Safe Automotive soFtware architEcture (SAFE)

Co-summit 2015, 10-11 March 2015, Berlin - Germany

Dr. Stefan Voget

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

July 2014

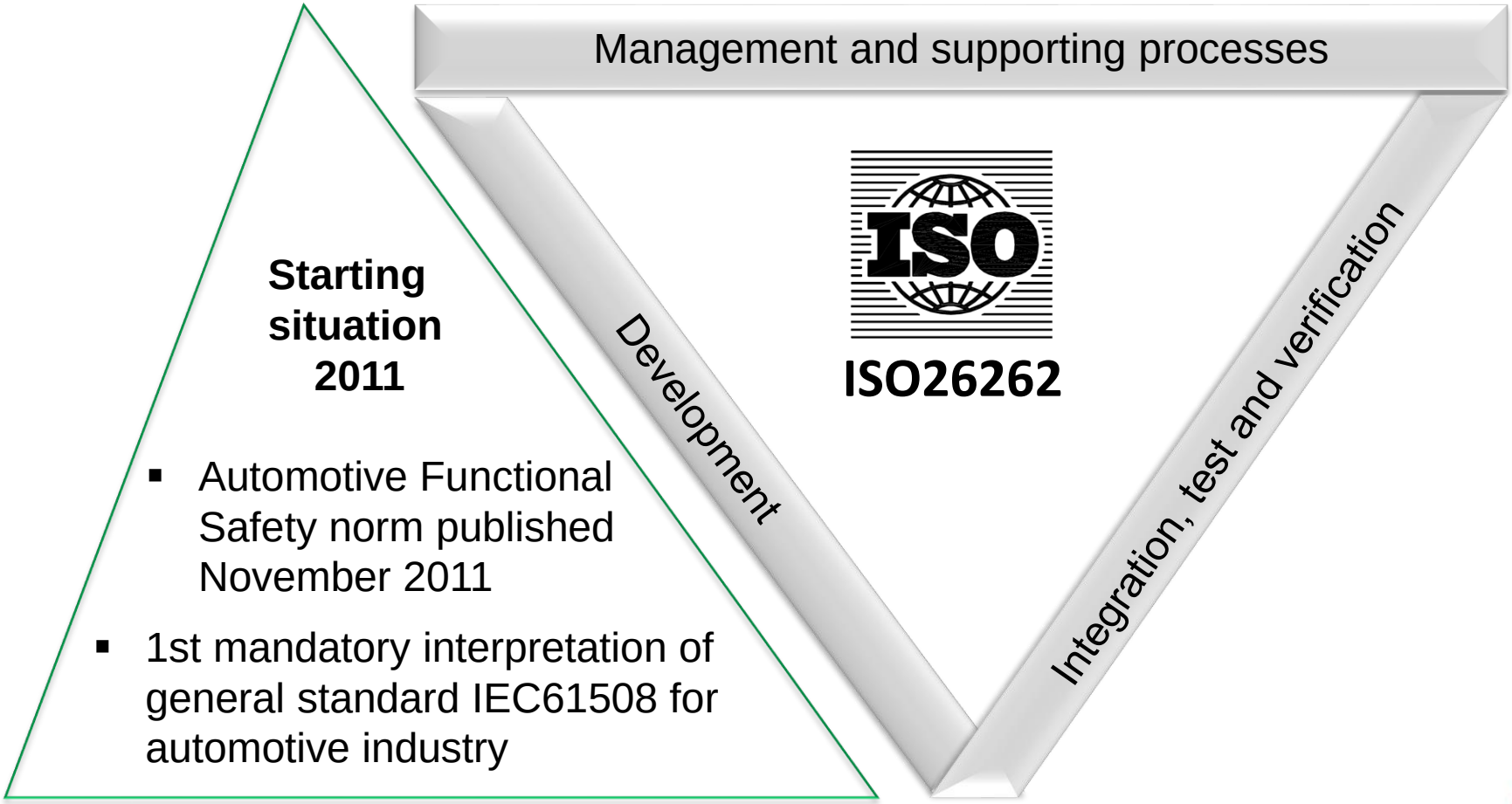
- GM recalls 8.4 Mill. vehicles
- Faulty ignition switch

