TESACO

WE MAKE FUTURE MOBILITY SAFE AND RELIABLE.

A practical approach for the implementation of SOTIF requirements in ADS and ADAS development

FISITA Intelligent Safety Conference China

In collaboration with CHINA SAE

Udo Steininger
Managing Director

FISITA ISCC 2025
Xi’an, 2025 Sept. 13 - 14

Content

1 **Introduction**

2 SOTIF Requirements for Level 4 ADS for People & Goods Movers (Case Study)

3 Expected SOTIF Requirements for future ADAS Development

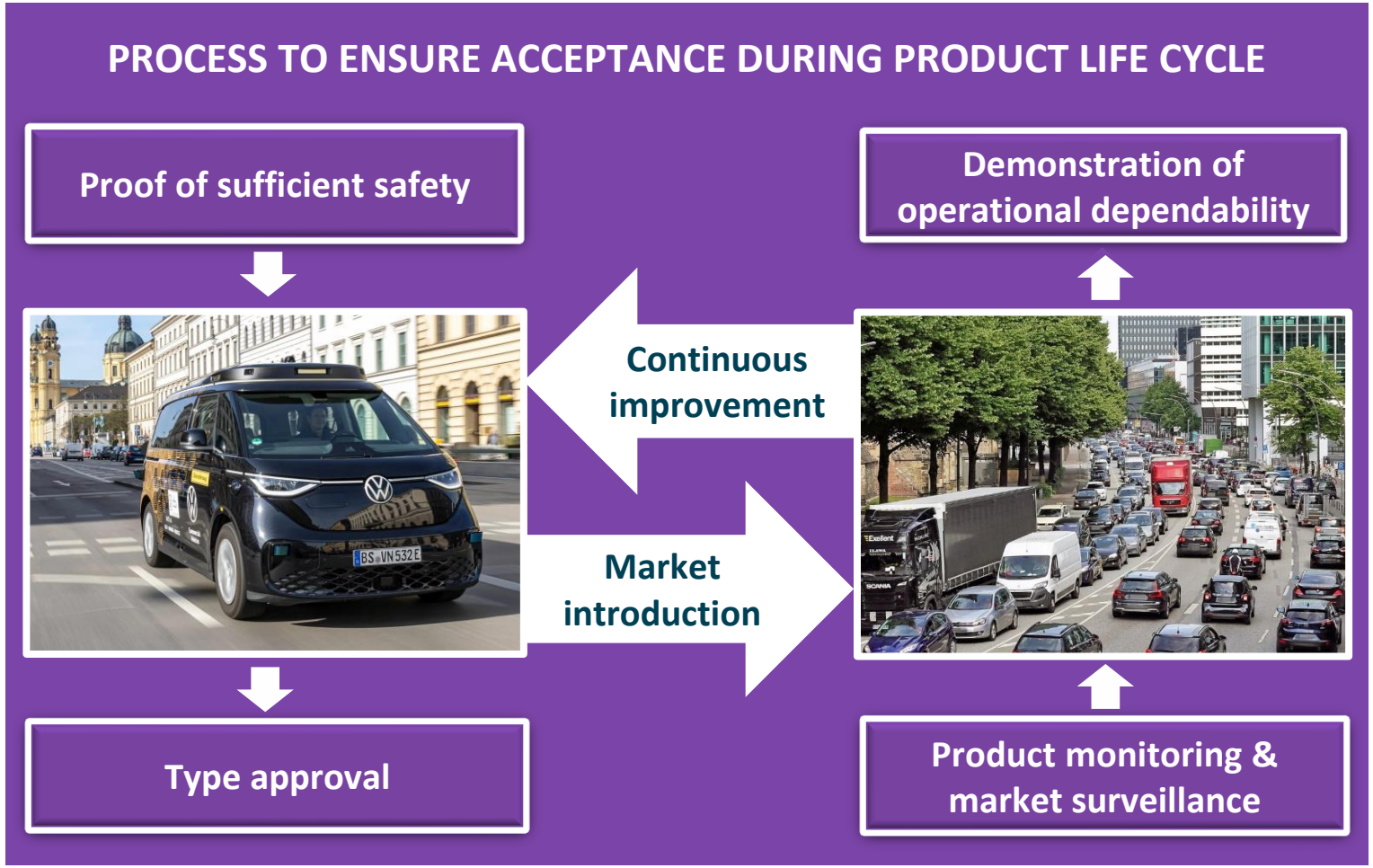
4 Resume & Outlook

ADS & ADAS safety lifecycle

National regulations, EU implementing regulation and UNECE regulations for **fully automated and autonomous driving,** i.e., SAE level 3 & 4, explicitly requires consideration of

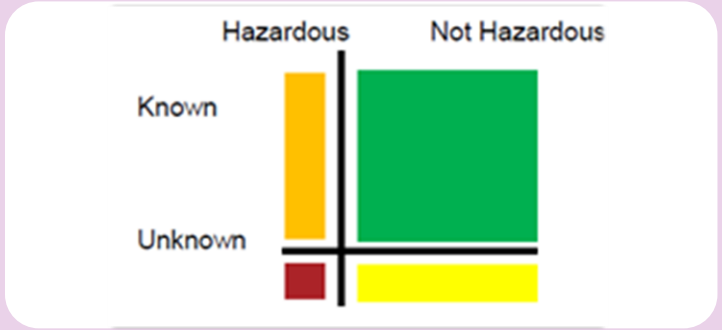
