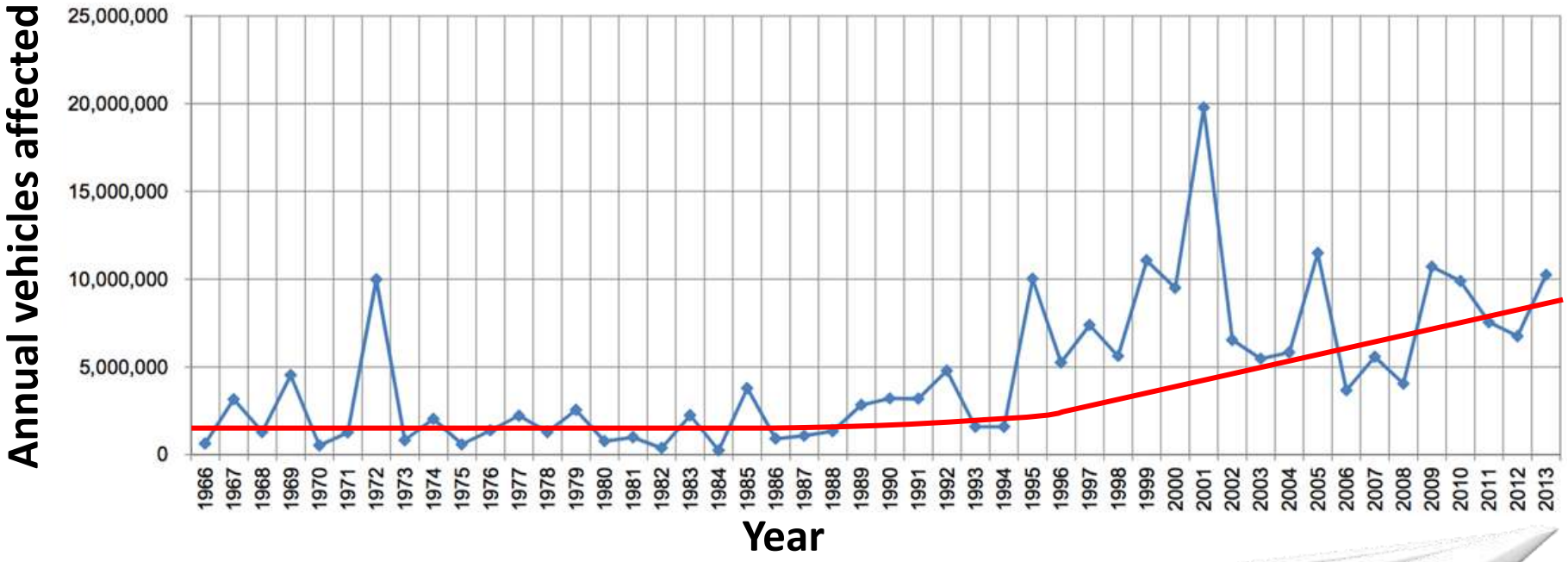
makes Functional safety safe

SAFE in the project landscape

SAFE modeling

Safe Motivation

Recalls for safety-related components

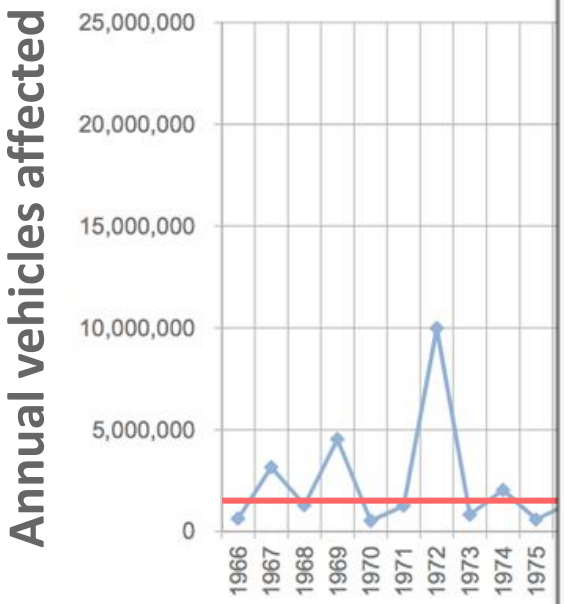


October 2013 | November 2013 | July 2014

(Source: Vice Media Inc. 2014)

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

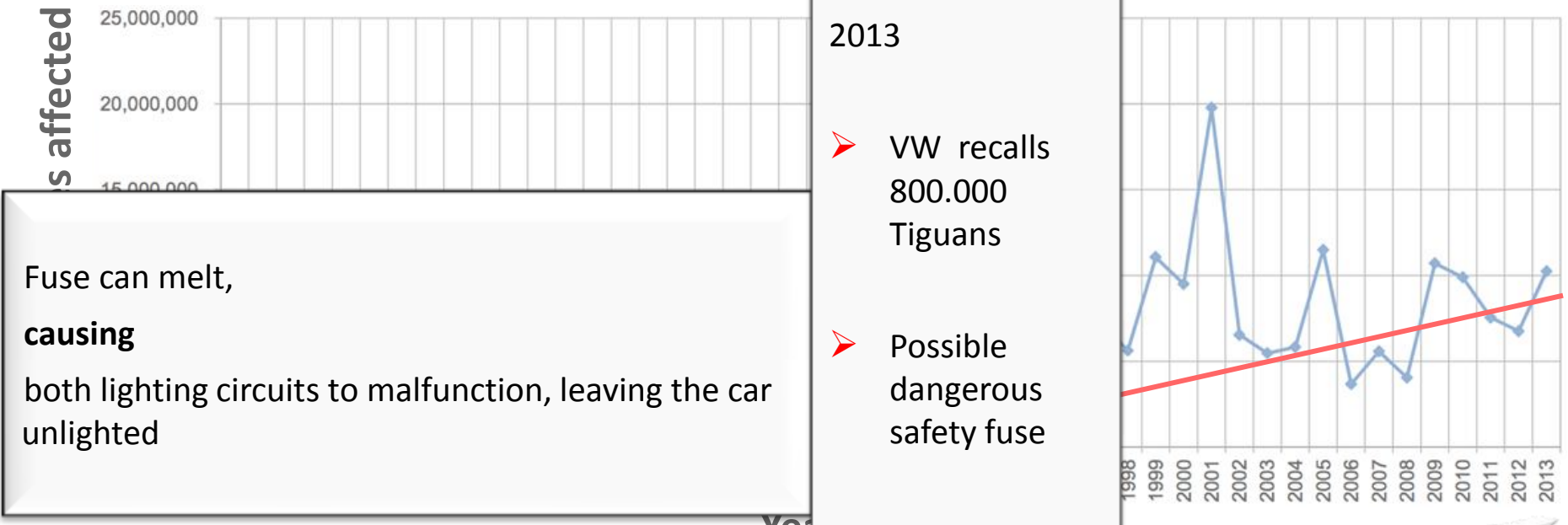
airbags to set off or lose their function

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

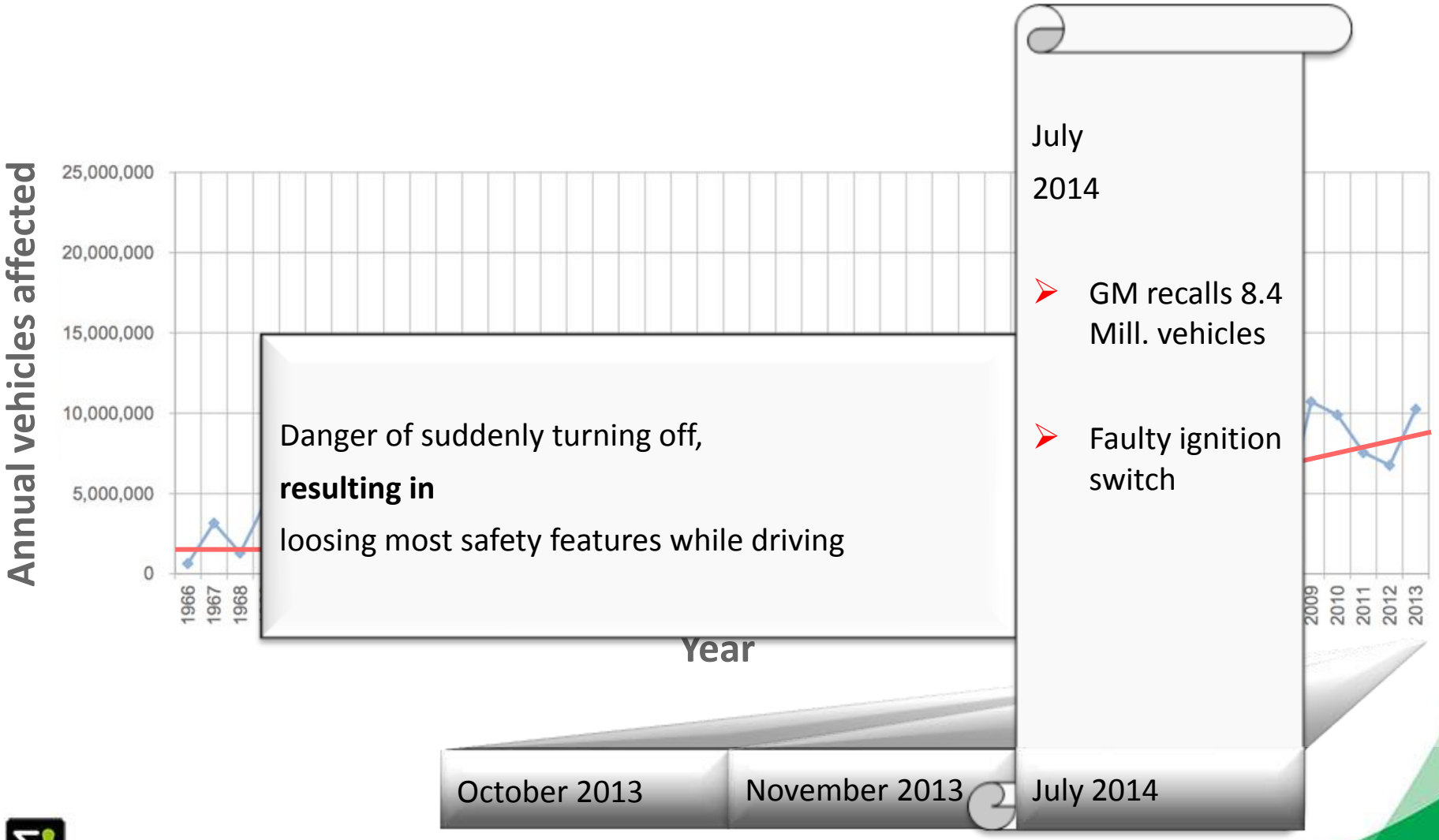
- VW recalls 800.000 Tiguans
- Possible dangerous safety fuse

October 2013 | November 2013 | July 2014

(Source: Vice Media Inc. 2014)

Safe Motivation

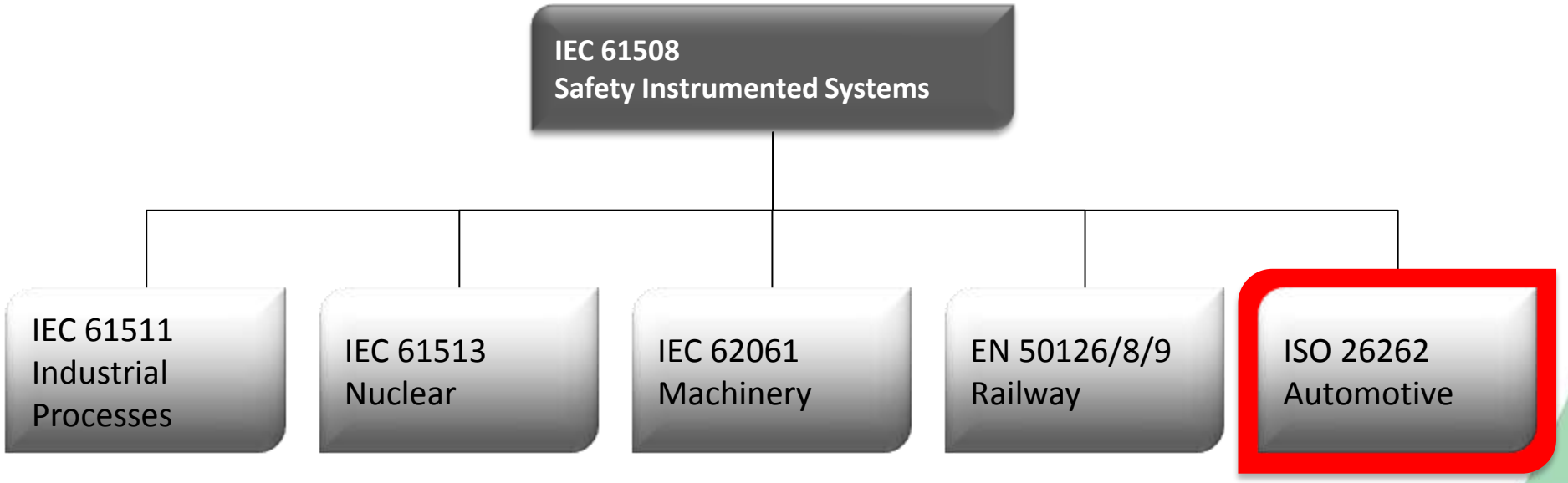
Recalls for safety-related components



(Source: Vice Media Inc. 2014)