October 2013 | November 2013 | July 2014

(Source: Vice Media Inc. 2014)

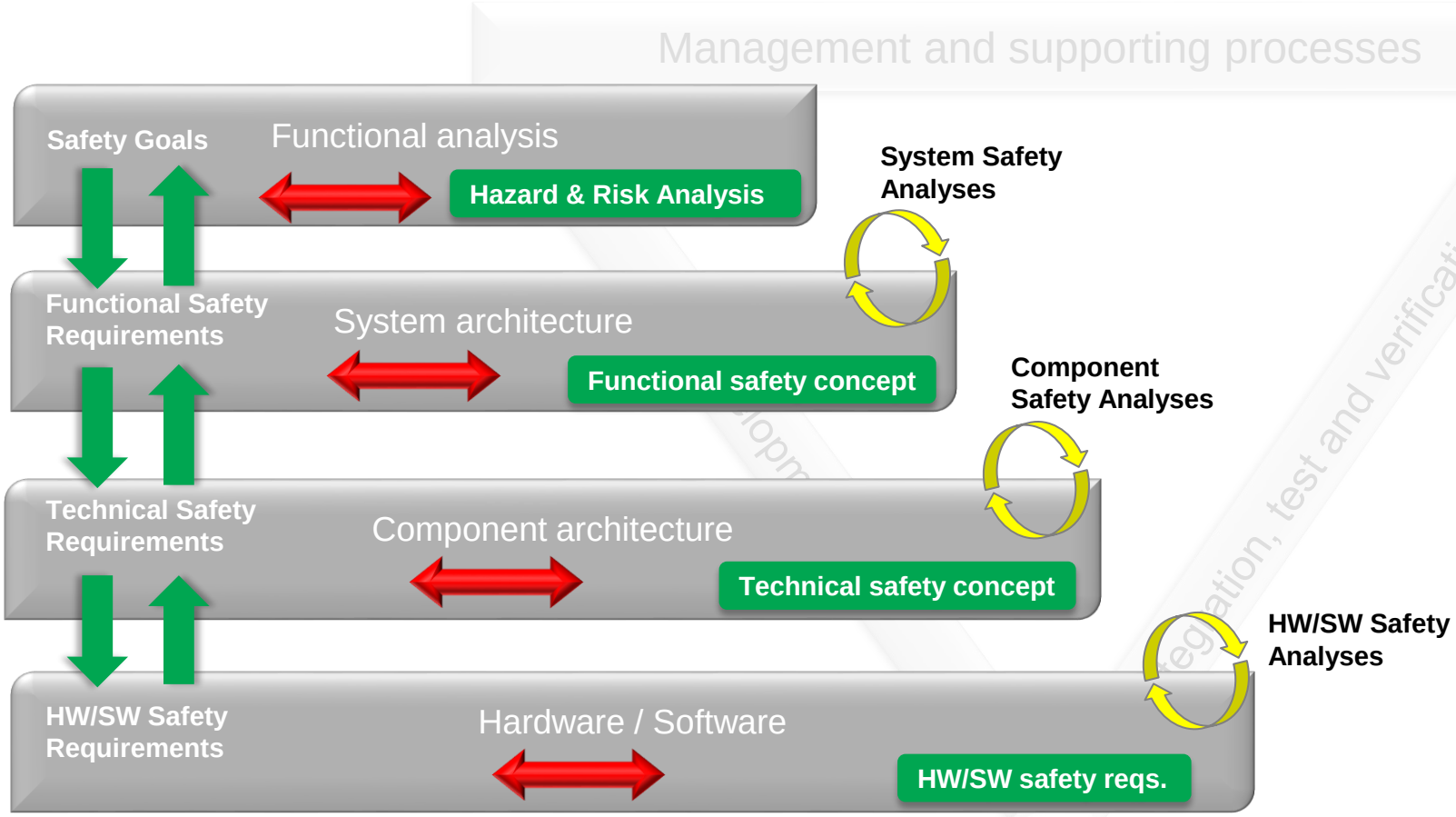
SAFE Motivation

Scope of SAFE - ISO26262 Development Lifecycle



SAFE Motivation

Scope of SAFE - ISO26262 Development Lifecycle



SAFE Motivation

Scope of SAFE - ISO26262 Development Lifecycle

Safety Goals

Functional Safety Requirements

Technical Safety Requirements

HW/SW Safety Requirements

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