- ISO 26262 for functional safety
- **ISO 21448 for SOTIF**
- ISO/SAE 21434 for cybersecurity

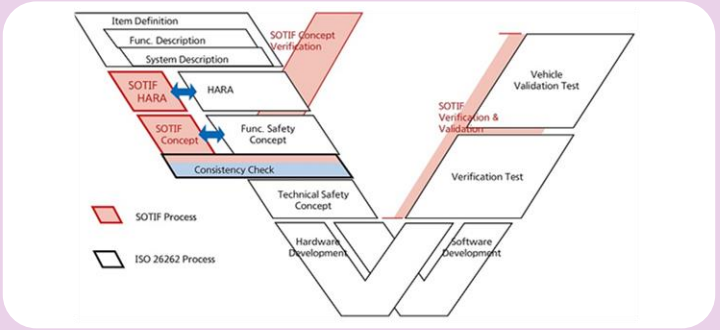
Currently **no comparable SOTIF requirements in ADAS regulations**



© Volkswagen, dpa / Soeren Stache

SOTIF application phases for ADS & ADAS





© Intel, AZT

Method Development

(responsibility of, o.a., standardization boards)

Sufficient safety = argument for positive risk balance + only technically unavoidable residual risks remaining

System Development

(responsibility of manufacturer & supplier)

Practical approach for implementation of SOTIF requirements in ADS and ADAS development

System Deployment

(responsibility of manufacturer & authorities)

Improved product monitoring and market surveillance to demonstrate operational dependability

