Rolf Johansson

Research Project: FUSE

FUnctional Safety and Evolvable architectures for autonomy

Partners:
SP, Volvo Cars, KTH, Semcon, Qamcom, Comentor

http://www.fuse-project.se/
rolf.johansson@sp.se

FUSE

The Problem – Project Challenge

•Today, most common accident cause :
Driver misjudgments

Tomorrow:
Autonomous driving

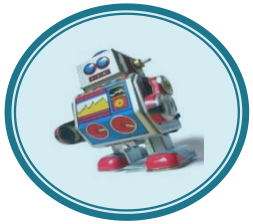
But

We need to make sure that autonomous driving is safe
(today we don't)

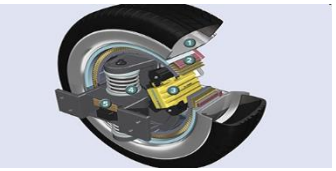
Three Dimensions of Autonomy

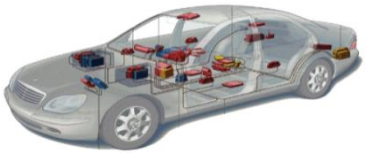
How much autonomy?

Driver only	Assisted Driver	Semi-automated	Highly automated	Fully automated



Autonomy in how much?

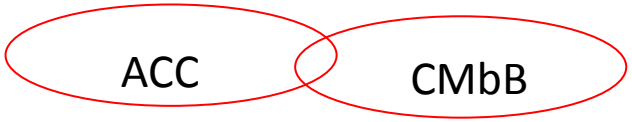




The ITS environment (source: ETSI)

Autonomy of how much?

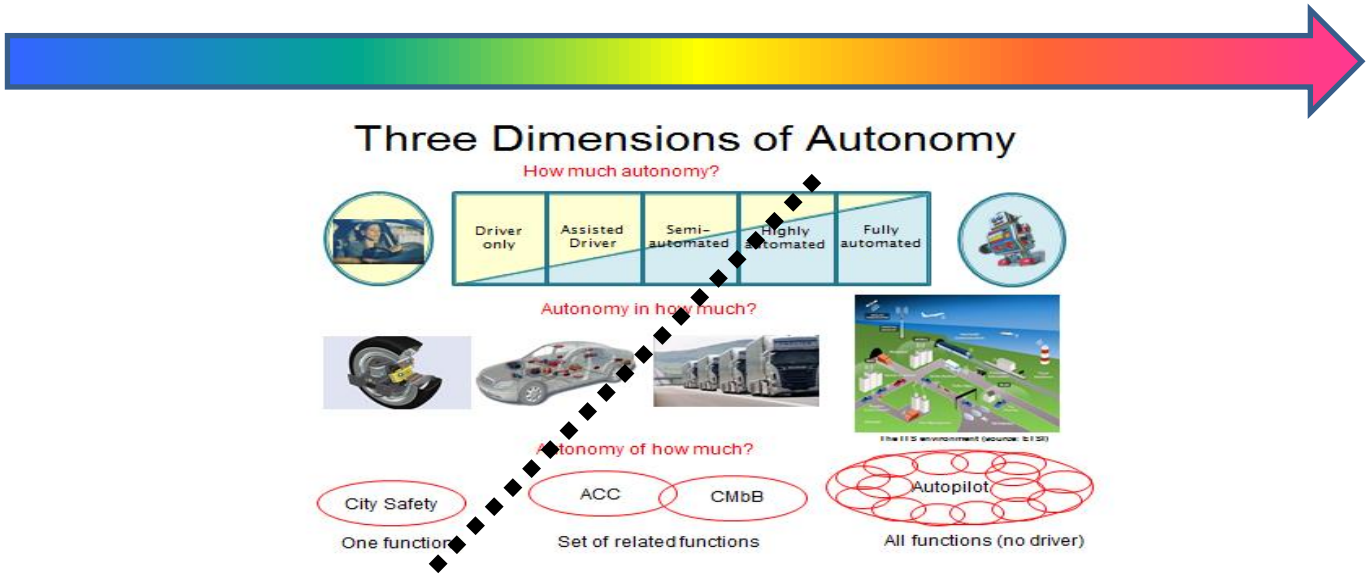
One function



Set of related functions

All functions (no driver)

Towards More Autonomy in More



What happens to <u>Functional Safety</u> when passing the dotted line?

- How to define it? (Lacking definitions in ISO 26262)
- How to achieve it? (Demand for architectural patterns, and division of responsibility)
- How to prove it? (Demand for new compositional safety arguing)

ISO26262 - Automated Driving and Autonomous Vehicles

- Two types of reasons why ISO26262 becomes problematic
  - Things are (much) more complicated
    - Extremely complex functionalities
    - Architectures much more complex
  - Things are fundamentally different
    - Manual driver not in the loop