Concept: Influence from other technologies

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

Concept: Hazard and risk analysis

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

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

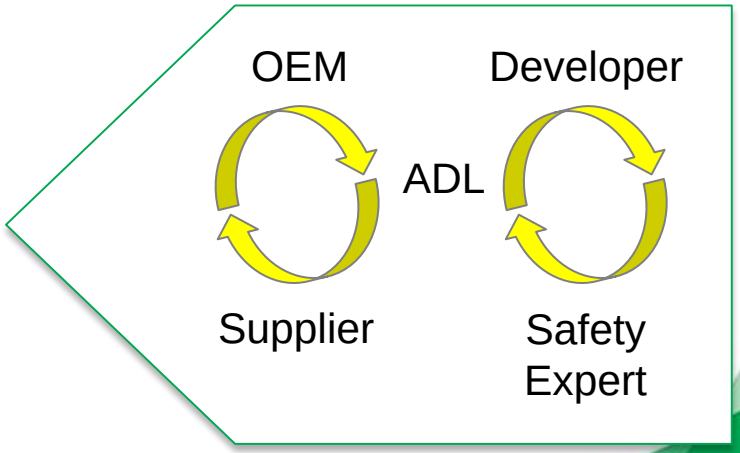
- ISO26262 defines more than 1000 requirements
- Challenge for automotive industry:
  - Reach acceptable risk level by ensuring process compliance with ISO26262