Content

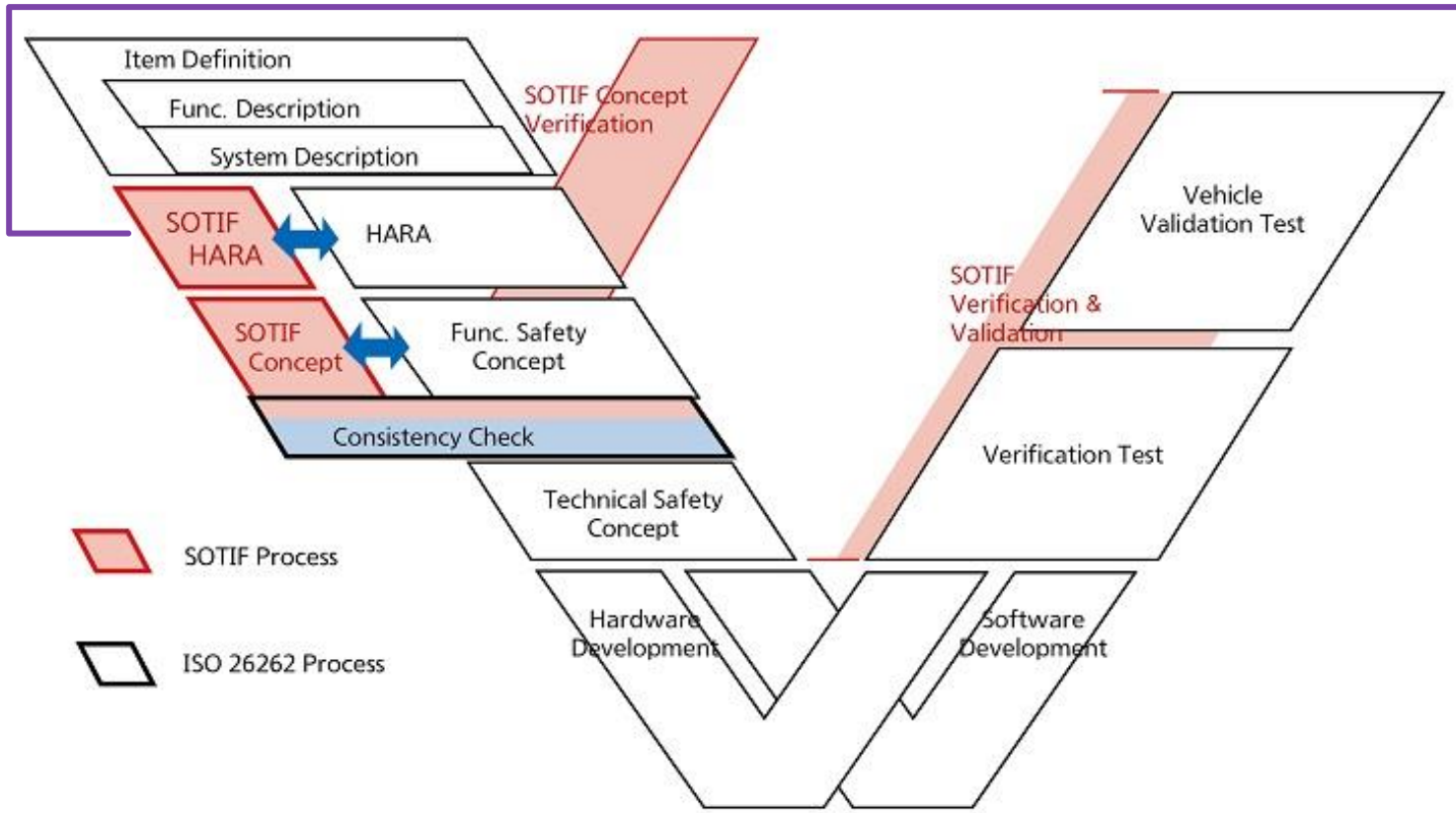
1 Introduction

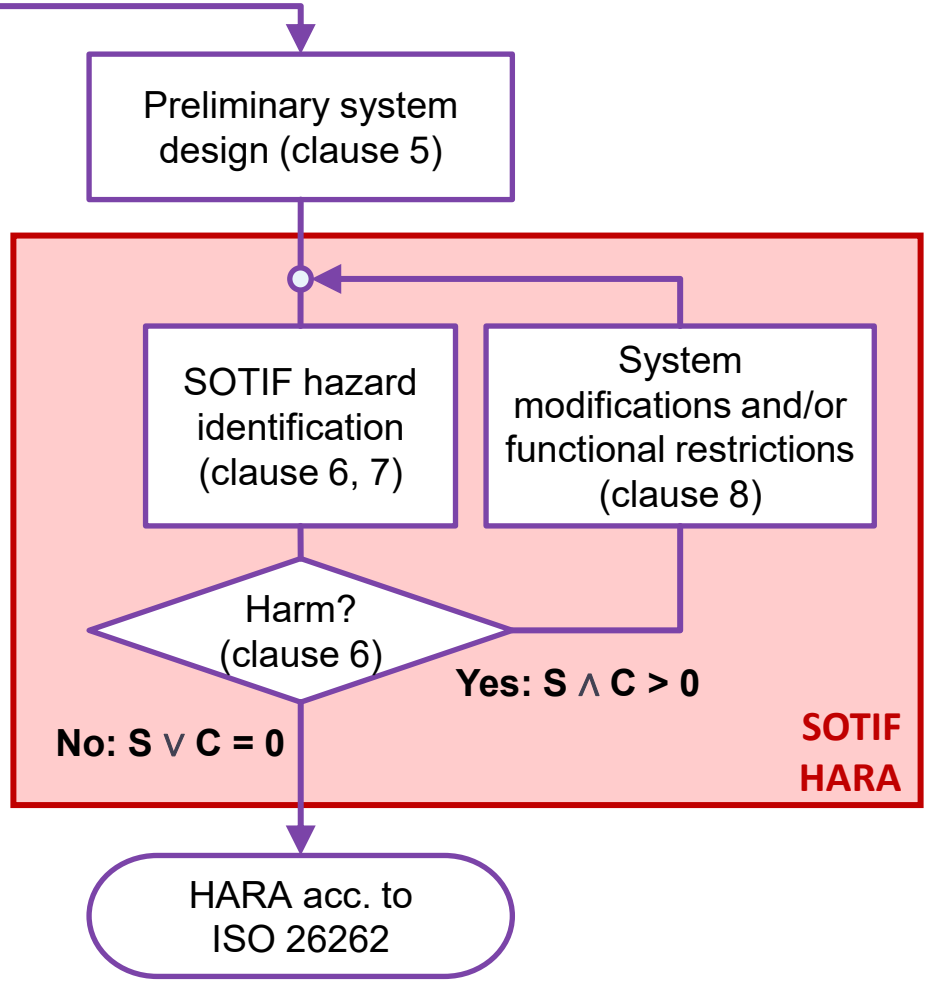
2 **SOTIF Requirements for Level 4 ADS for People & Goods Movers (Case Study)**