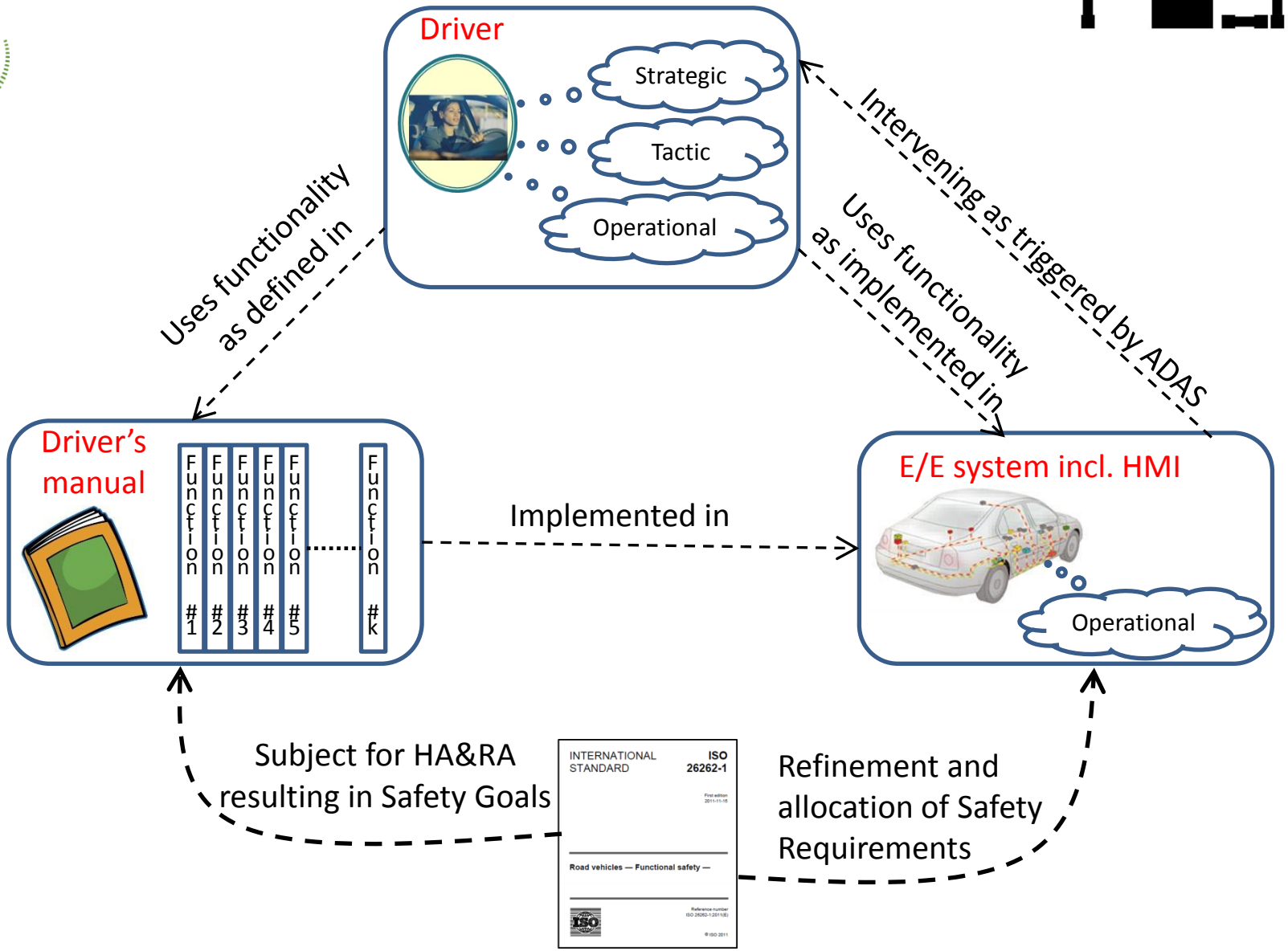
Focus of FUSE

- Functional safety
- Scalable Architectures
- New methods for development and safety analysis

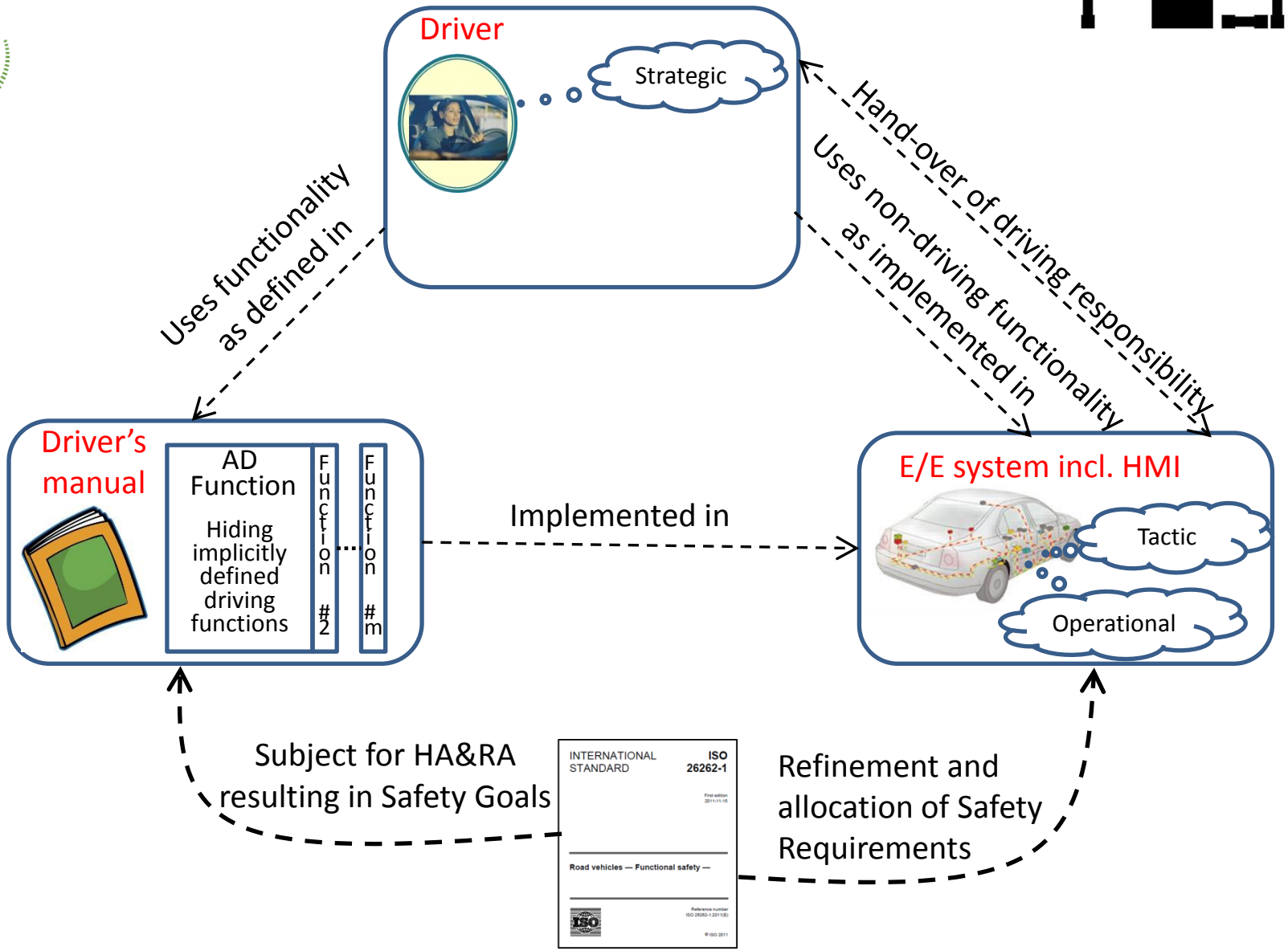
} for Autonomy

Well complements other efforts focusing on: sensing, estimation, control strategies and algorithms, HMI, …