Approach

- Provide model based development process that integrates functional-safety

Solution of SAFE

- Architecture description language
- Tools
- Methods and application Rules



Agenda

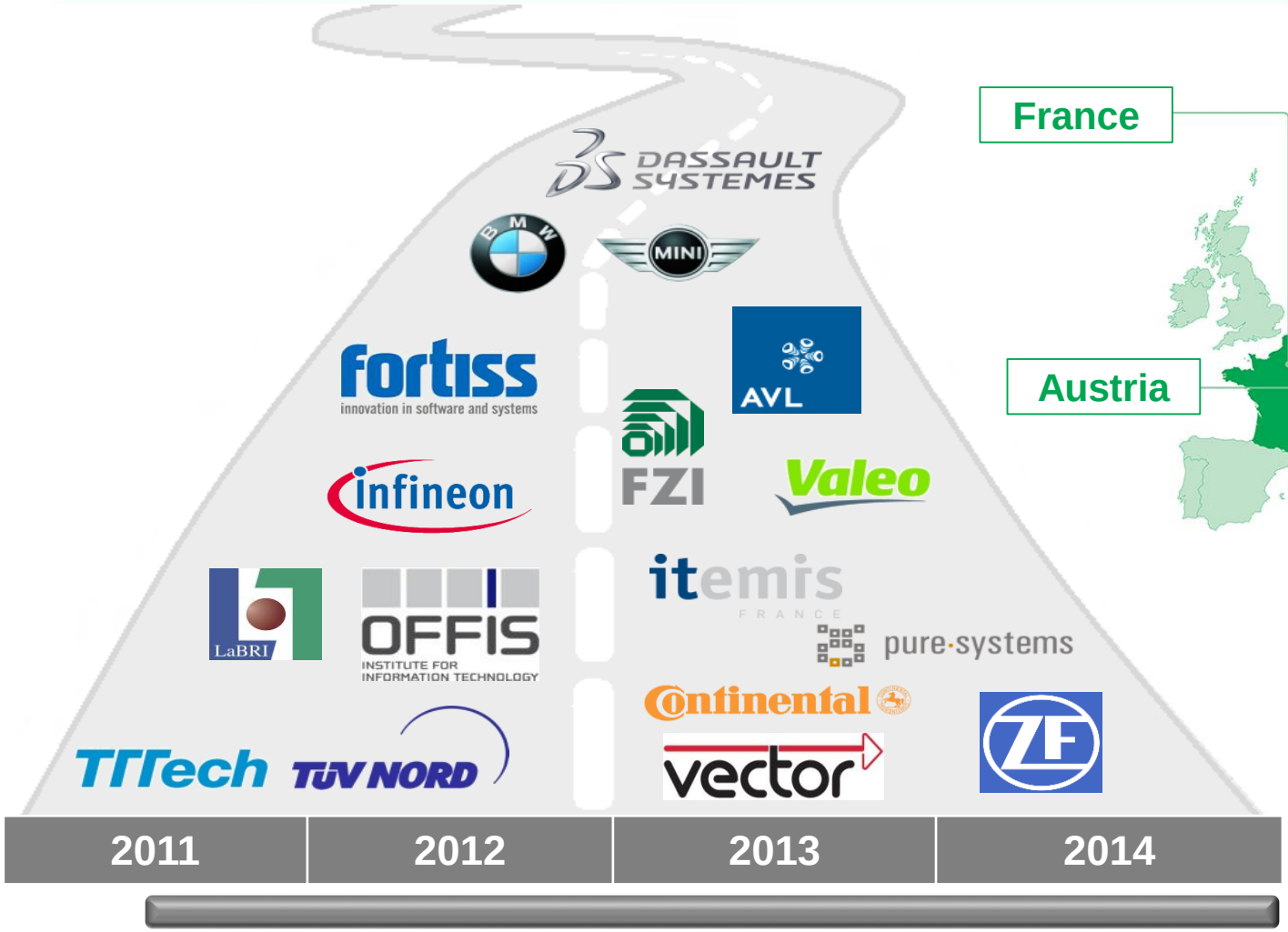
SAFE motivation

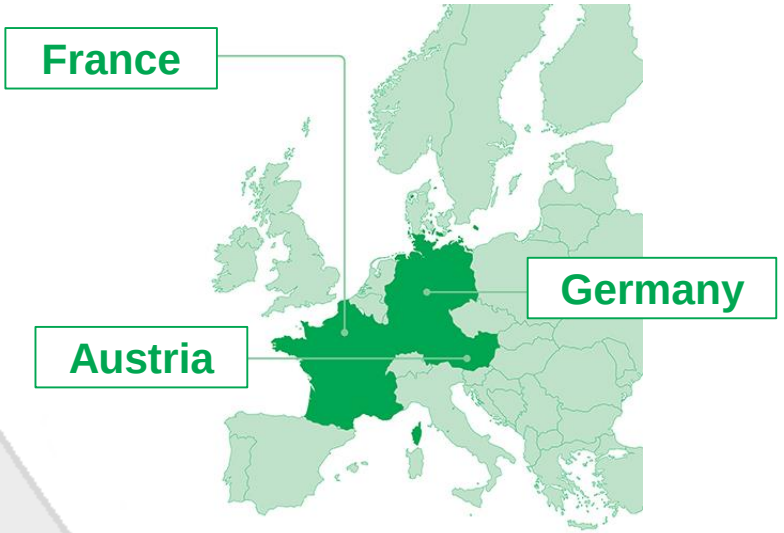
makes Functional safety safe

SAFE in the project landscape

SAFE and standardization

SAFE in the project landscape
Who did it?