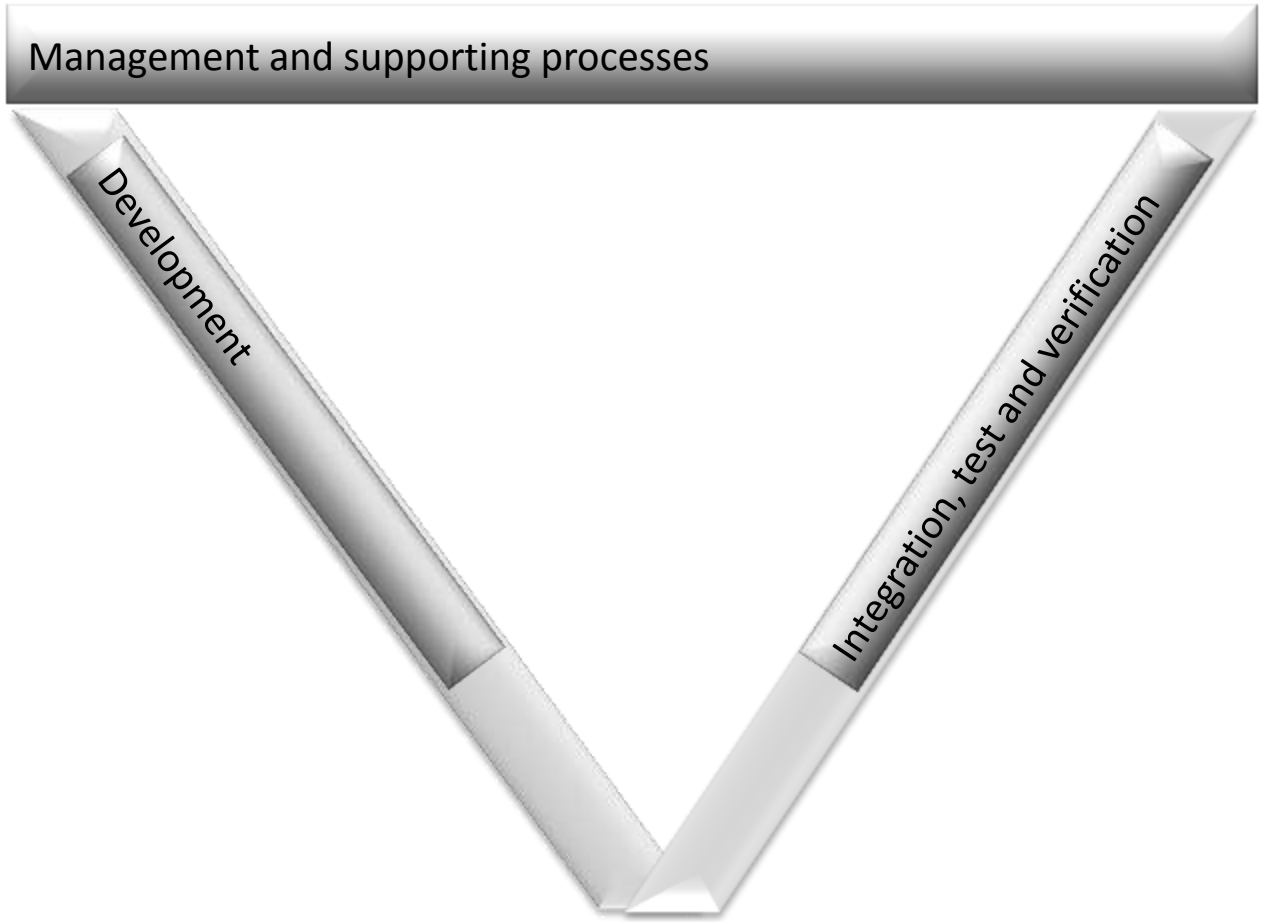
Safe Motivation
Starting point – 2011

- Automotive Functional Safety standard published November 2011
- 1st mandatory interpretation of general standard IEC61508 for automotive industry