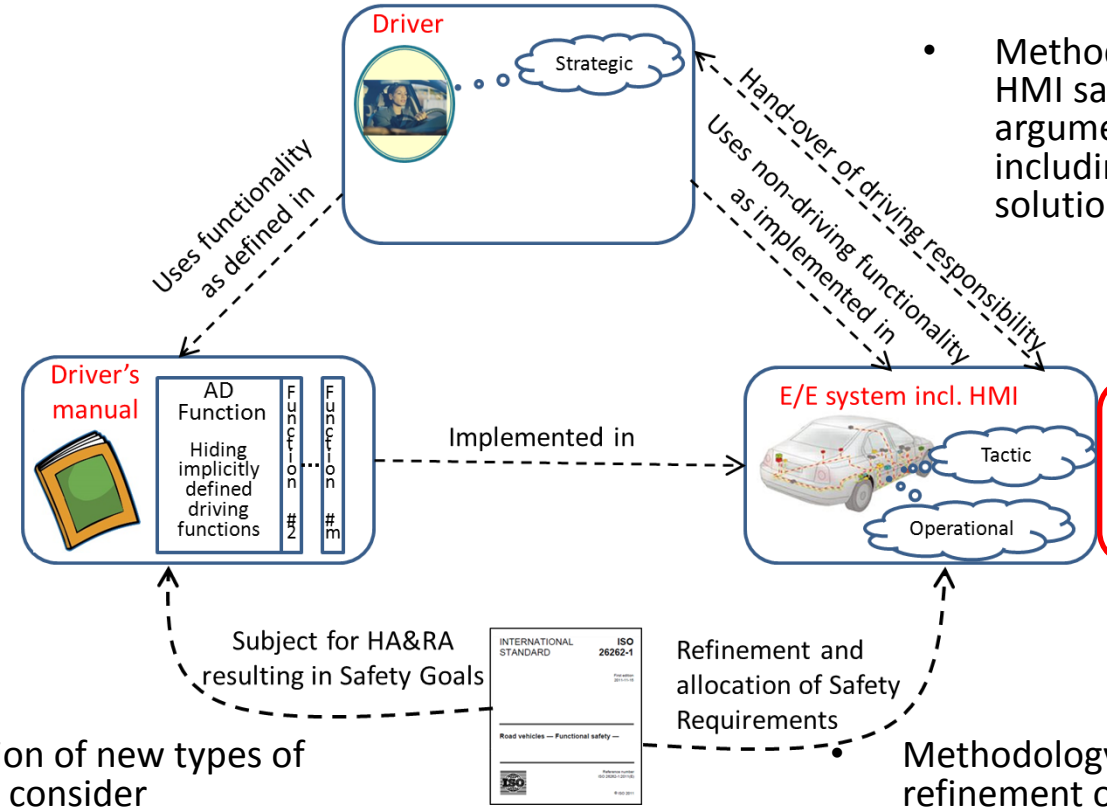
Manual driving



Highly automated driving



FUSE Contributions

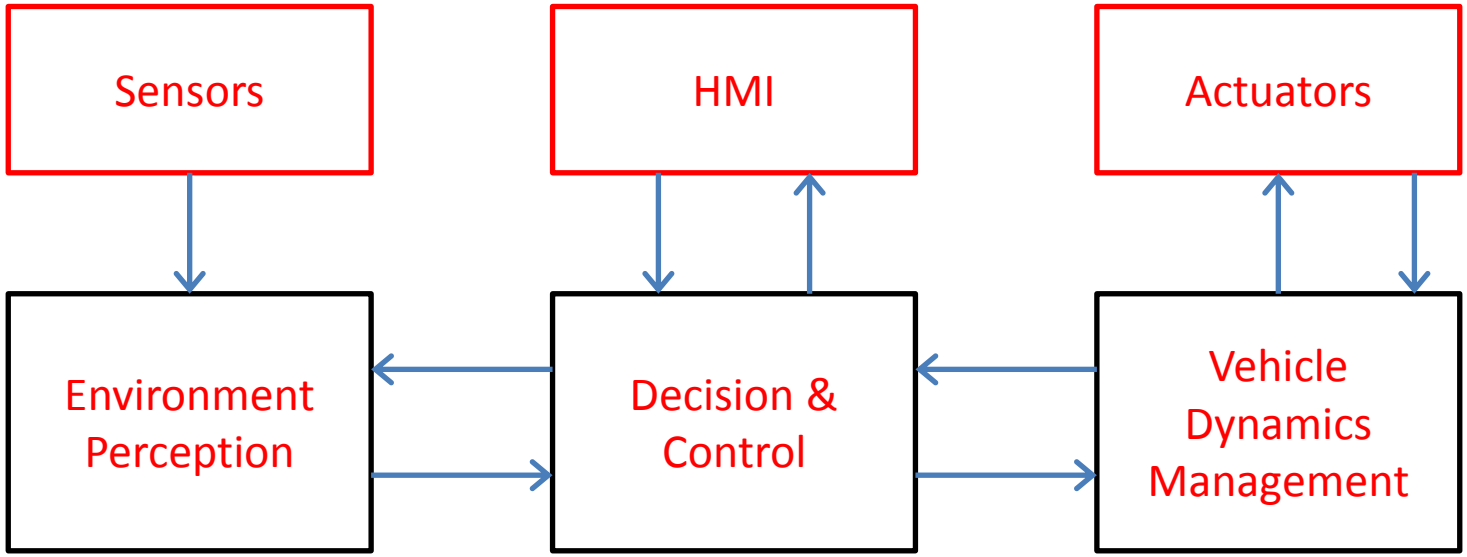


- Methodology for HMI safety argumentation, including specific solutions
- Architectural Pattern for Functional Safety Concept

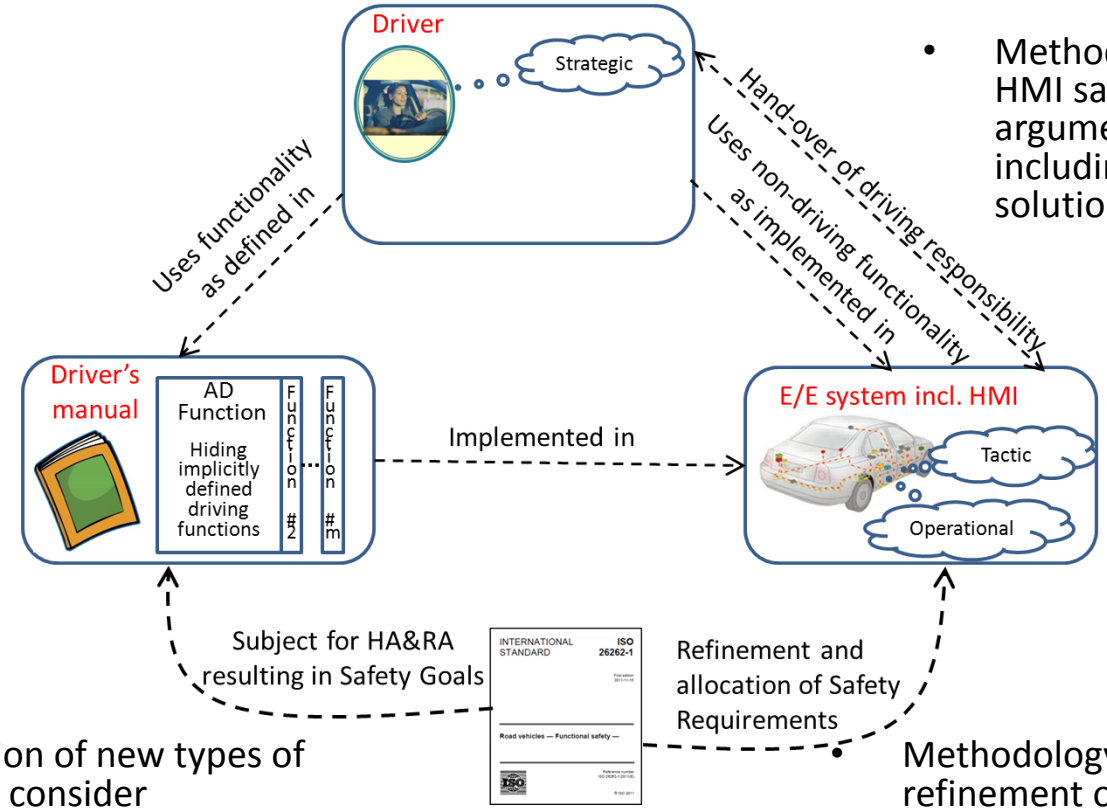
- Identification of new types of Hazards to consider
- Methodology framework for Hazard Analysis and Risk Assessment
- Guidelines for detailed Hazardous Events including explicit tolerance margins

- Methodology framework for refinement of safety requirements
- Patterns for dividing safety requirements on FSC top level
- Formulation of the functional safety problem for a sensor fusion block
- Disarming of the Trolley problem paradox