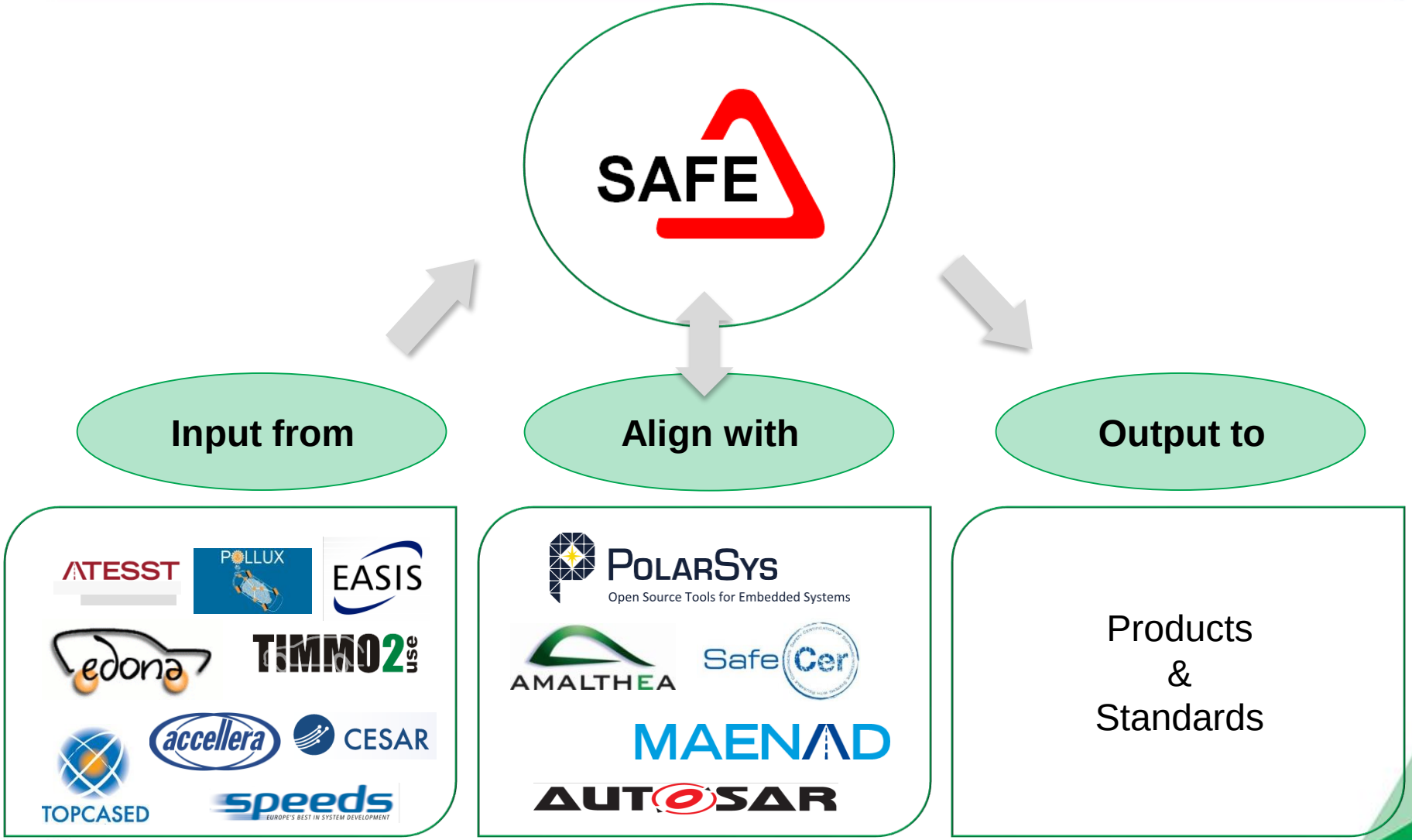


Start: 01.07.2011

End: 31.12.2014