3 Expected SOTIF Requirements for future ADAS Development

4 Resume & Outlook

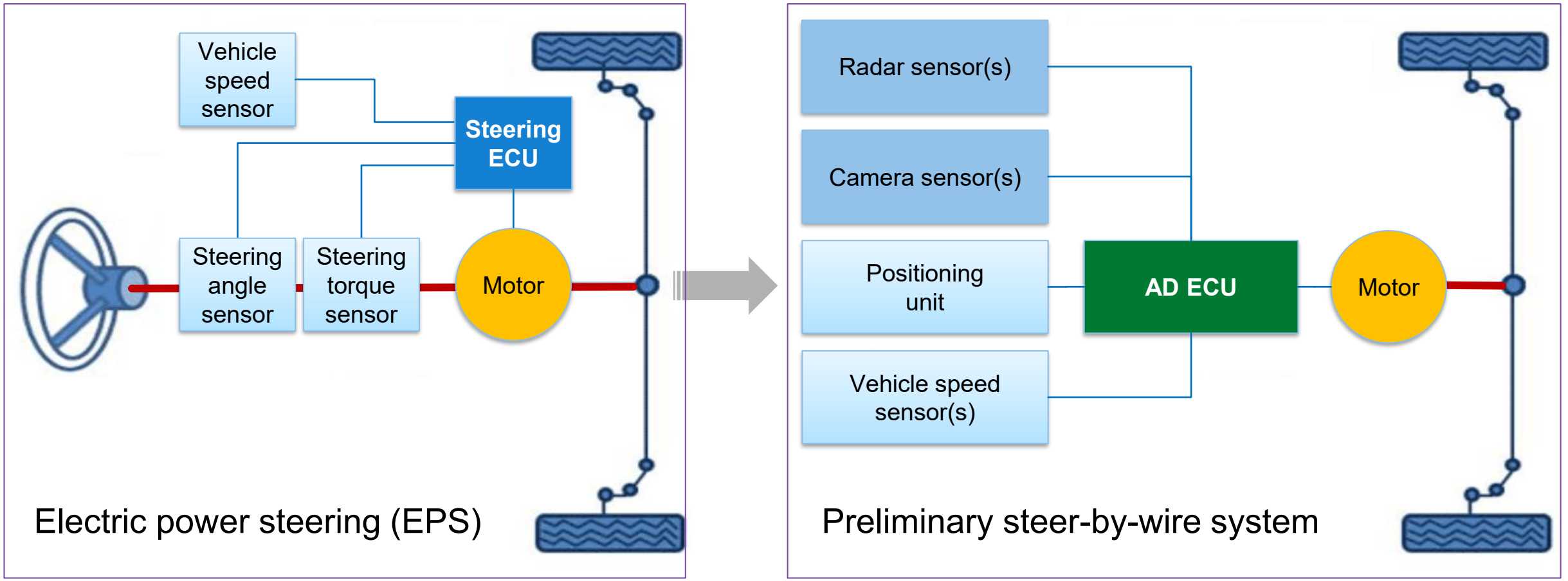
SOTIF integration into comprehensive safety lifecycle