Functional Safety Concept Architecture



FUSE Contributions



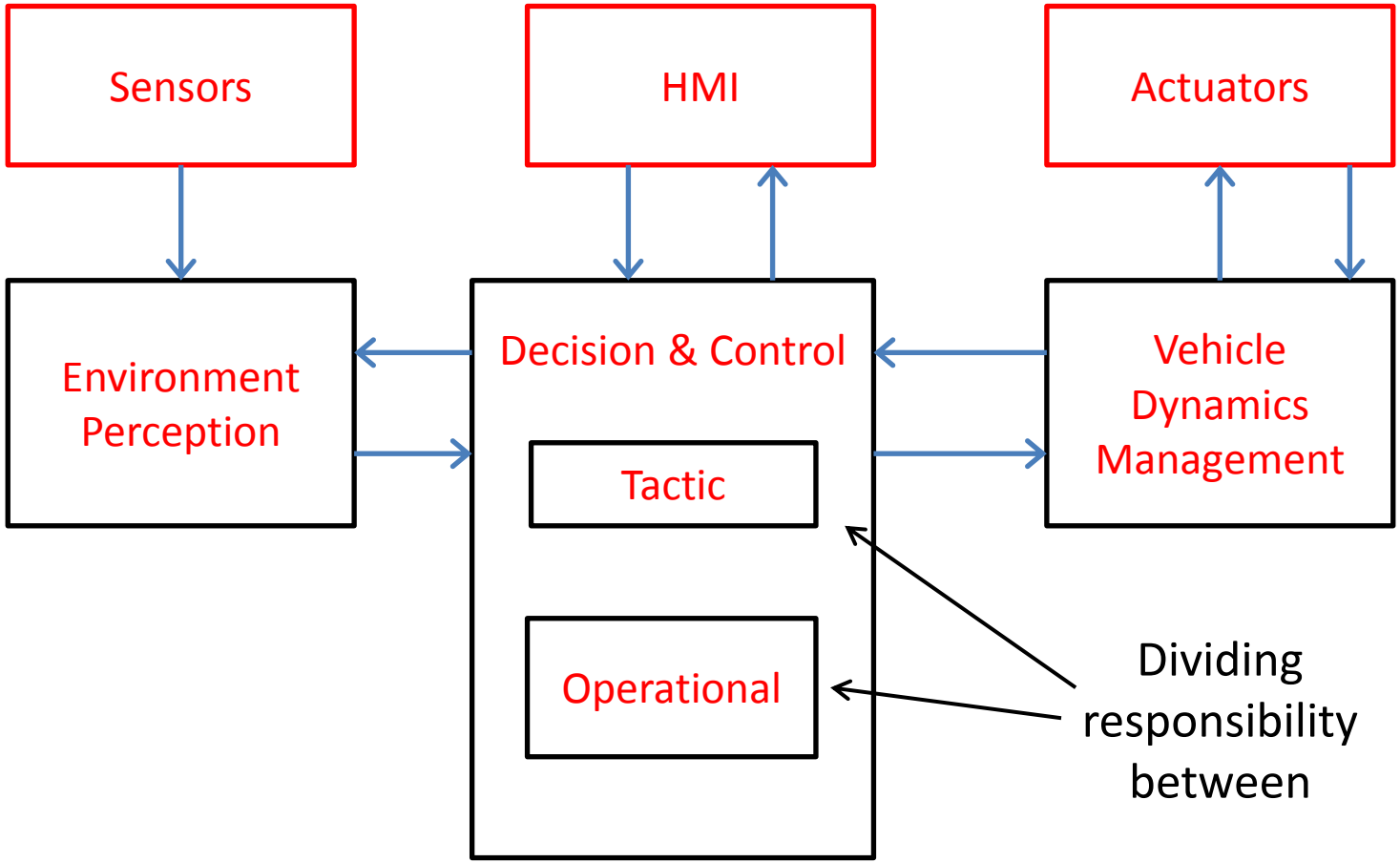
- Methodology for HMI safety argumentation, including specific solutions
- Architectural Pattern for Functional Safety Concept

- Identification of new types of Hazards to consider
- Methodology framework for Hazard Analysis and Risk Assessment
- Guidelines for detailed Hazardous Events including explicit tolerance margins

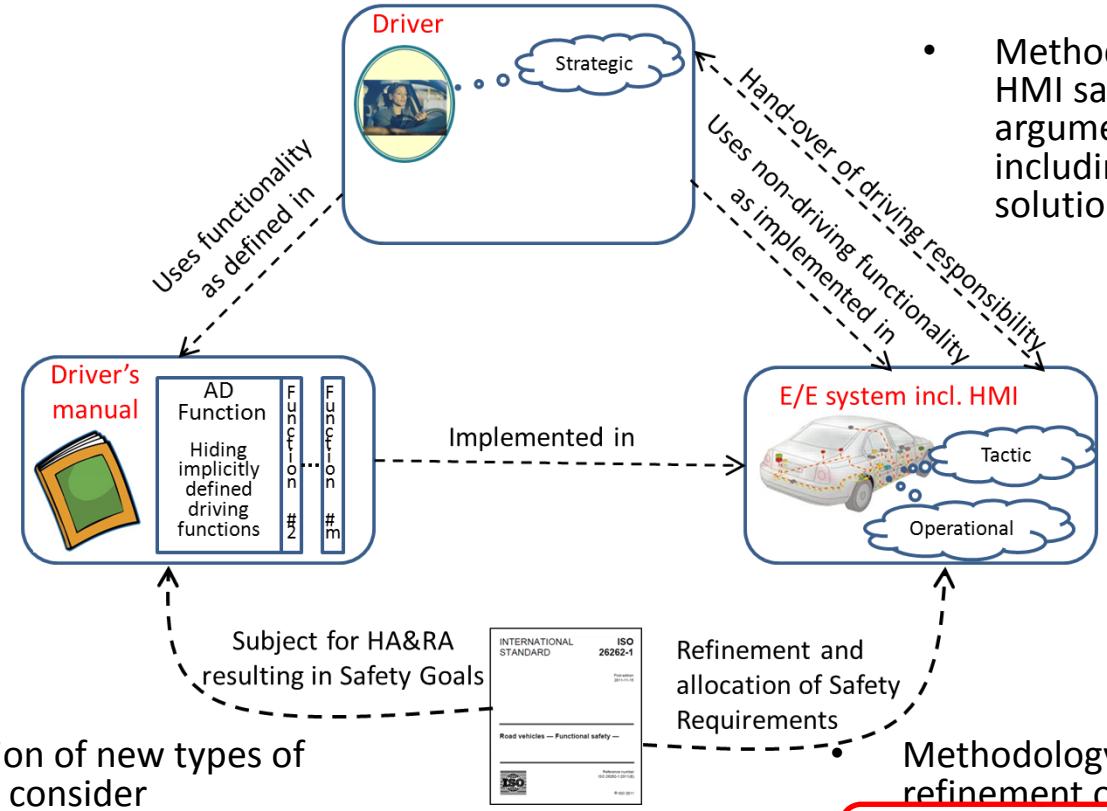
- Methodology framework for refinement of safety requirements
- Patterns for dividing safety requirements on FSC top level
- Formulation of the functional safety problem for a sensor fusion block
- Disarming of the Trolley problem paradox

“Do you know that your self-driving car is programmed to choose whom to kill”

Functional Safety Concept Architecture



FUSE Contributions



- Methodology for HMI safety argumentation, including specific solutions
- Architectural Pattern for Functional Safety Concept