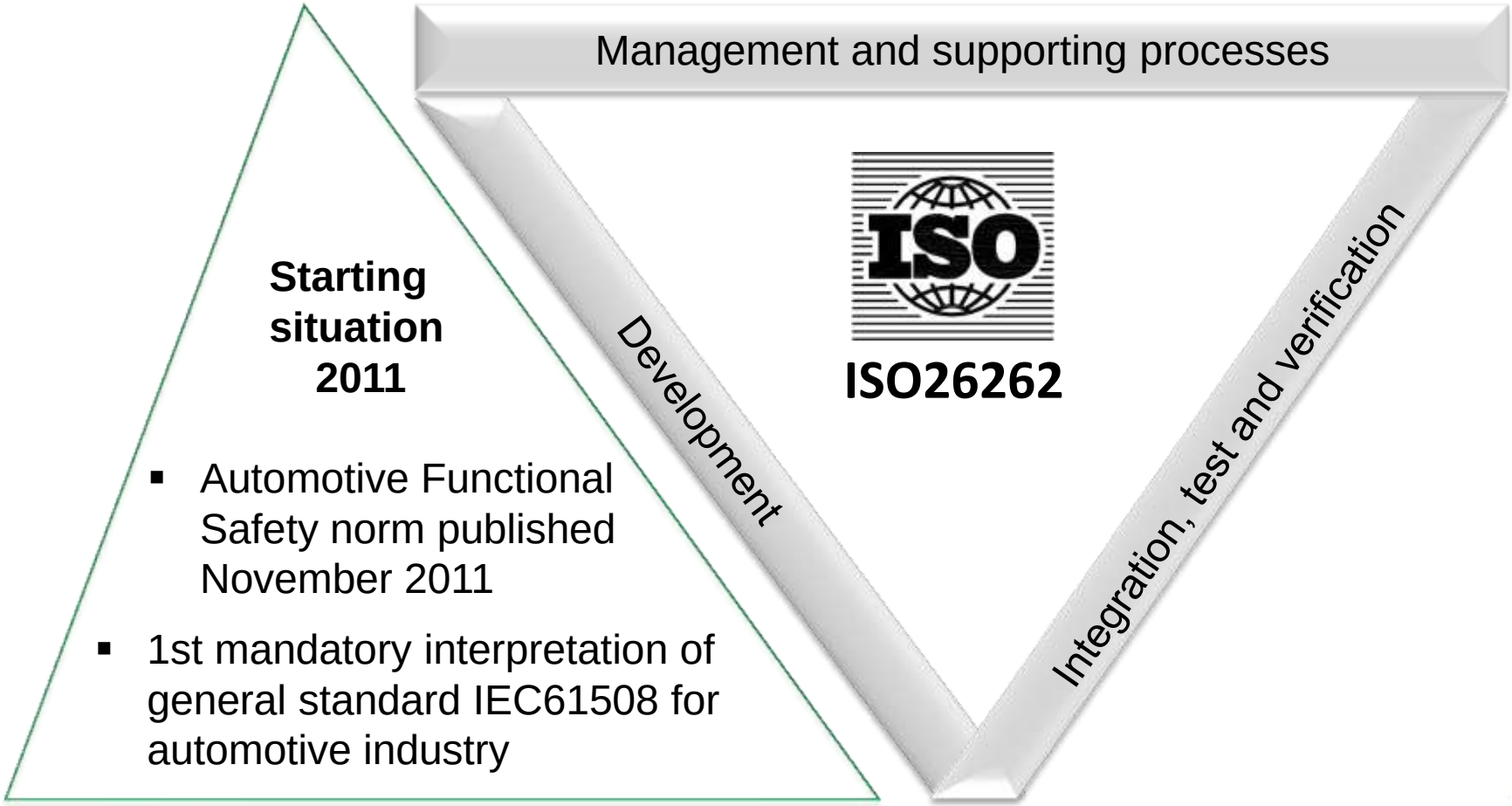
Safe Motivation

Scope of SAFE - ISO26262 Development Lifecycle



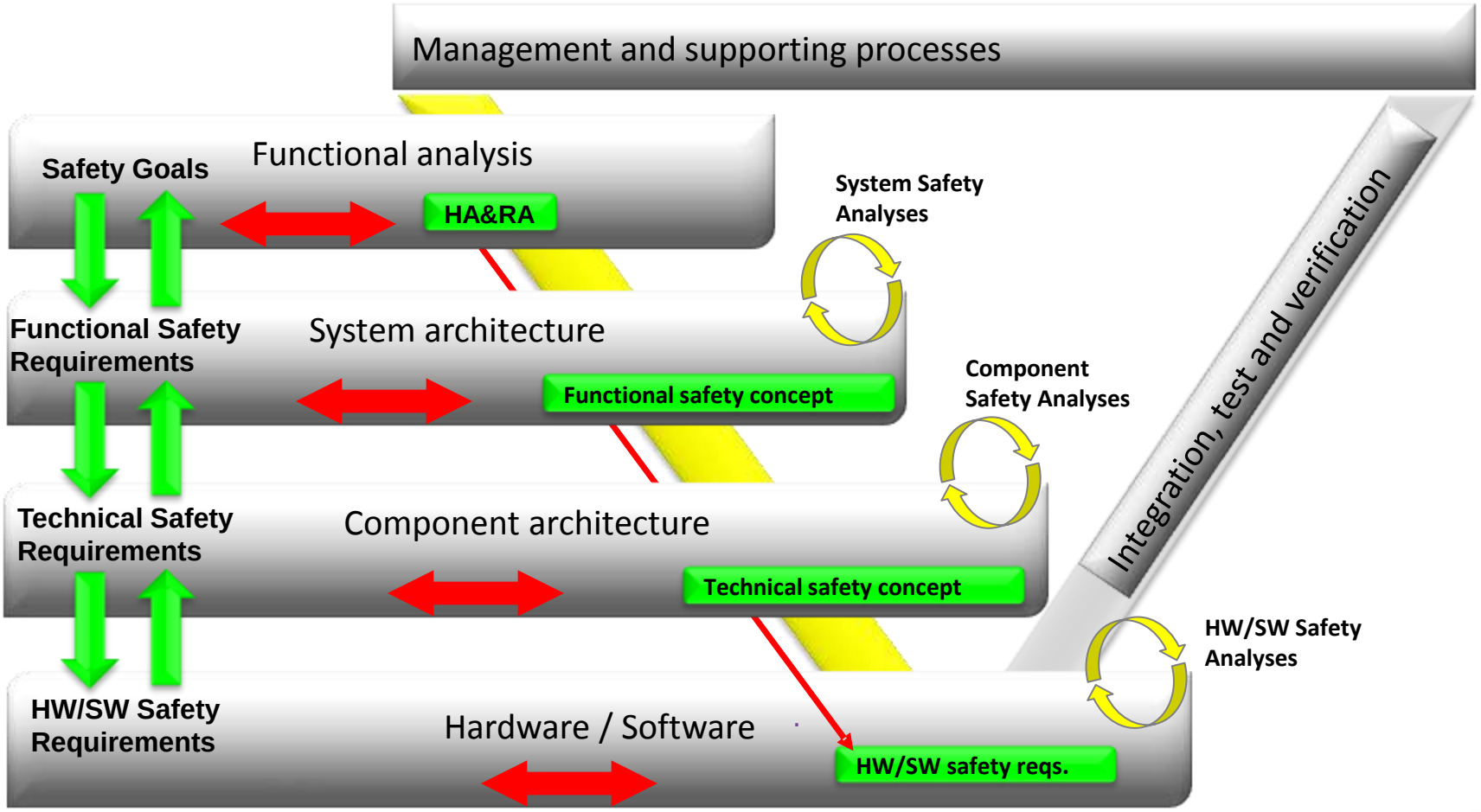
Safe Motivation

Scope of SAFE - ISO26262 Development Lifecycle



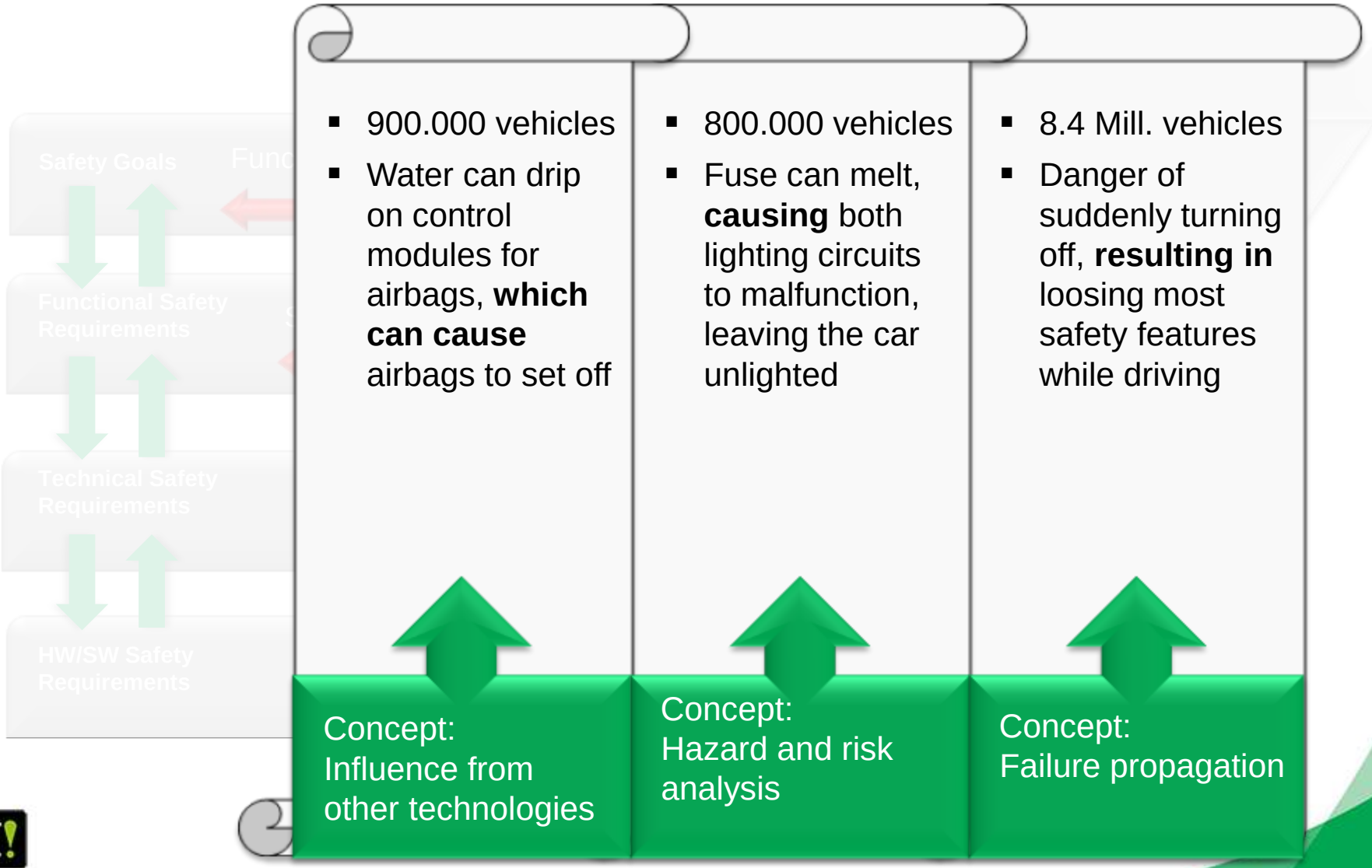
Safe Motivation

Scope of SAFE - ISO26262 Development Lifecycle



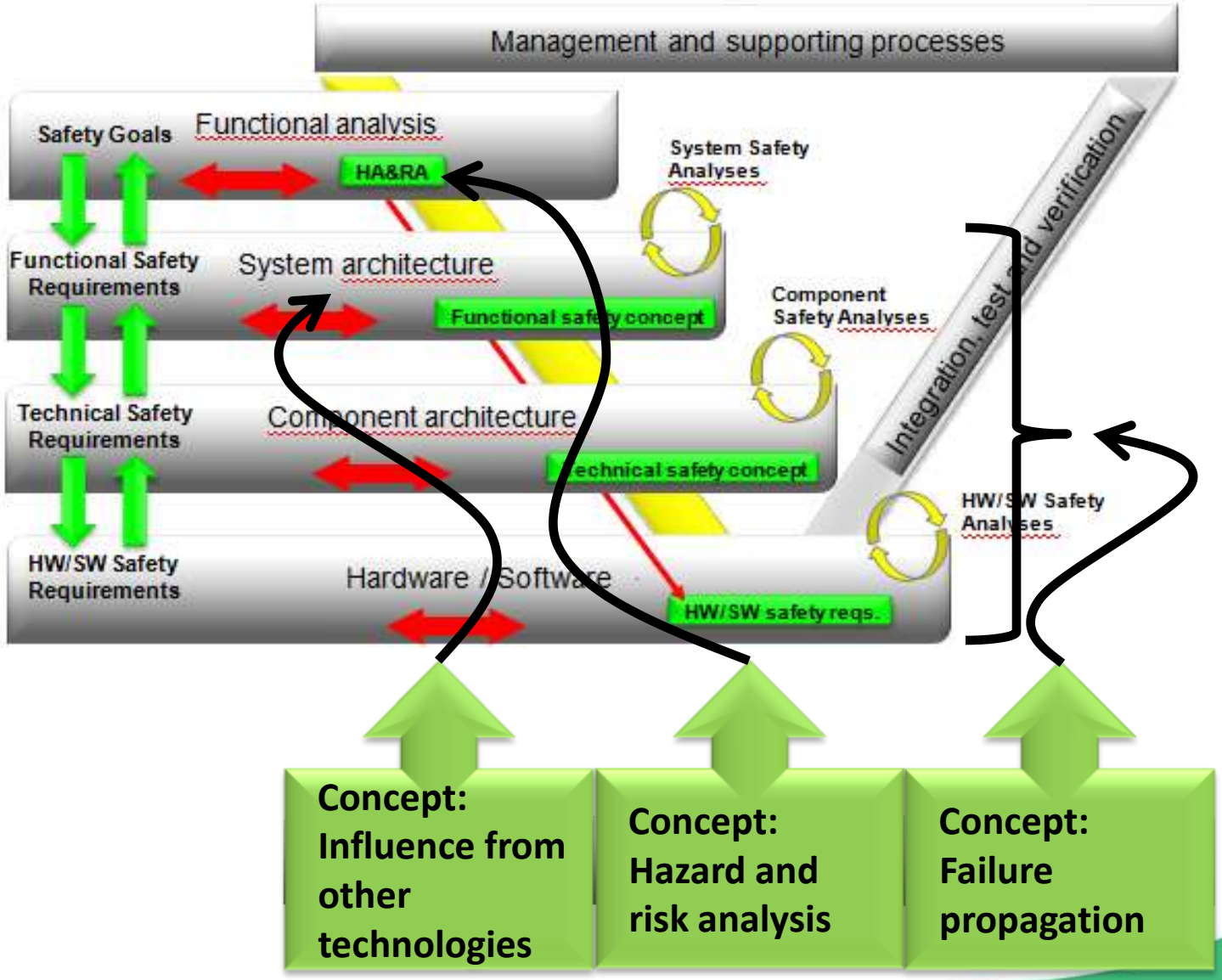
Safe Motivation

Scope of SAFE - ISO26262 Development Lifecycle



Safe Motivation

Recalls for safety-related components



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

Agenda

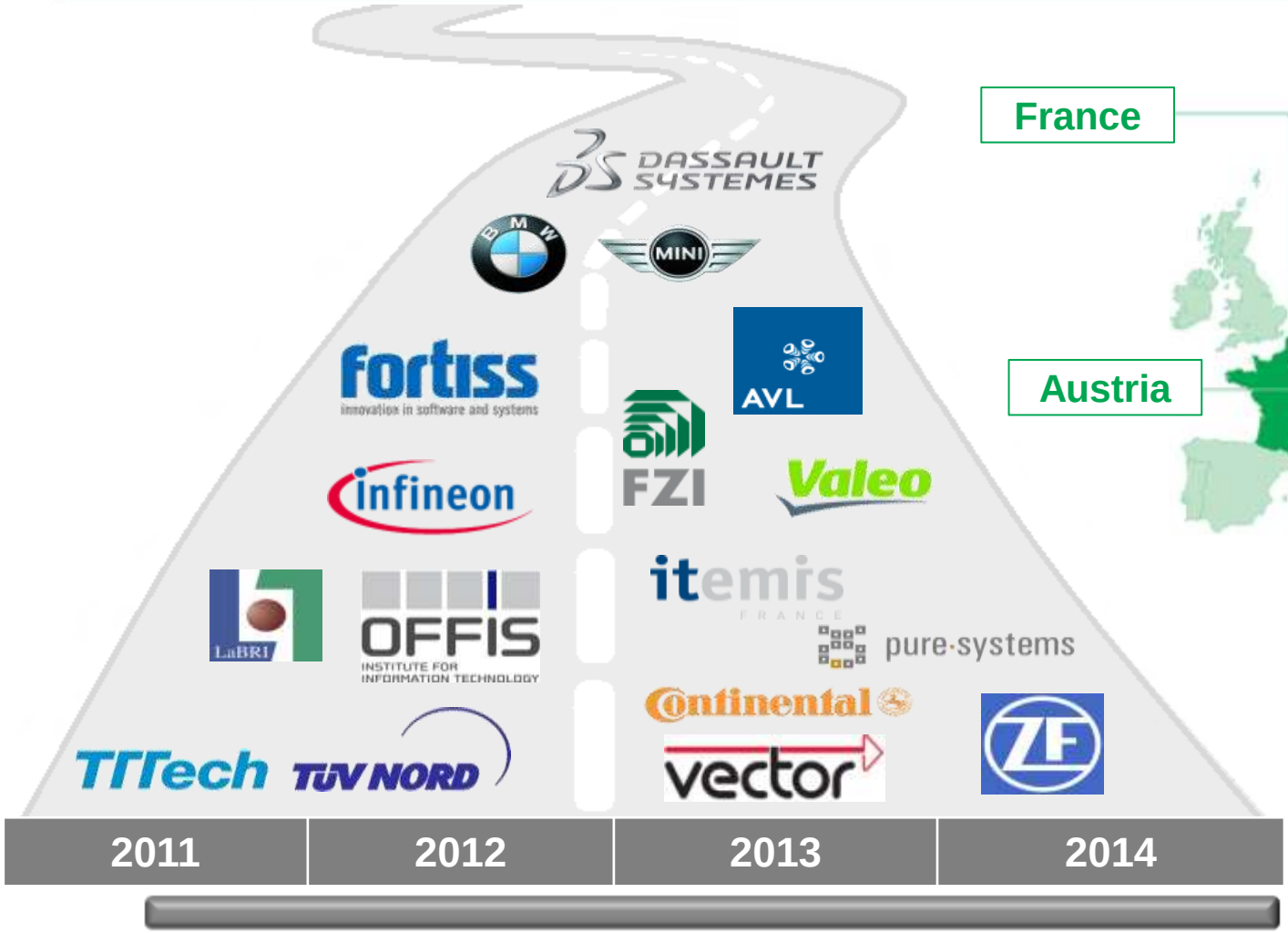
SAFE motivation

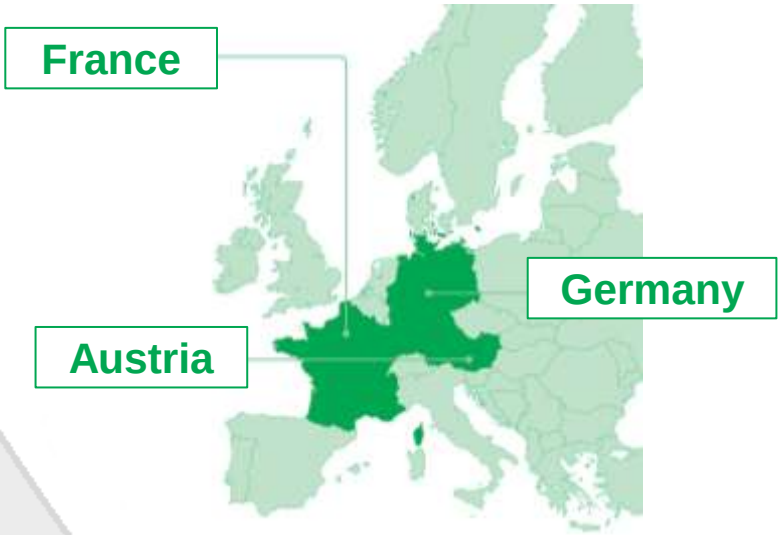
makes Functional safety safe

SAFE in the project landscape

SAFE modeling

SAFE in the project landscape
Who did it?