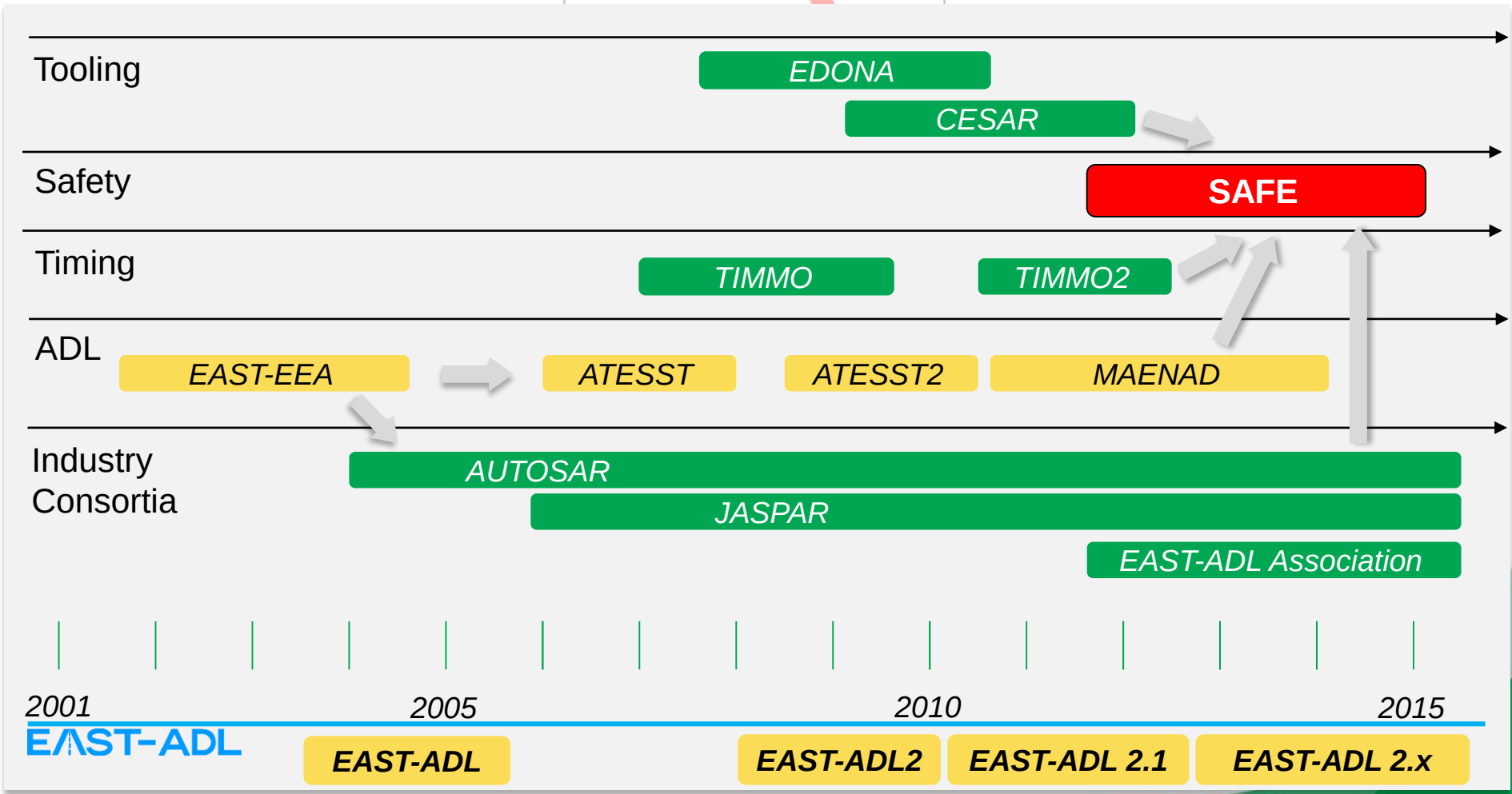
SAFE in the project landscape

How did we work with others?