- Identification of new types of Hazards to consider
- Methodology framework for Hazard Analysis and Risk Assessment
- Guidelines for detailed Hazardous Events including explicit tolerance margins

- Methodology framework for refinement of safety requirements
- Patterns for dividing safety requirements on FSC top level
- Formulation of the functional safety problem for a sensor fusion block
- Disarming of the Trolley problem paradox

Example on set of related Safety Goals

Generic SG XX:
Do not collide with any objects on the road in front of the ego vehicle, ASIL X

Generic SG kk:
Do not collide with a vehicle being on the road in front of the ego vehicle, ASIL K

Generic SG ll:
Do not collide with large objects on the road in front of the ego vehicle, ASIL L

Generic SG mm:
Do not collide with small objects or vulnerable road users being on the road in front of the ego vehicle, ASIL M

SG k1:
Do not collide with a higher impact speed than 65 km/h with a vehicle being on the road in front of ego vehicle, ASIL D

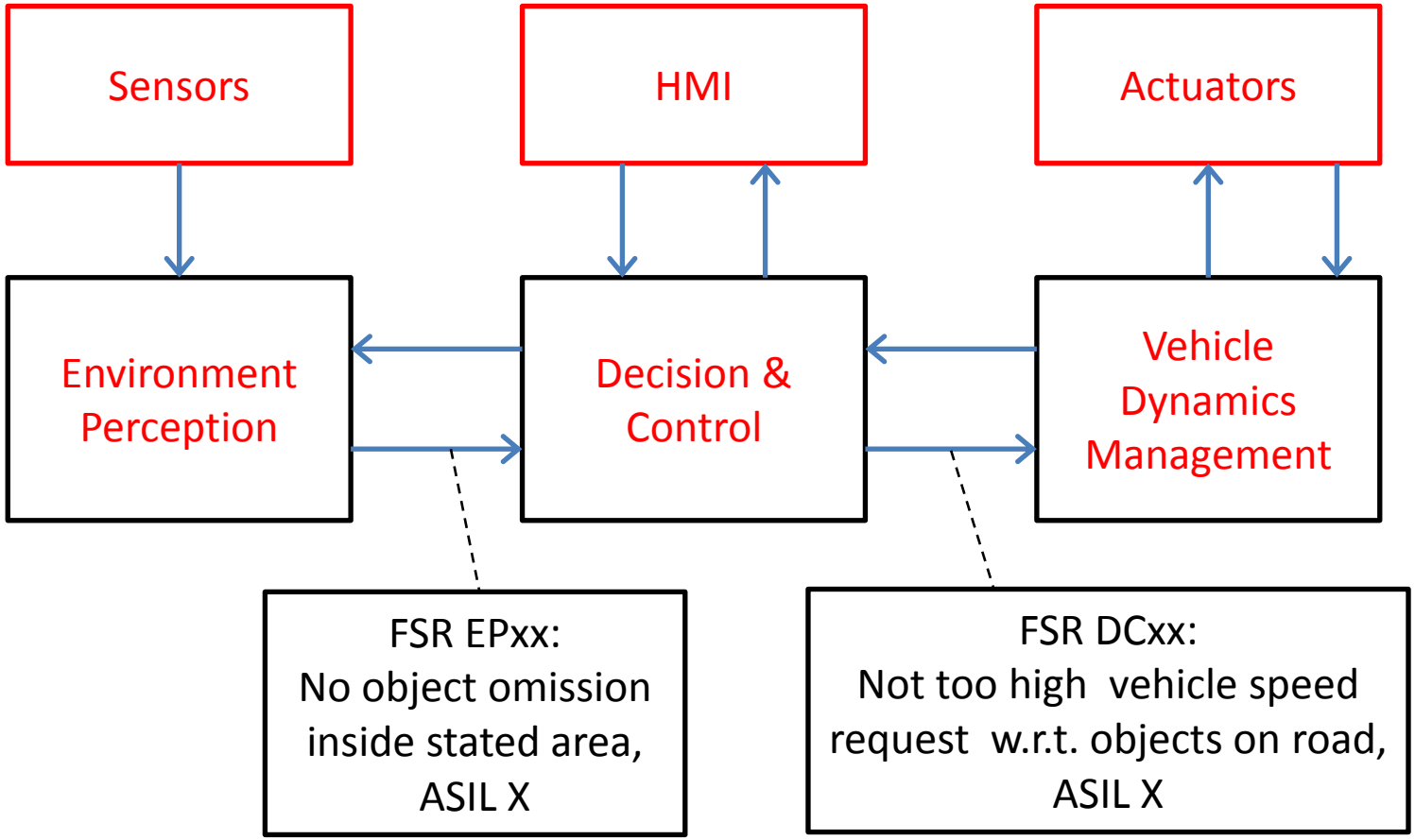
SG k2:
collide with a higher speed than 40 km/h vehicle being on the front of ego vehicle, ASIL C

SG k3:
collide with a higher speed than 25 km/h vehicle being on the front of ego vehicle, ASIL B

SG k4:
collide with a higher speed than 15 km/h vehicle being on the front of ego vehicle, ASIL A

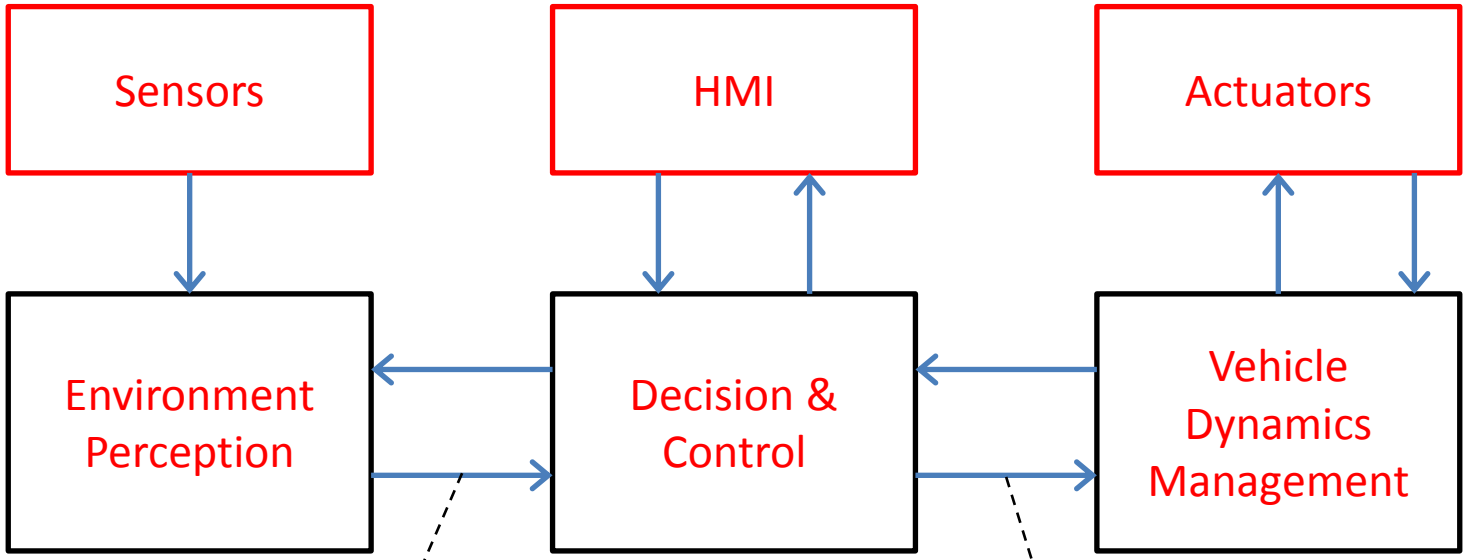
Functional Safety Concept Architecture

Generic SG XX:
Do not collide with any objects on the road in front of the ego vehicle, ASIL X