R. Mariani: Can we trust autonomous systems? ICRI-CARS, Oct. 17, 2017
http://www.icri-sc.org/fileadmin/user_upload/Group_VCI/Events/Kickoff_2017/Mariani_Intel_ICRI-CARS_kickoff_v1.pdf

Derivation of preliminary steer-by-wire for level 4



Is preliminary system design free of SOTIF hazards / harms?

Example SOTIF hazard caused by Performance Insufficiency (PI)

PI SOTIF hazard: False positive or false negative recognition / misinterpretation of objects caused by limitations of environmental perception sensor systems results in harm

Preliminary system design: Use of typical sensor set from ADAS and 1st generation of level 3 systems

- 3D-rardar systems are very powerful in object detection but less suitable for classification (low resolution, not able to distinguish between beverage can and road vehicle)

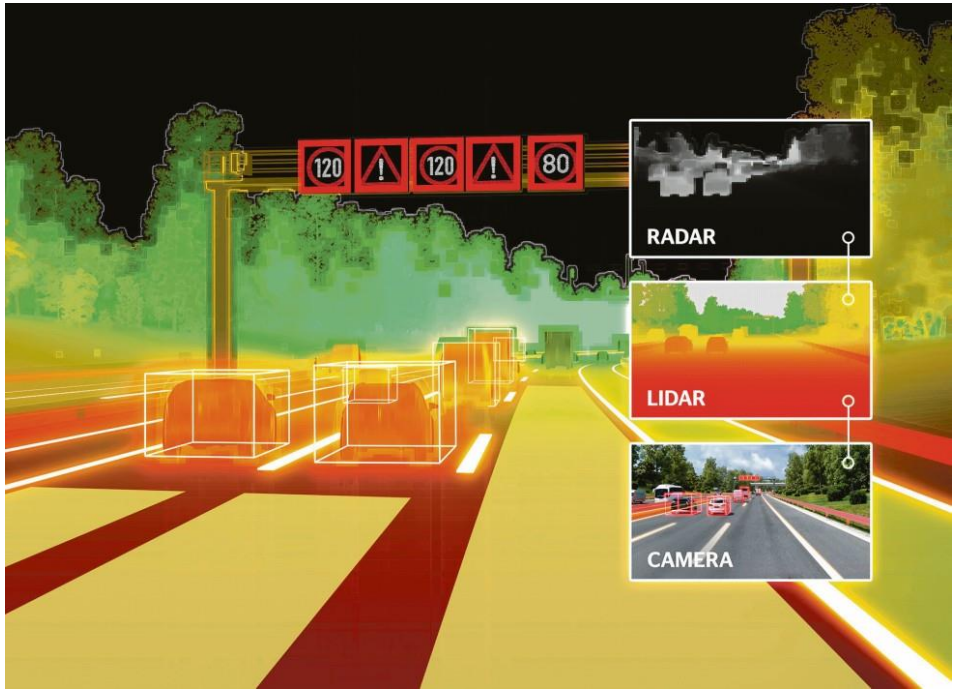
- Camera systems are very powerful for object classification but less suitable for detection (e.g., in absence of contrast or at reduced visibility)