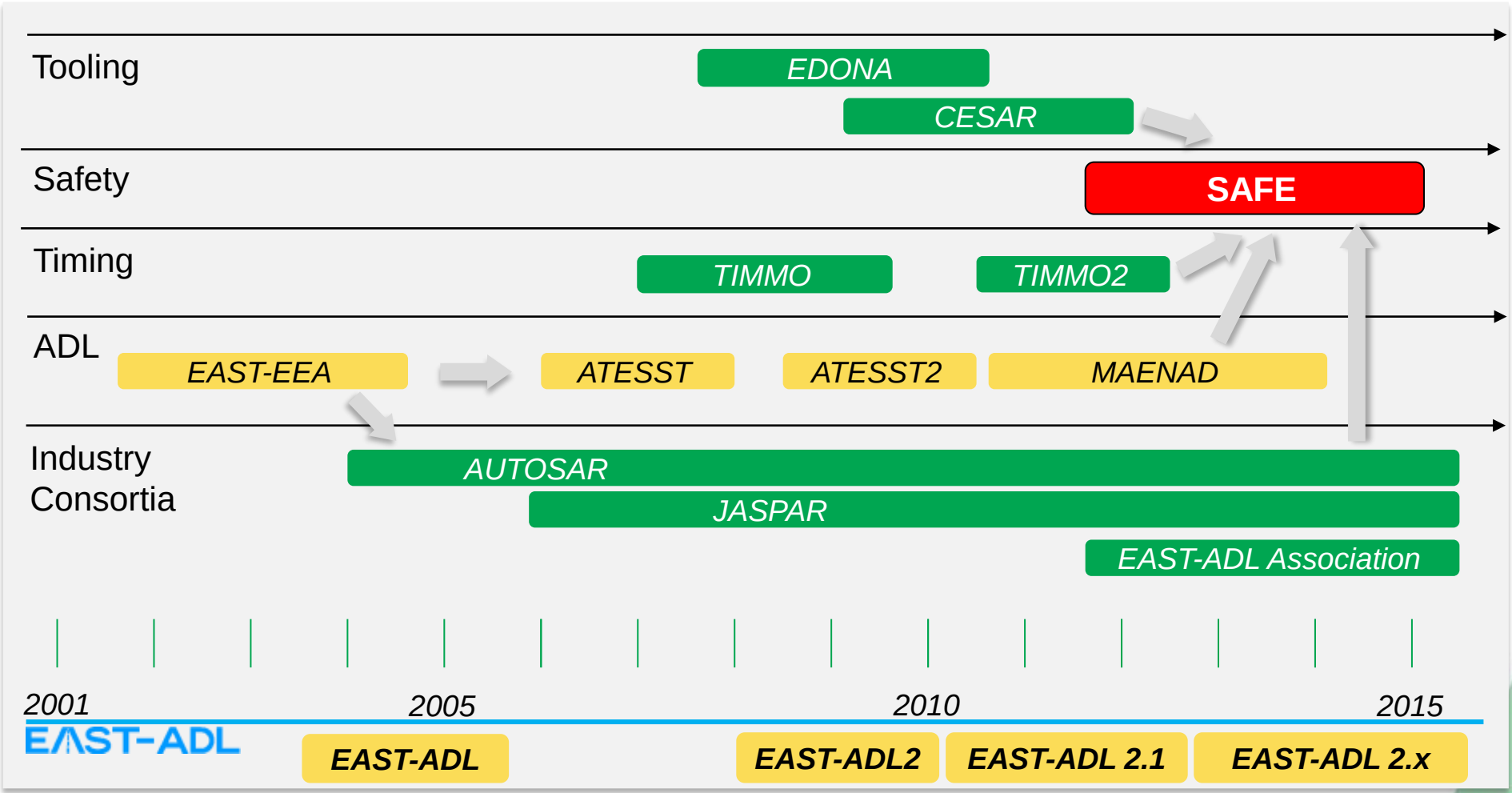


Start: 01.07.2011

End: 31.12.2014

SAFE in the project landscape

How did we work with others?