Functional Safety Concept Architecture

SG k1:
Do not collide with a higher impact speed than 65 km/h with a vehicle being on the road in front of ego vehicle, ASIL D

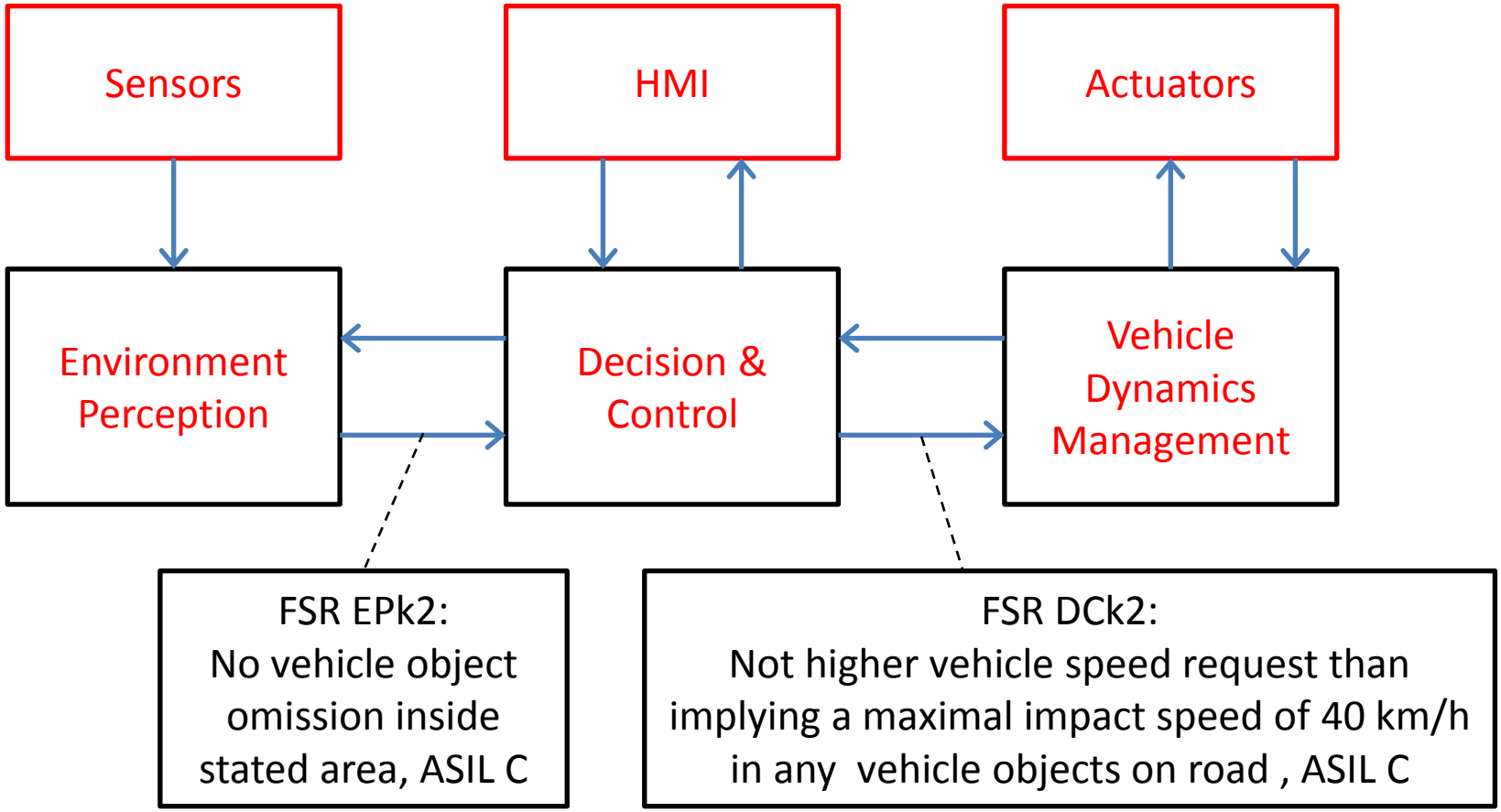


FSR EPk1:
No vehicle object omission inside stated area, ASIL D

FSR DCk1:
Not higher vehicle speed request than implying a maximal impact speed of 65 km/h in any vehicle objects on road , ASIL D