Example SOTIF hazard caused by Performance Insufficiency (PI)

System modification: Improvement of environmental perception

- Implementation of a partial redundant / diverse sensor system that bridge the gap in performance between radar and camara systems, usually **lidar**

- Alternatives, e.g.,
  - ➢ Substitution of 3D-radar by 4D-/full-range-radar with high resolution
  - ➢ Improvement of sensor data fusion, e.g., using AI algorithms



Example SOTIF hazard caused by Insufficient Specification (IS)

IS SOTIF hazard: Single point failure vulnerability caused by 1oo1 design results in harm

- Safety of conventional EPS based on human driver intervention in combination with mechanical connection between steering wheel and steered wheels by steering column in case of failure in E/E system
  - ➢ Deactivation of EPS in case of failure provides a safe state
  - ➢ High safety integrity (ASIL D) only necessary for avoidance of unintended self steering, not for actual EPS function (typically ASIL B)
  - ➢ 1oo1 fail-safe sufficient for human driving
- Without human driver and steering column, single point failures of elements (sensors, ECU, actuator) or power supply results in failure / loss of steering function
- **According to ISO 21448, 1oo1 fail-safe design is insufficient for driverless level 4 vehicles**

Example SOTIF hazard caused by Insufficient Specification (IS)

System modification: Redundancy

- To achieve fail-operational design, full 2oo3 architecture would be necessary
- Typical fields for application of full 2oo3 architectures are passenger aircrafts or nuclear power plants
- Systems are very cost-, space- and energy-intensive and lead to high complexity of entire E/E architecture → not applicable / useful for road vehicles
- For advanced level 3 and 1st generation of level 4 systems, fail-degraded design will prove adequately (see backup slide for definition of fault tolerance regimes + reference)

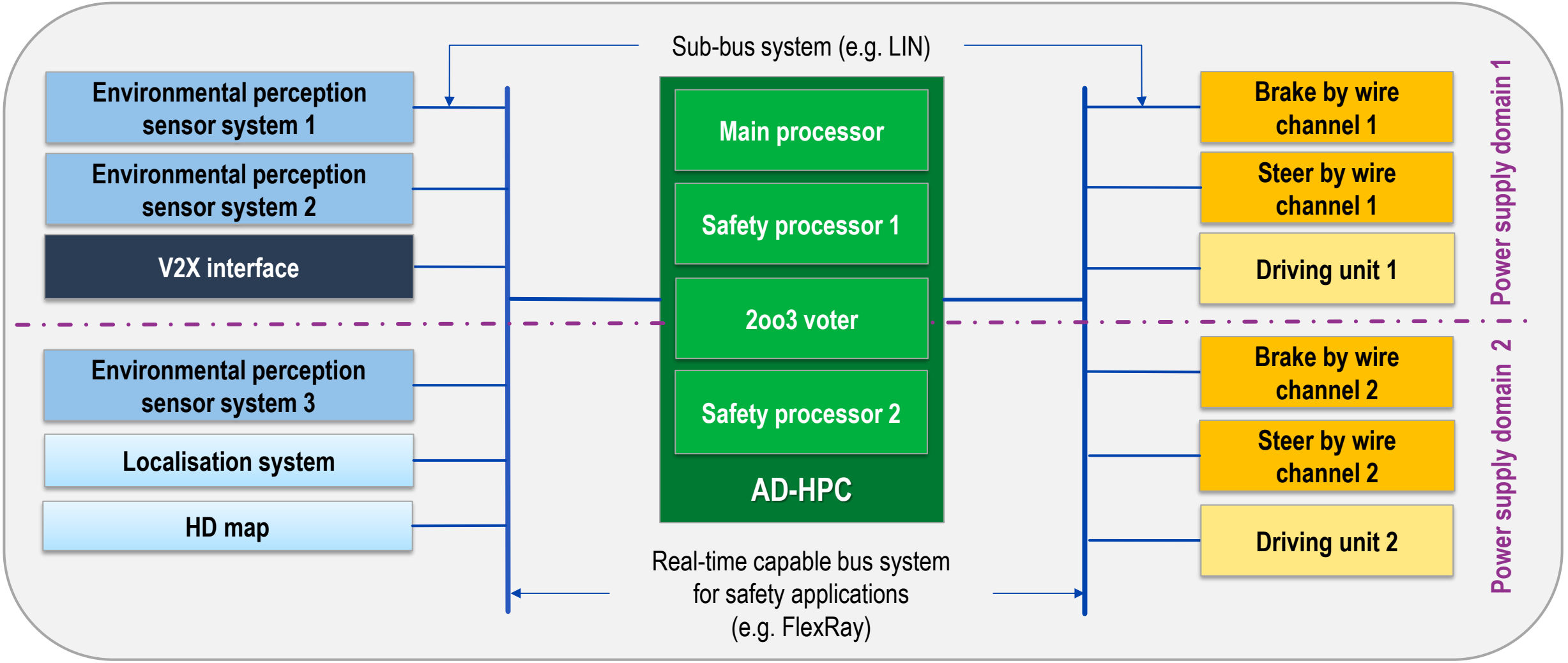
ADS design features for driverless level 4 vehicles