SAFE in the project landscape

Influence of SAFE

SAFE

Architecture Description Language

AUTOSAR

Industry standard for
SW configuration

EAST-ADL

Industry standard for
functional architecture

Tools

EICOSE

ARTEMIS innovation
Cluster on transportation

Requirements

ISO

ISO26262

Methodologies and application rules

OMG

Standardization group for
SW engineering

Agenda

SAFE motivation

makes Functional safety safe

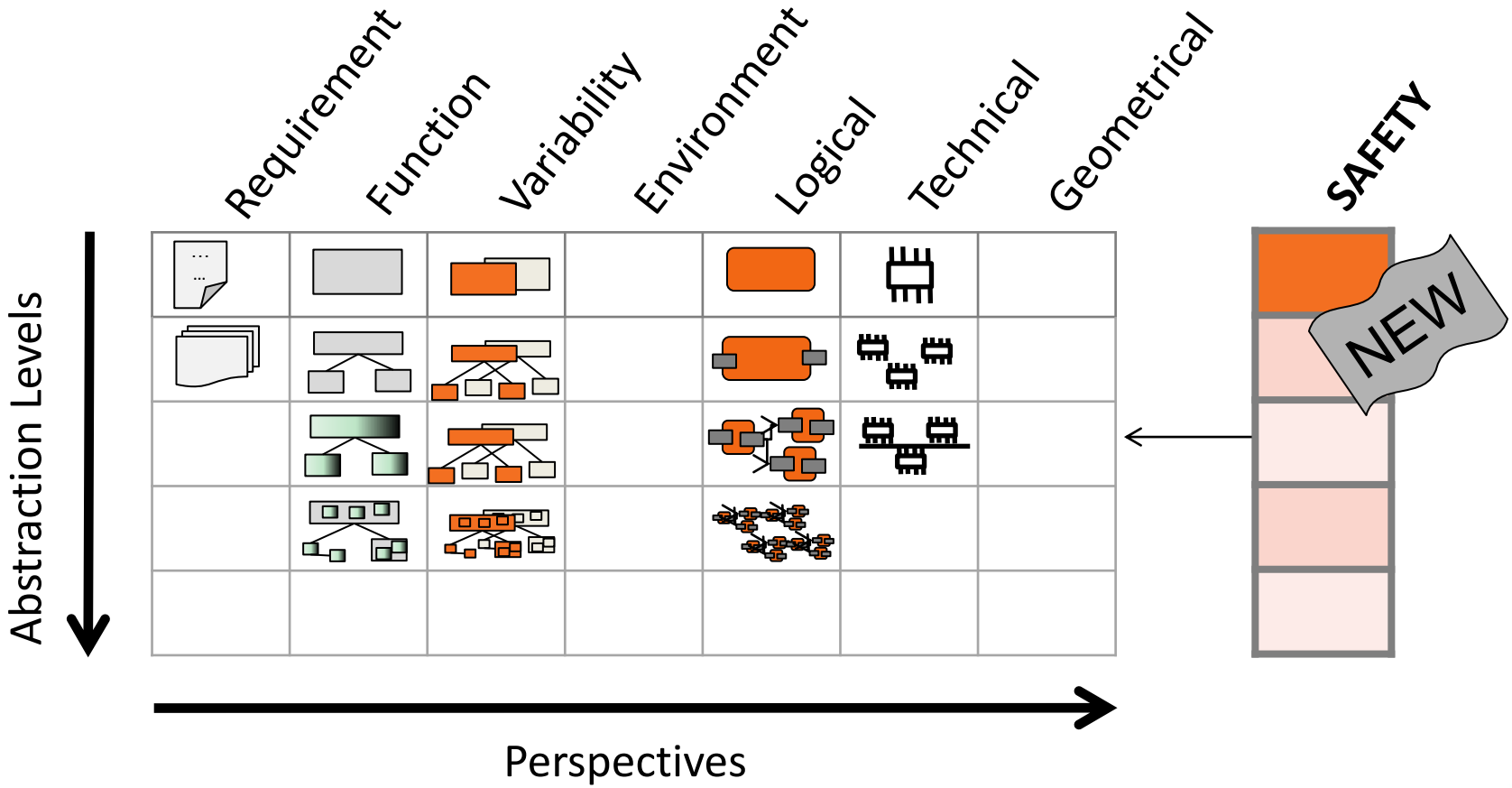
SAFE in the project landscape

SAFE modeling

Content

- **Open Meta-model**
  - **Scope**
  - Structure
  - Exemplified insight

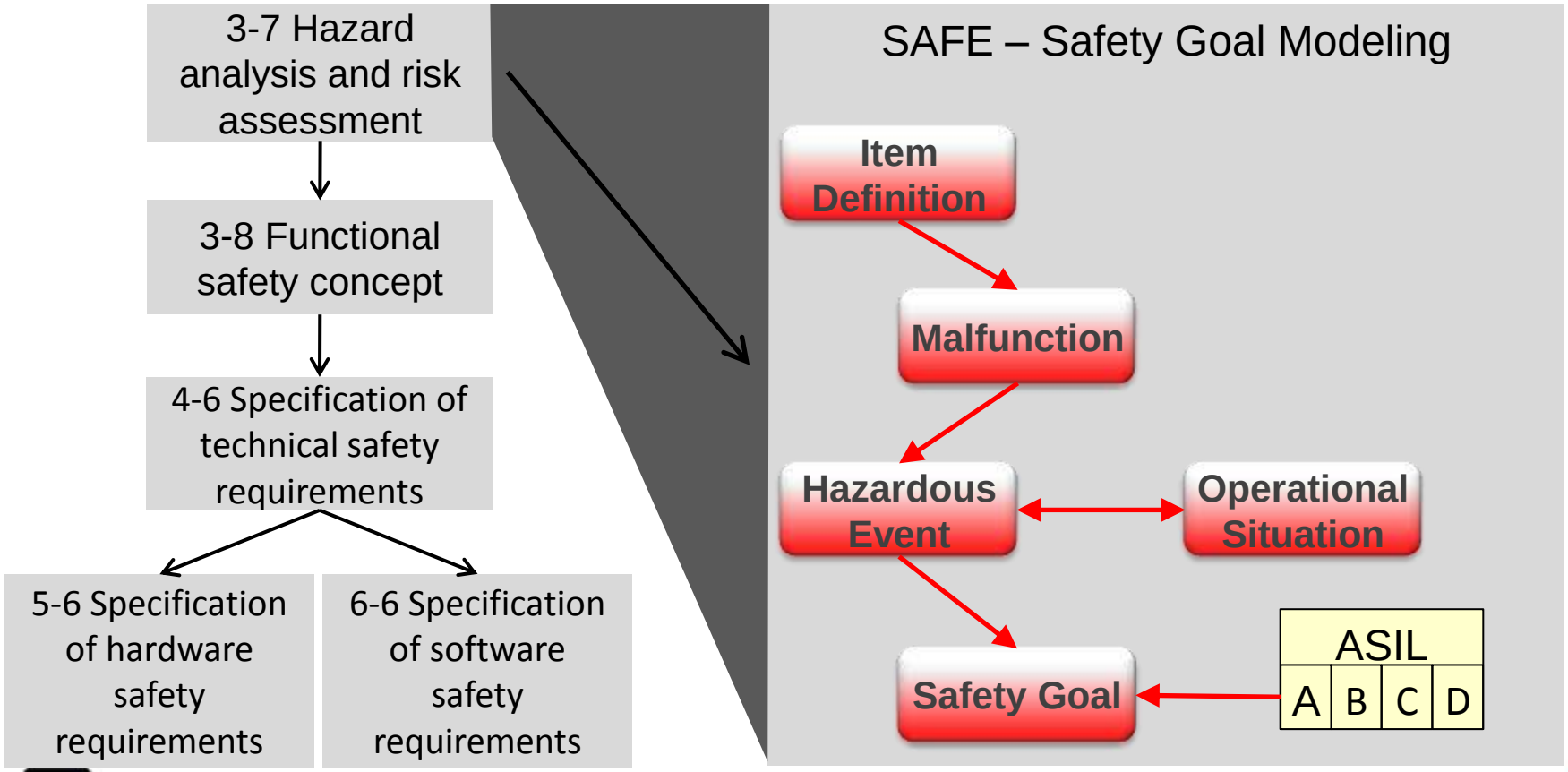
SAFE Modeling
Model Based Development



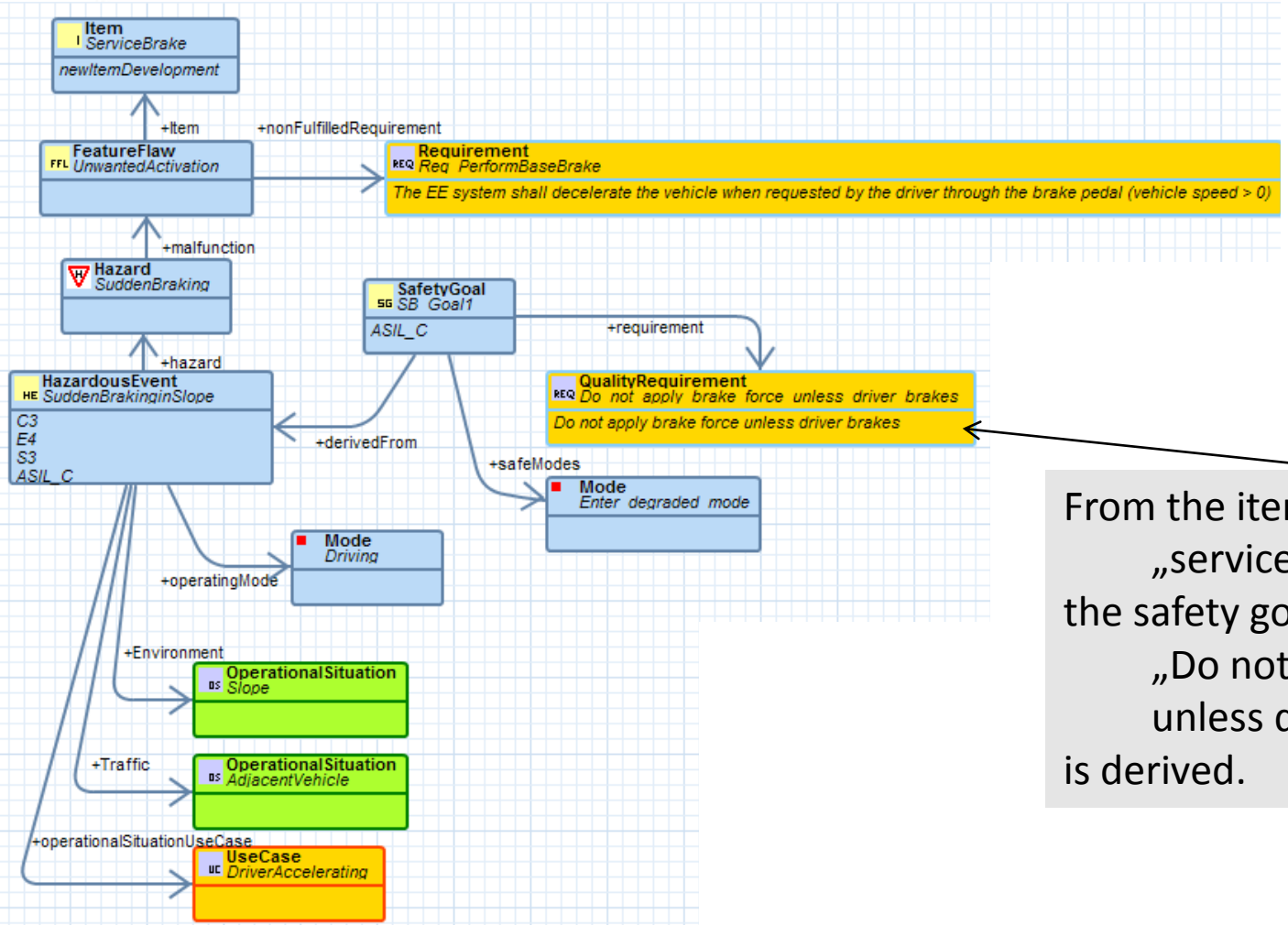
SAFE Modeling

Hazard analysis and risk assessment

ISO26262



SAFE Modeling
Hazard and Risk Analysis

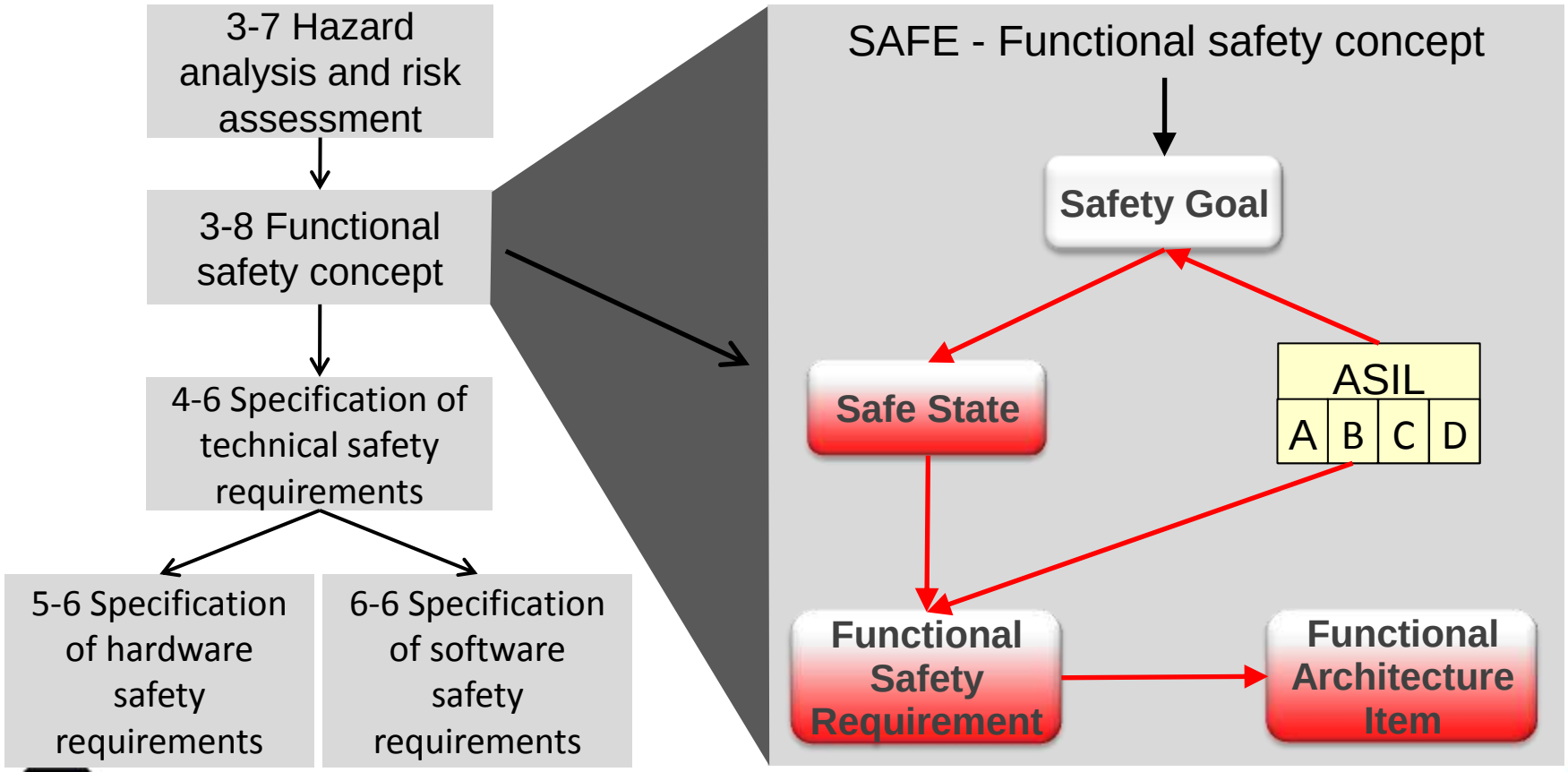


From the item
„service brake“
the safety goal
„Do not apply brake force unless driver brakes“
is derived.

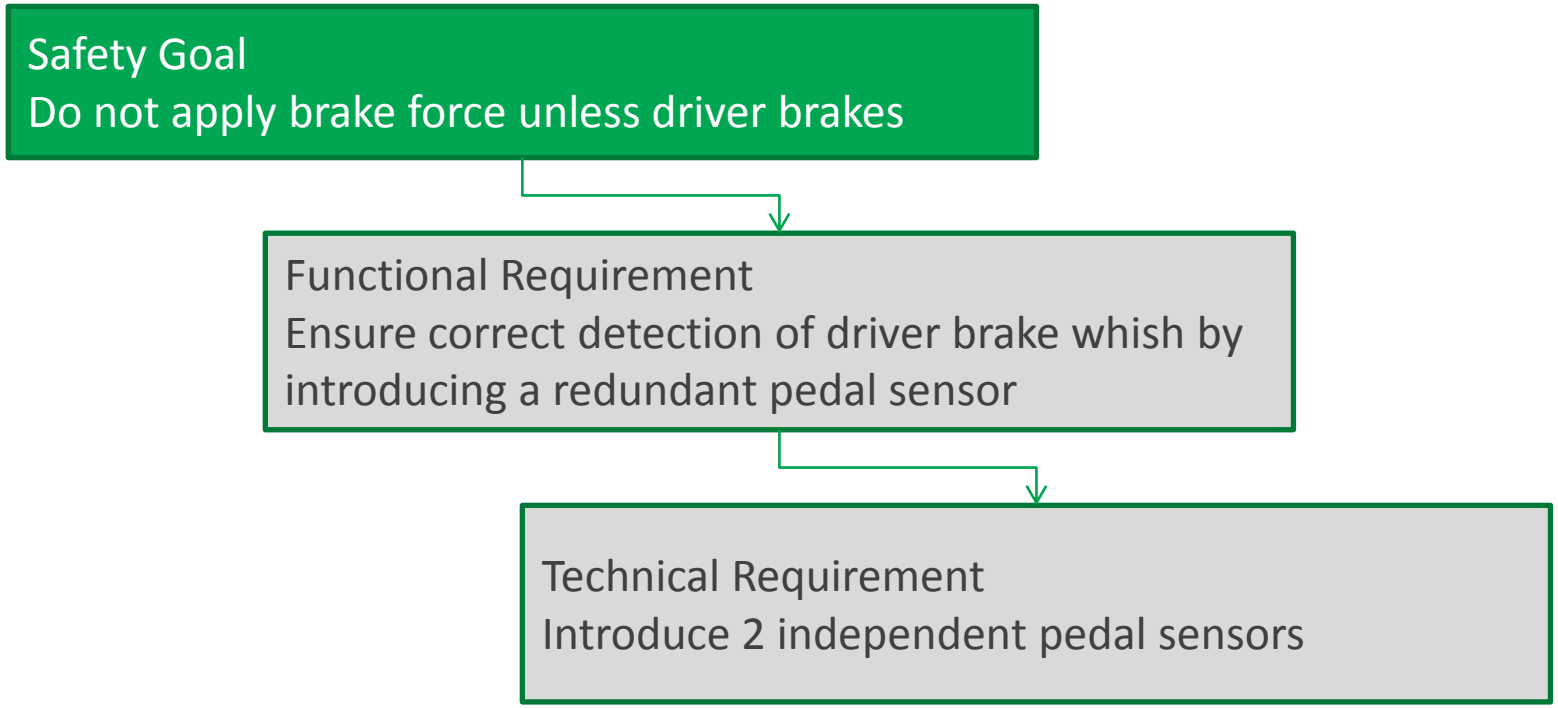
SAFE Modeling
Functional safety concept

ISO26262

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



SAFE Modeling
Derived safety requirements

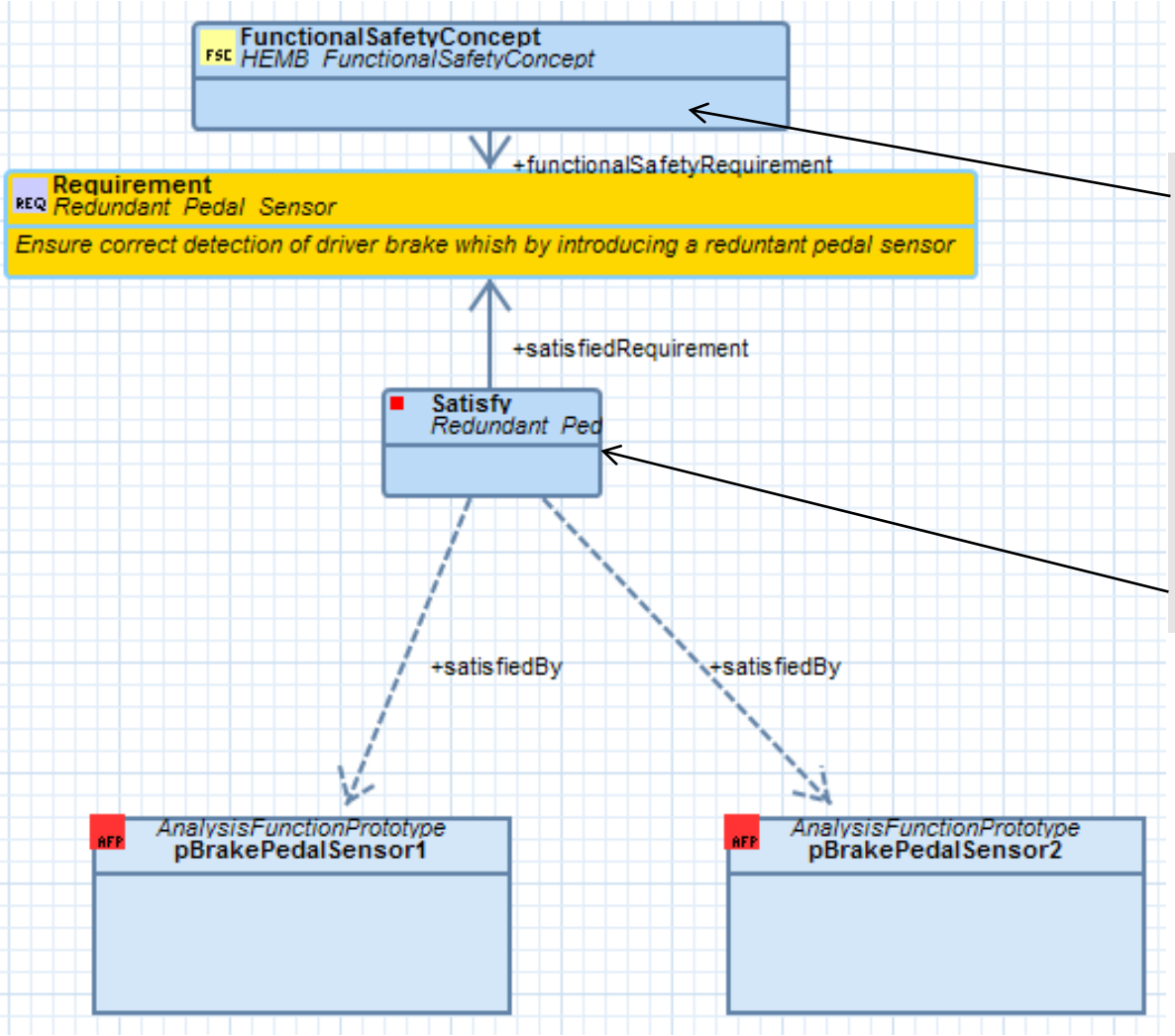


Safety goals are top level safety requirements.