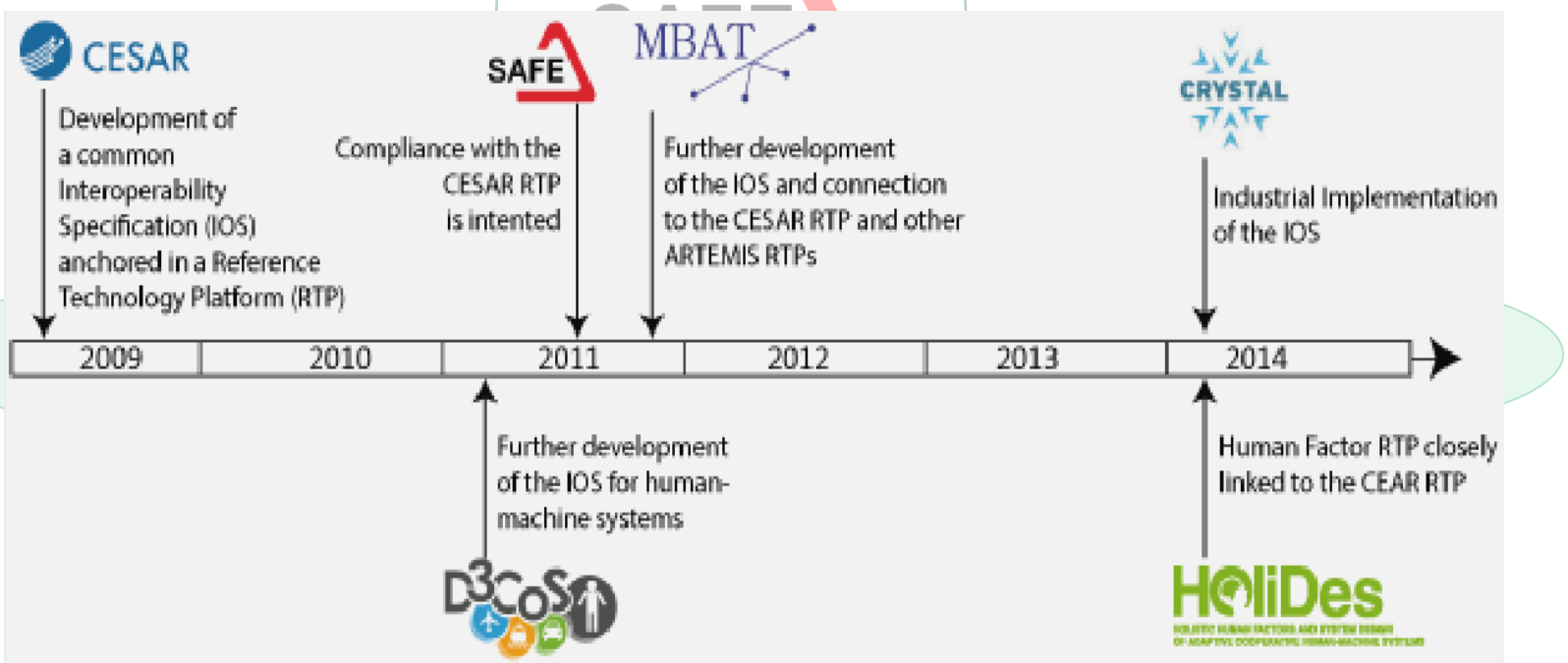


SAFE in the project landscape

How did we work with others?