Comprehensive HARA (considering SOTIF & functional safety) results in an **ASIL D capable** and **fail-degraded** ADS with

- 3 independent partial redundant / diverse environmental perception sensor systems
- AD high-performance computer (AD-HPC) with 3 independent processing channels - e.g., 1 main processor, 2 safety processors - and a 2oo3 voting function
  - ➢ Main processor with comprehensive performance and low / no safety integrity (QM)
  - ➢ Safety processors with lower performance and high safety integrity (to achieve ASIL D for overall system, both channels could have ASIL B(D))
  - ➢ Voter needs to have overall safety integrity, i.e., ASIL D in this example
- Double-redundant power supply, drive-by-wire systems and drive units

(Note: Point to point connections of preliminary system design substituted by bus systems)

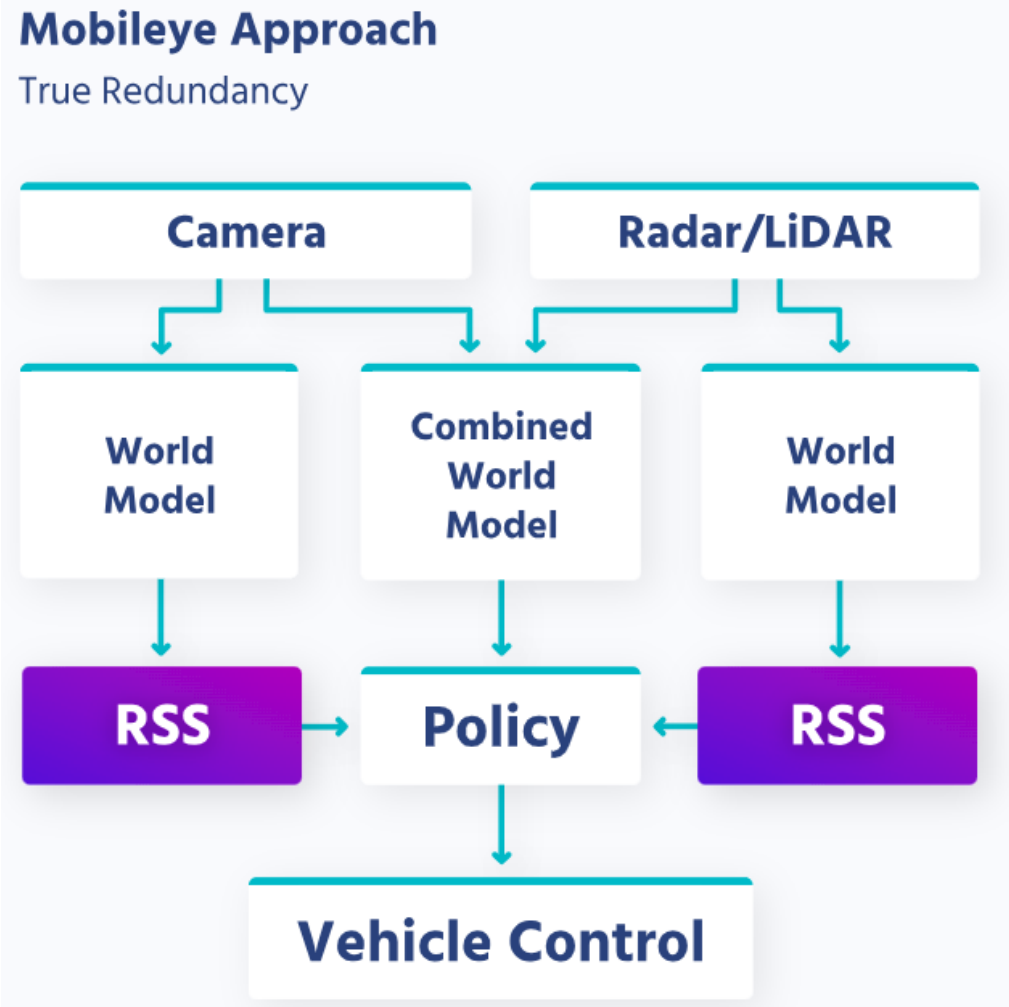
Generic block diagram for driverless level 4 vehicles