They are derived by safety requirements on analysis level.

These analysis level safety requirements are derived by safety requirements on design level.

SAFE Modeling
Functional Safety Concept



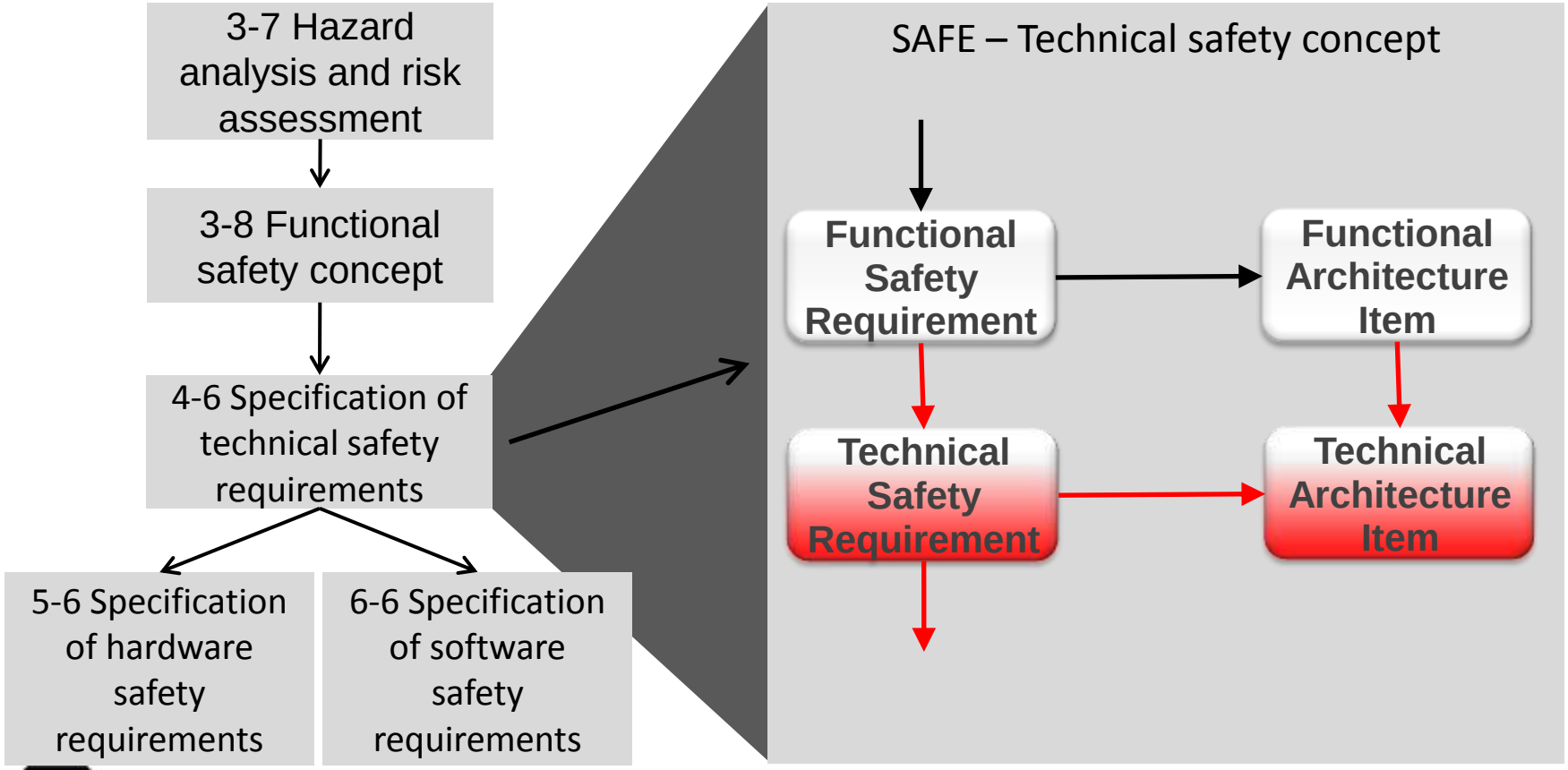
On analysis level, the functional safety concept contains the safety requirements derived from the safety goal.

The satisfy relationship traces their fulfillment on horizontal level.

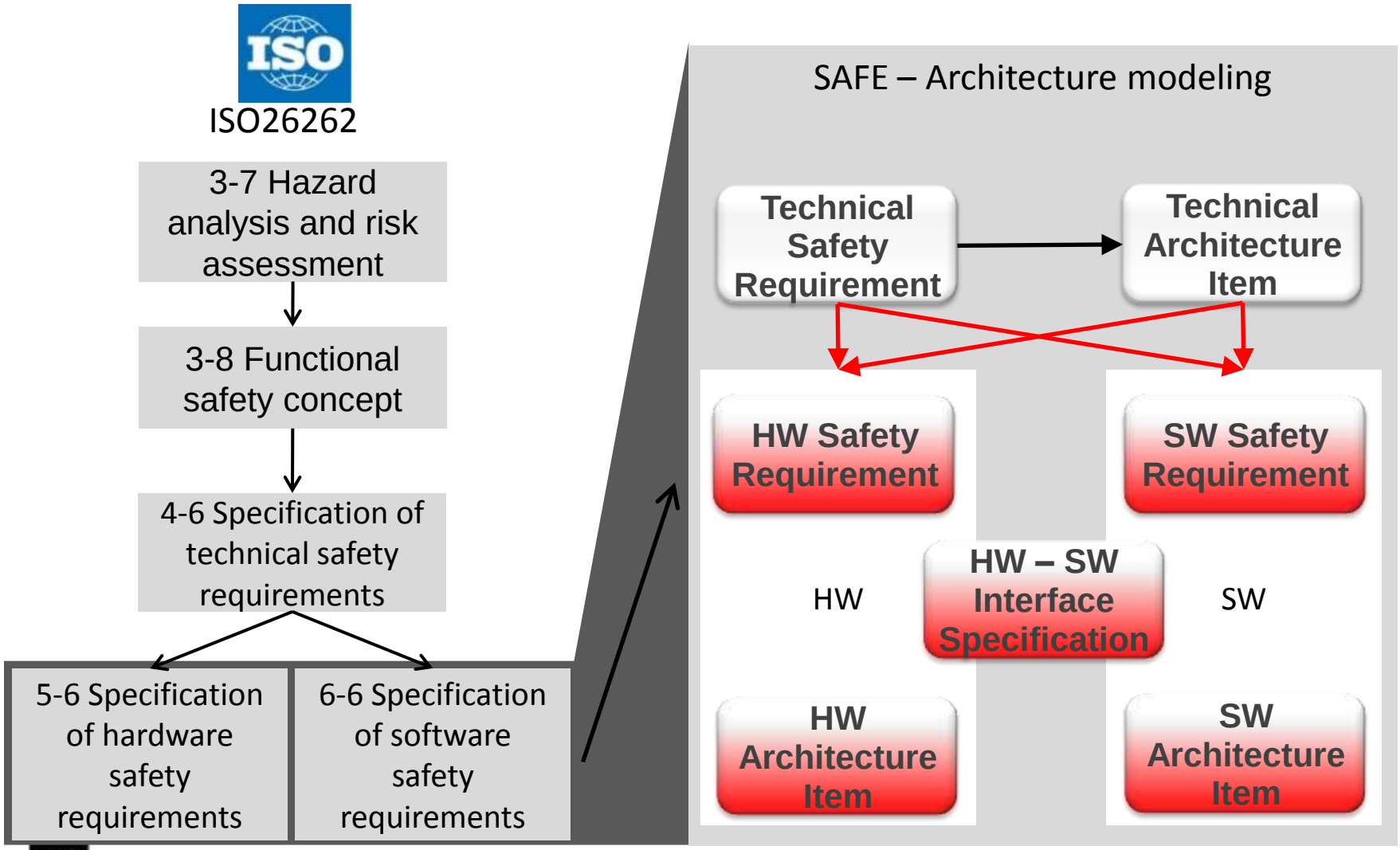
SAFE Modeling
Technical safety concept

ISO26262

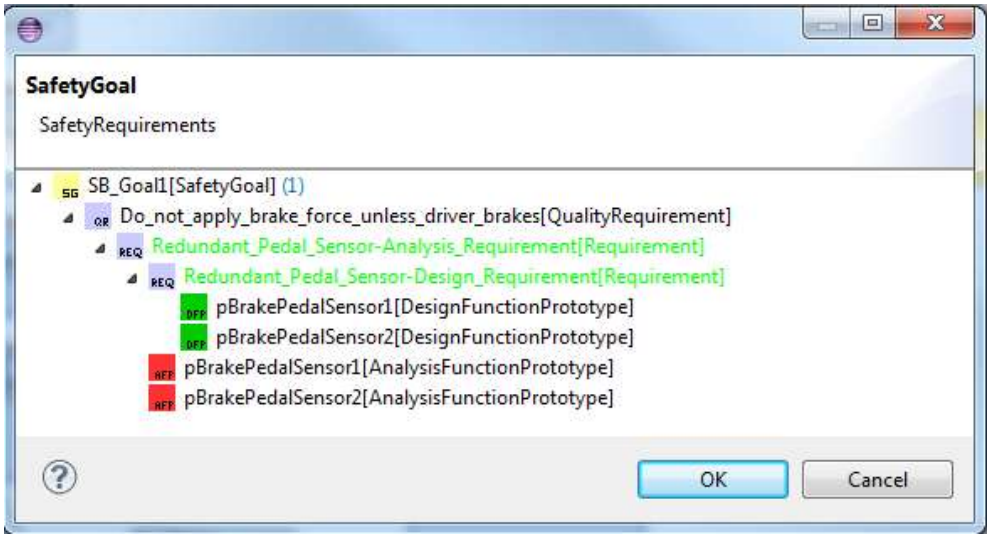
Specification of the technical safety requirements and their allocation to system elements for implementation by the system design.