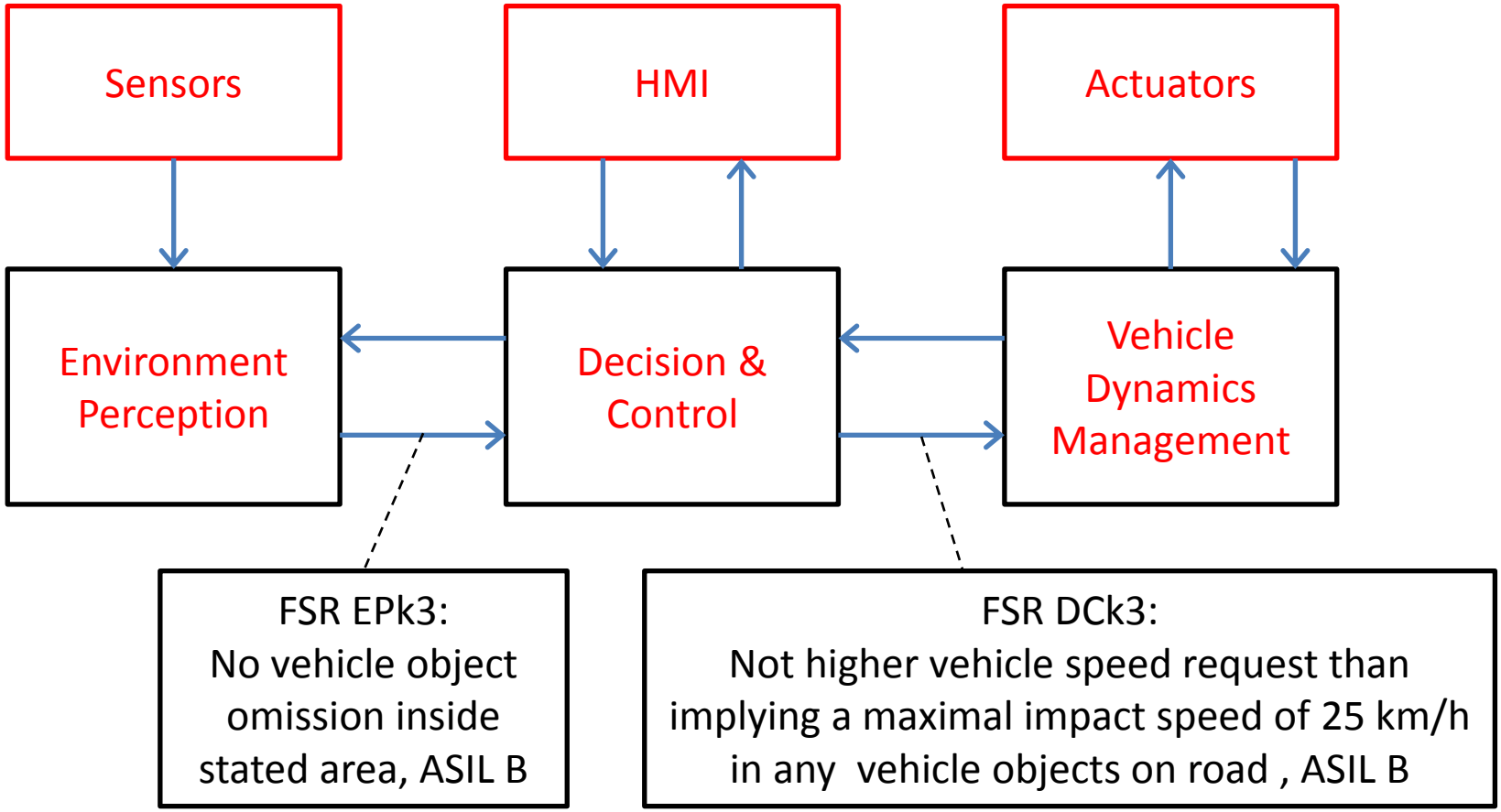
Functional Safety Concept Architecture

SG k2:
Do not collide with a higher impact speed than 40 km/h with a vehicle being on the road in front of ego vehicle, ASIL C



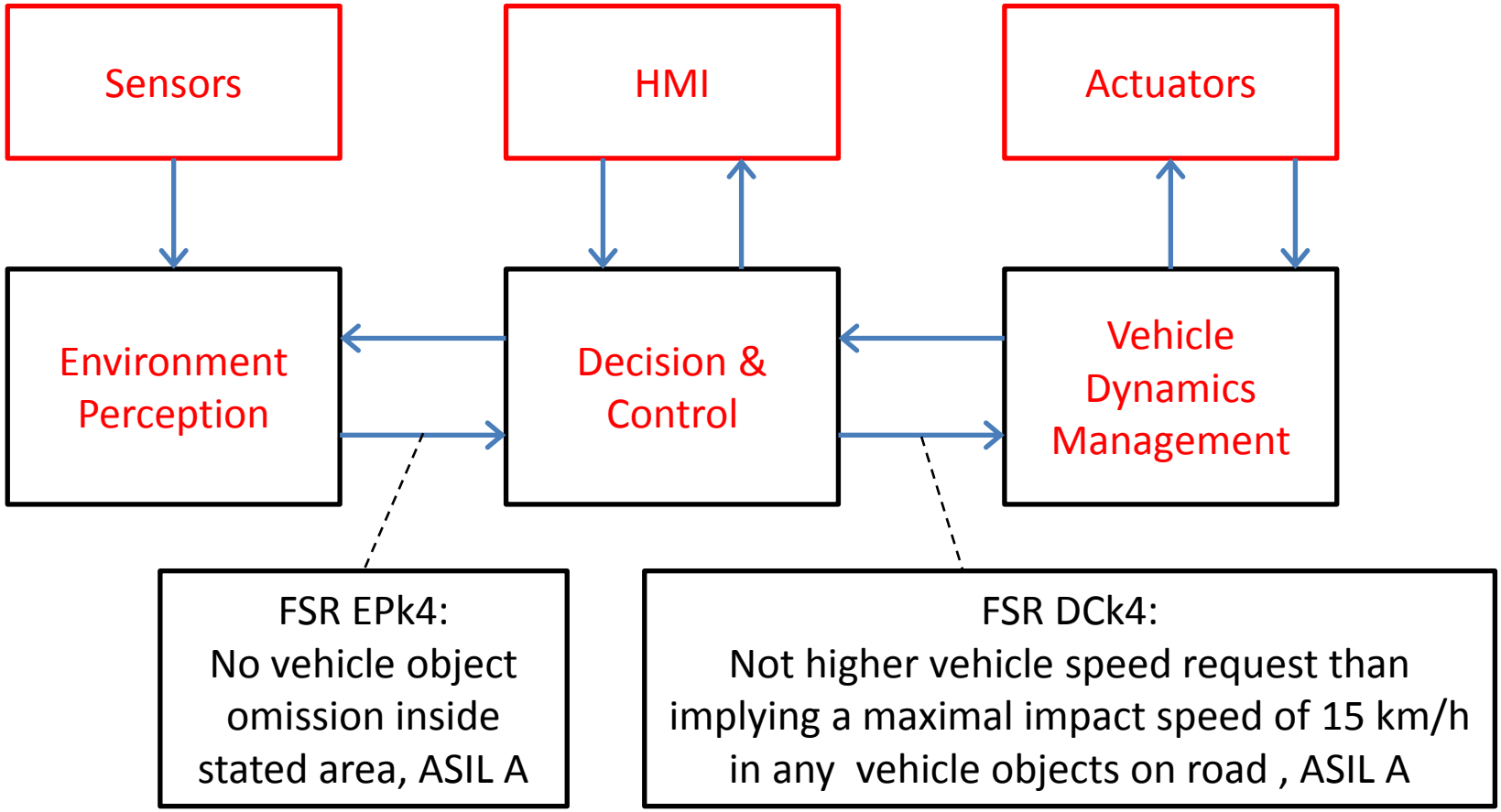
Functional Safety Concept Architecture

SG k3:
Do not collide with a higher impact speed than 25 km/h with a vehicle being on the road in front of ego vehicle, ASIL B