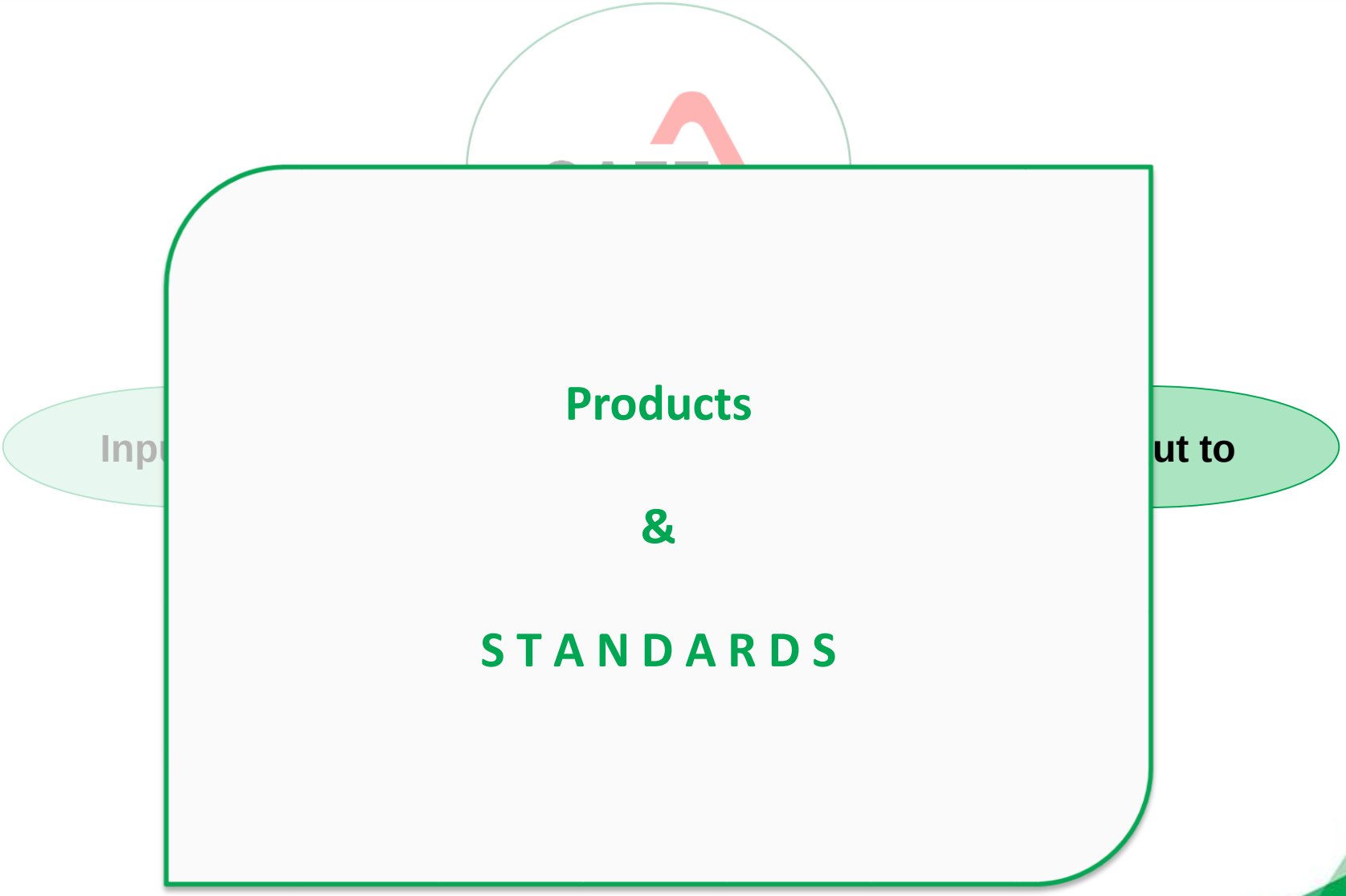


SAFE in the project landscape
How did we work with others?



* Source: SafeTRANS News (news.safetrans-de.org)

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



Agenda

SAFE motivation

makes Functional safety safe

SAFE in the project landscape

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

EICOSE

ARTEMIS innovation Cluster on transportation

Requirements

ISO

ISO26262

Methodologies and application rules

OMG
OBJECT MANAGEMENT GROUP

Standardization group for SW engineering

SAFE and standardization
Summary

Made first implementation of the standard

ISO 26262 published in 2011 → we started in 2011

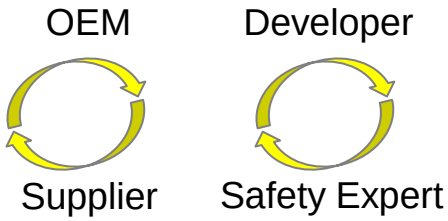
All partners had the same goal to ensure safety

Not only for Europe but for whole world

Provided commercial tools and trainings to the market

Set standards

Exploitation from a 1st Tier point of view



Thank you for your attention