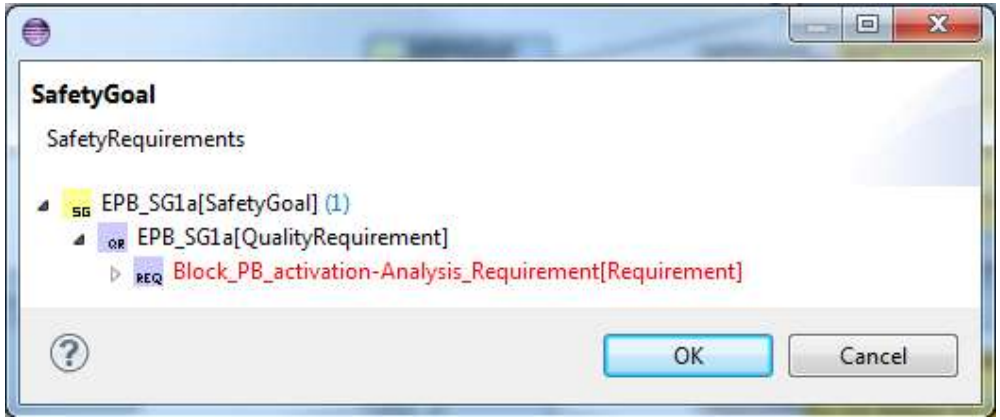


SAFE Modeling
HW-SW Safety concept



SAFE Modeling
Safety Goal Fulfillment





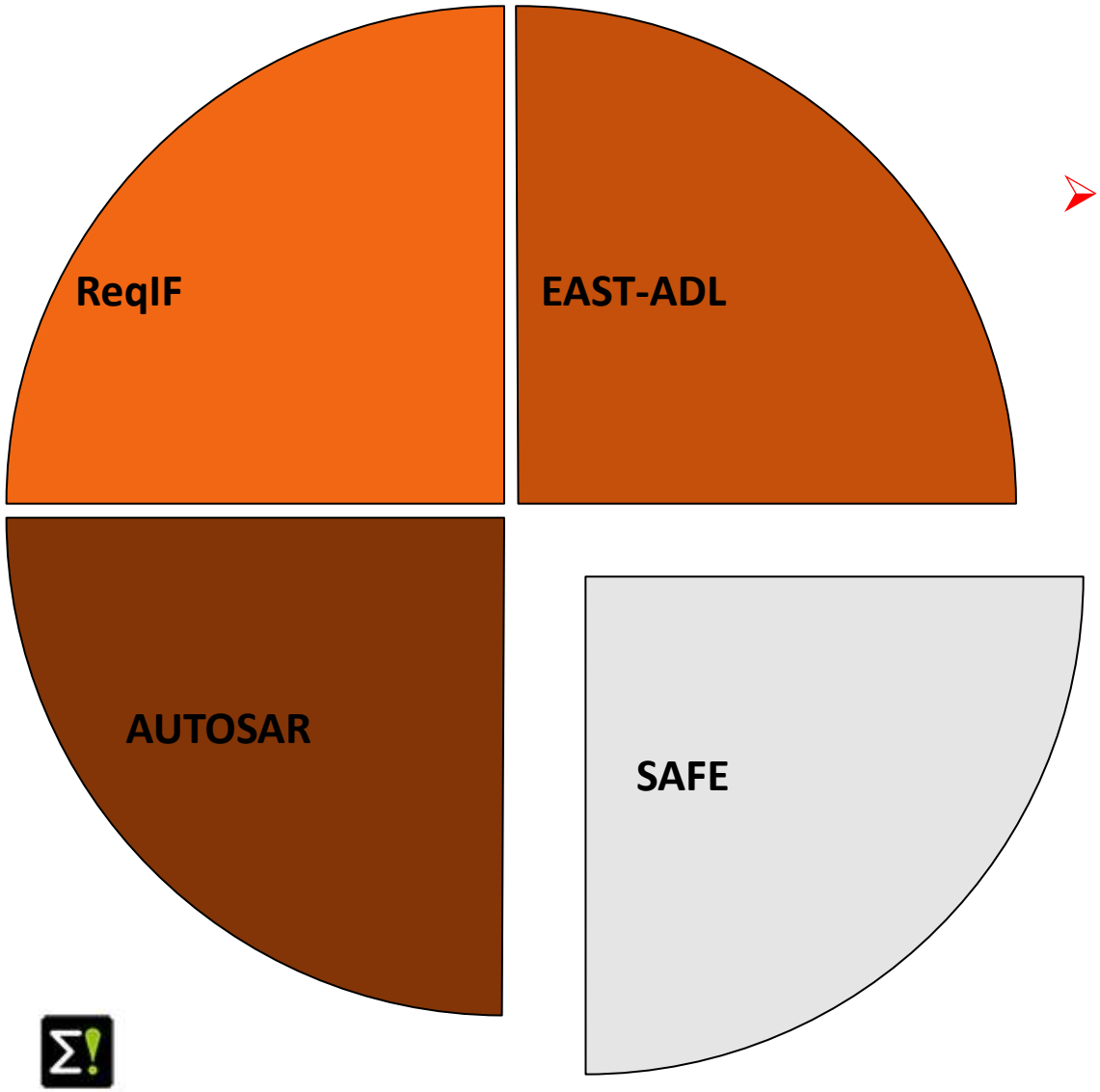
These views show the safety requirements tracing tree. The satisfying architecture elements are shown as leaves of the tree.

In case a safety requirement is satisfied, it is shown in green text color, otherwise in red text color.

Content

- **Open Meta-model**
  - Scope
  - **Structure**
  - Exemplified insight

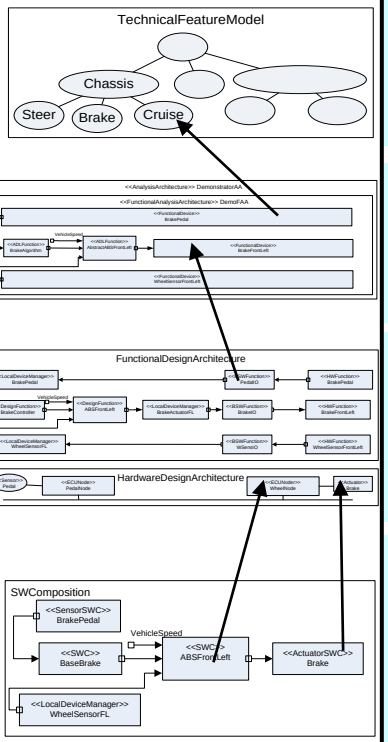
SAFE Modeling
Scope

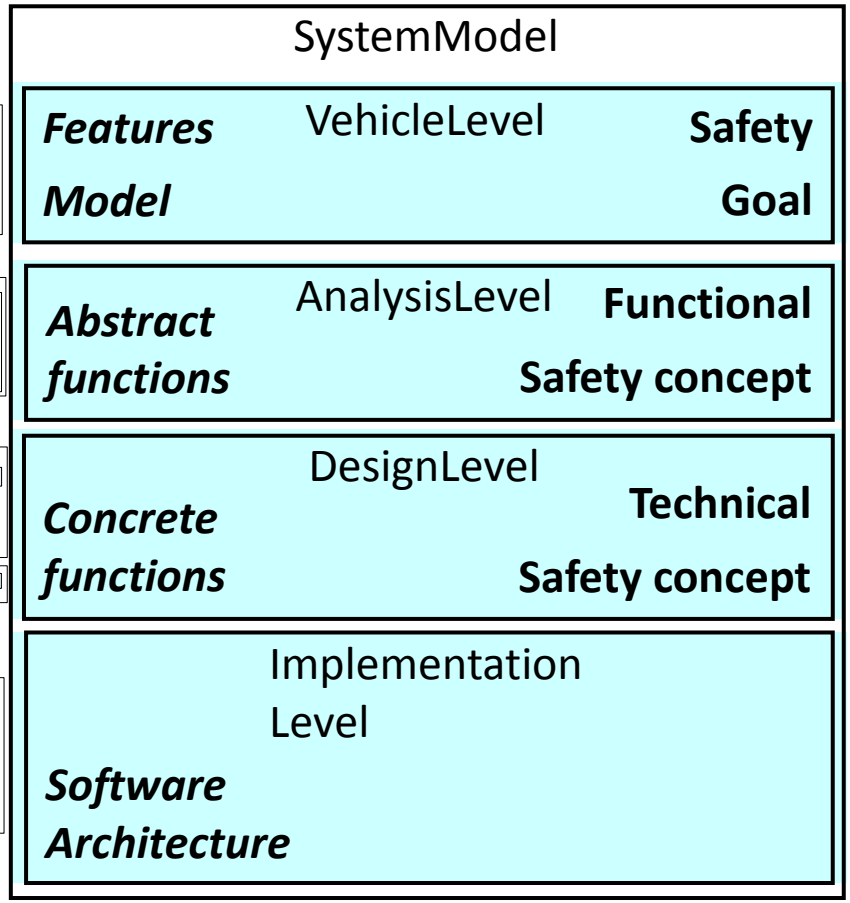


- SAFE Meta-Model completes automotive architecture languages

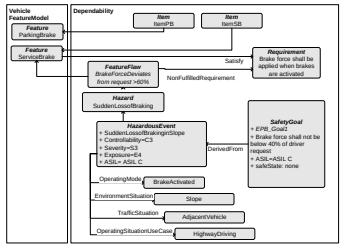
SAFE Modeling
From Requirement to AUTOSAR

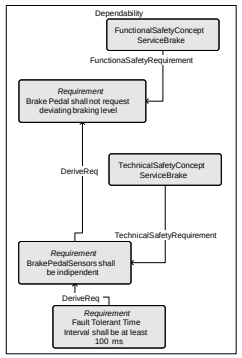
Model Based Development





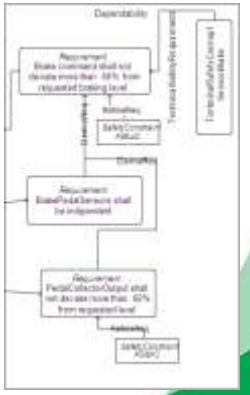
Safety Analysis





Derive

Refine



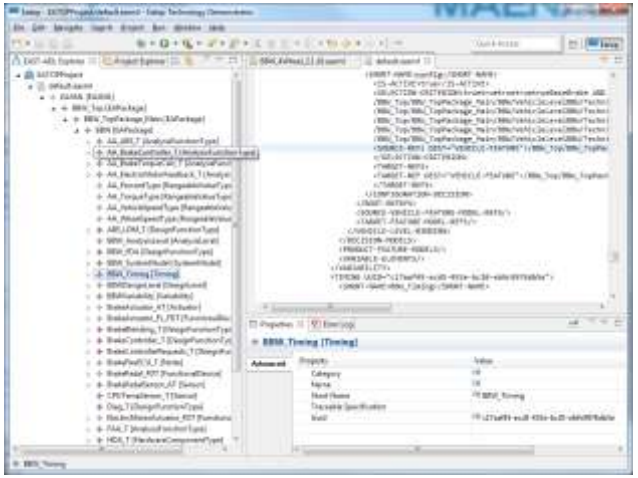
SAFE Modeling
EAST-ADL Technology

- EAST-ADL Association
  - synchronize further refinement of the language
  - provide an entry point for EAST-ADL information

EAST-ADL
WWW.EAST-ADL.INFO

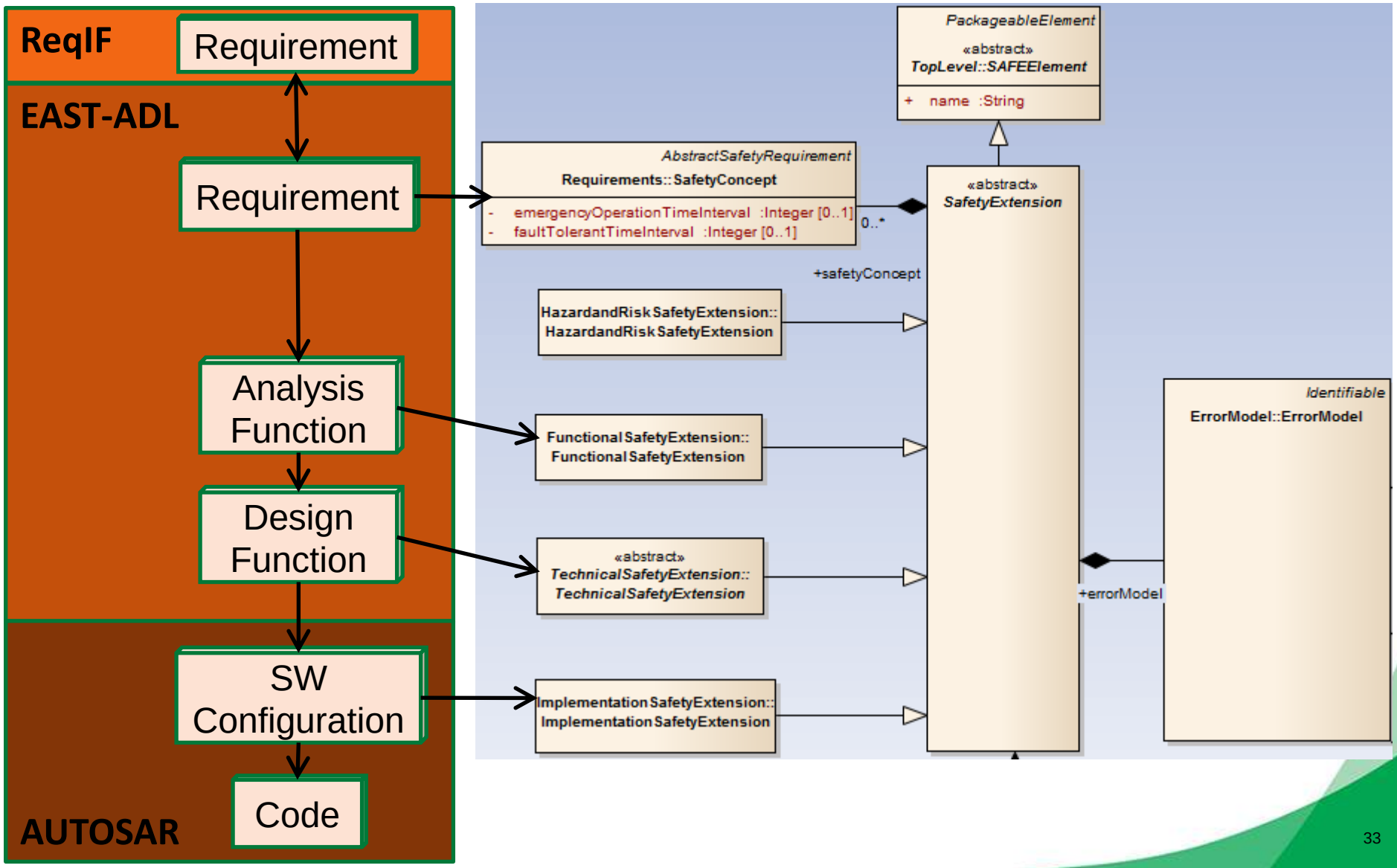
- EATOP: EAST-ADL Tool Platform
  - Modelling infrastructure
  - Plugins for analysis and synthesis
  - Eclipse project eclipse.org/eatop
- LinkedIn Group