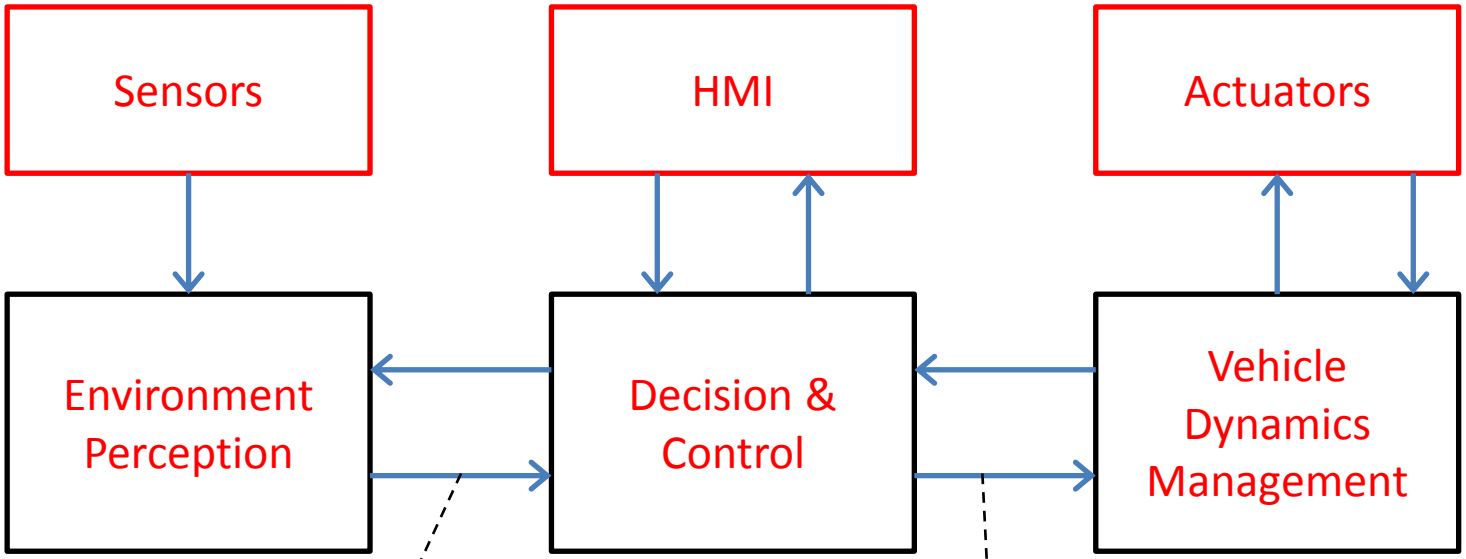


Functional Safety Concept Architecture

SG k4:
Do not collide with a higher impact speed than 15 km/h with a vehicle being on the road in front of ego vehicle, ASIL A



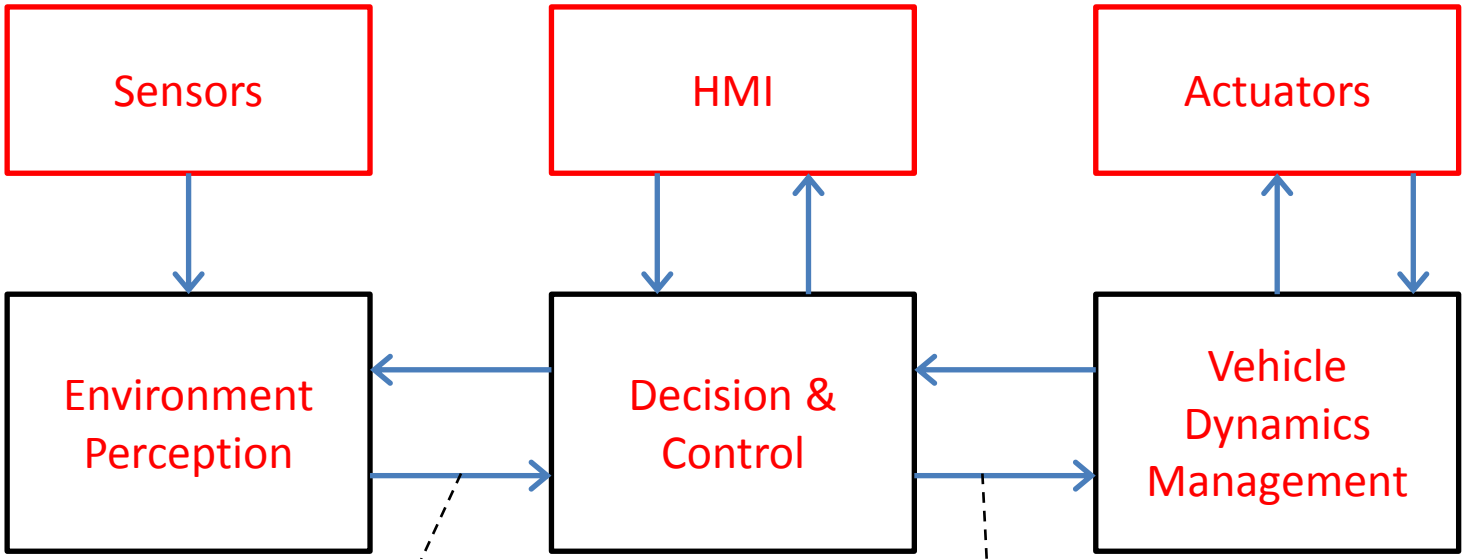
Example: DC assumes maximum brake retardation $a_b = 7\ m/s^2$ to apply if object detected in next moment



No vehicle object omission before:
30 m, ASIL D
40 m, ASIL C
50 m, ASIL B
60m, ASIL A

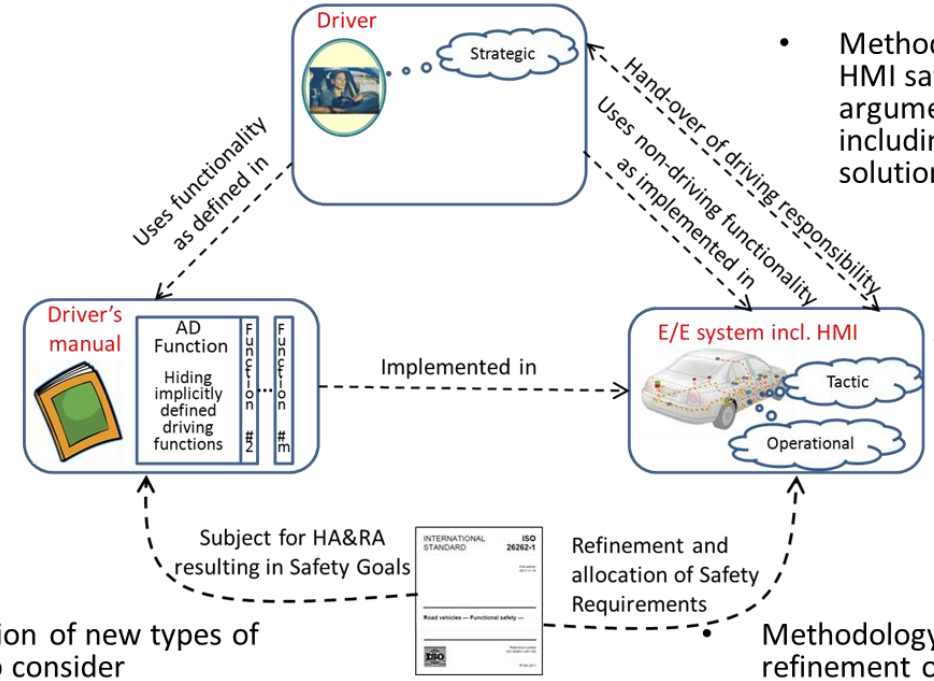
ASIL D → V_R < 98 km/h
ASIL C → V_R < 94 km/h
ASIL B → V_R < 98 km/h
ASIL A → V_R < 105 km/h

Example: DC assumes maximum brake retardation $a_b = 7\ m/s^2$ to apply if object detected in next moment



No vehicle object omission before:
20 m, ASIL D
21 m, ASIL C
22 m, ASIL B
23m, ASIL A

ASIL D → V_R < 88 km/h
ASIL C → V_R < 73 km/h
ASIL B → V_R < 67 km/h
ASIL A → V_R < 66 km/h



- Methodology for HMI safety argumentation, including specific solutions

- Architectural Pattern for Functional Safety Concept

- Identification of new types of Hazards to consider
- Methodology framework for Hazard Analysis and Risk Assessment
- Guidelines for detailed Hazardous Events including explicit tolerance margins

- Methodology framework for refinement of safety requirements
- Patterns for dividing safety requirements on FSC top level
- Formulation of the functional safety problem for a sensor fusion block
- Disarming of the Trolley problem paradox

All results will be presented:
September 23rd
Volvo Cars, PVH