LinkedIn EASTADL



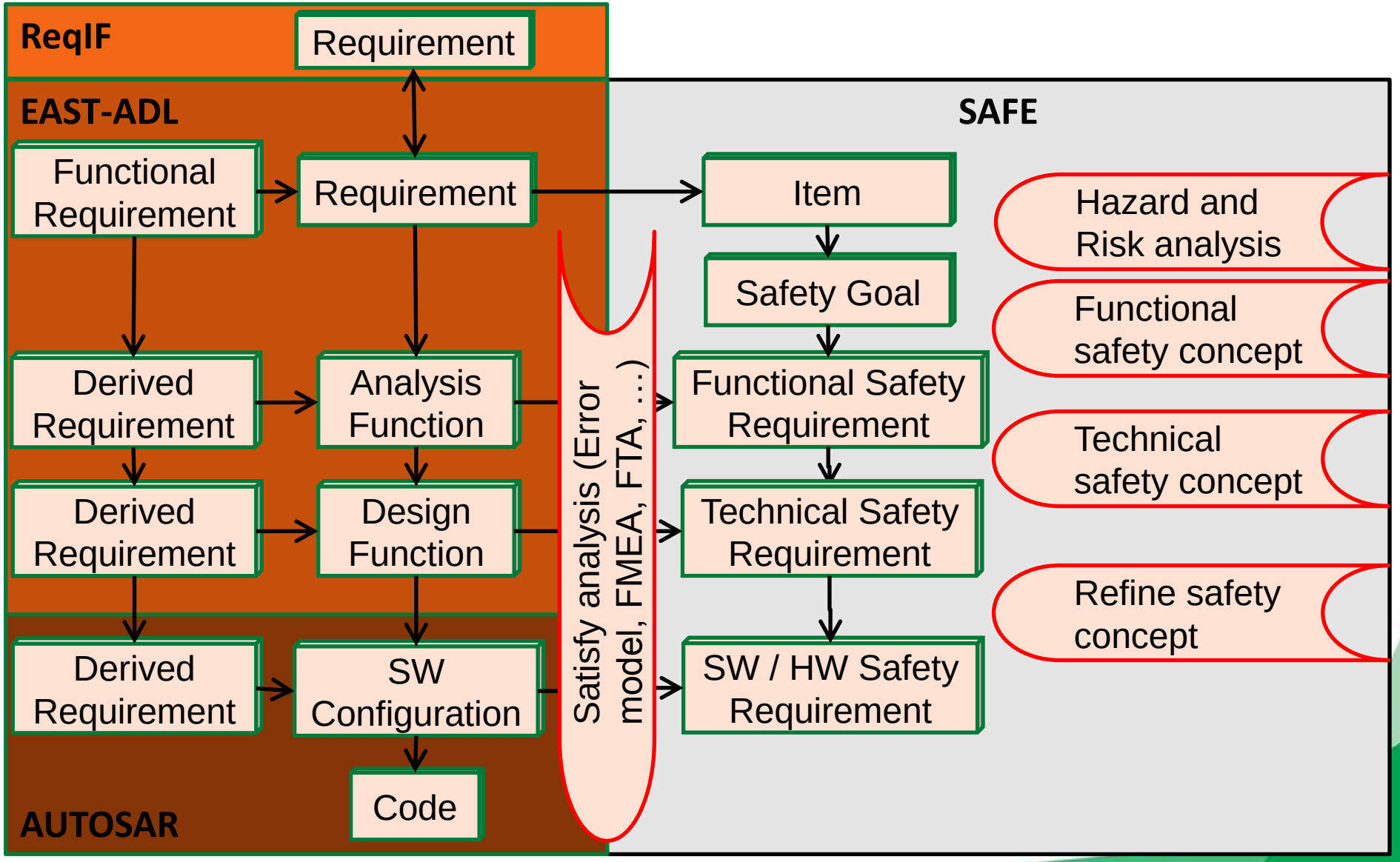
SAFE Modeling

Summary: Scope of SAFE Meta-Model



SAFE Modeling

Summary: Scope of SAFE Meta-Model



Content

- **Open Meta-model**
  - Scope
  - Structure
  - **Exemplified insight**

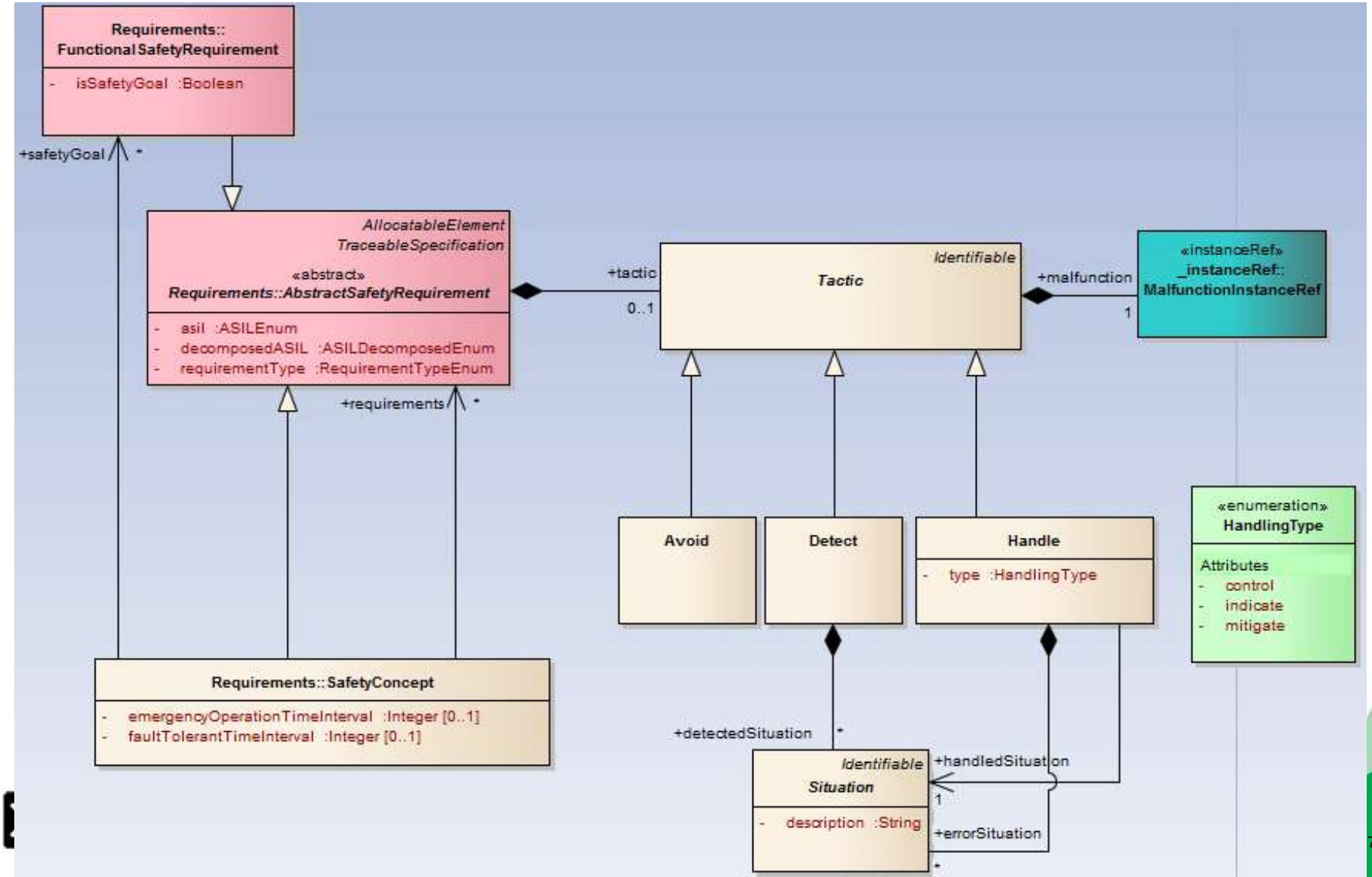
SAFE Modeling

How to react on a possible malfunction

- Tactic is a formalization for defining the role a given requirement has regarding error management.
- Tactic is defined in two steps
  1. Describe in a safety requirement what should not happen
  2. Define how to react if the malfunction happens nonetheless

SAFE Modeling

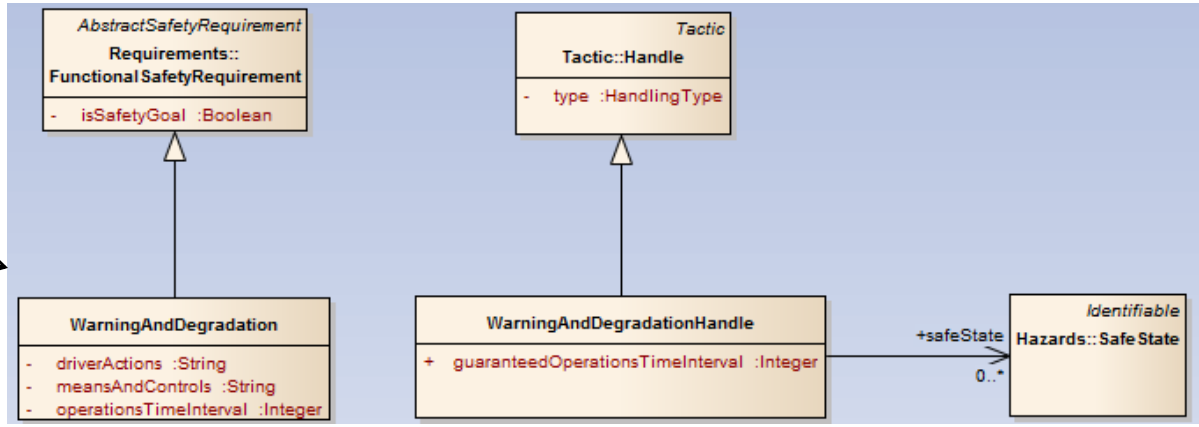
Tactic to react on a possible malfunction

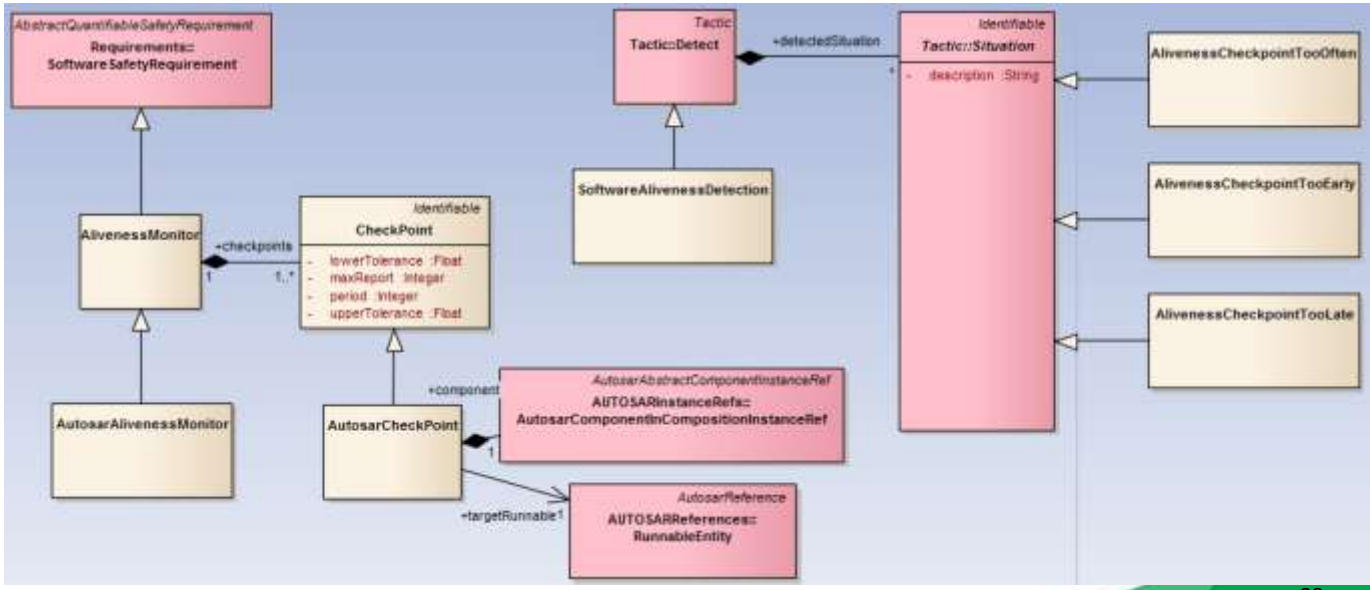


SAFE Modeling
Library of pre-defined tactics

Tactics on function level
- Warning and degradation concet

Tactics on SW level
- Aliveness Monitor
- Actuator Monitor
- CRC Checksum
- Comparison
- Context Range Check
- Cpu Self Test
- Filter
- Gradient Check
- Health Monitor
- Hearbeat
- Memory Self Test
- Voting





SAFE
Summary

SAFE created a DSL for the safety perspective

No seamless modeling:

- There is no unique DSL that covers all abstraction levels and all perspectives!

Limited usability

- The automotive DSLs (EAST-ADL, AUTOSAR, SAFE) are heavy!

Automatism still not sufficient

- Automatic model to model transformation and code generation is a key for handling the models

Thank you for your attention