Comparison with current SDS by Mobileye

- Partial redundant / diverse sensors
- 3 diverse “world models”
- Responsibility-Sensitive Safety (RSS), made up of formal logic and mathematical models, adheres to five safety rules:
  - (1) Maintaining safe distance
  - (2) Avoiding reckless cutting-in
  - (3) Respecting right-of-way
  - (4) Being cautious in limited visibility
  - (5) Avoiding crashes

https://www.mobileye.com/solutions/drive/



Discussion / limitations of case study

- Using safety principles according to ISO 21448 & ISO 26262, it was possible to draw up an ASIL D capable fail-degraded ADS for driverless level 4 vehicles that provides justifiable effort and controllable complexity
- Objective of case study was to show that SOTIF principles generally work, some restrictions have been accepted therefore, e.g.
  - Environmental perception & steering has been taken as example, principles work for other systems, too - results were transferred to complete ADS
  - Limitation to concept development phase, SOTIF principles have to be adopted in verification and validation phase (shown on slide 6) as well as in operation
  - Focus on how to deal with insufficiencies, neither systematic approach for SOTIF hazard identification has been shown (see backup slide for use of STPA) nor SOTIF argumentation / absence of unreasonably risk (discussed in detail in ISO 21448)

Content

1. Introduction
2. SOTIF Requirements for Level 4 ADS for People & Goods Movers (Case Study)
3. **Expected SOTIF Requirements for future ADAS Development**
4. Resume & Outlook

SOTIF requirements for lower levels of automation

- Starting from level 4 case study, we expect with **decreasing** SAE level that requirements to
  - ➢technical system **decrease**
  - ➢human actors **increase** (Note: For driverless level 4 vehicles there are no requirements to driver but there are, e.g., requirements to staff of technical supervision)

- There are SOTIF requirements in national regulations for autonomous driving, in EU implementing regulation 2022/1426 for fully automated driving as well as in UN regulations for level 3 systems but **not** in UN regulations **for level 2 systems**

SOTIF requirements for ADAS according to ISO 21448

- ISO 21448 addresses level 2 and gives examples how to identify level 2 SOTIF hazards
  - "Hazards can be triggered by … reasonably foreseeable misuse of the intended functionality. … Therefore, a proper understanding by the user of the functionality, its behavior and its limitations (including the human/machine interface) is essential to ensure safety."
  - "Derived hazardous misuse scenario: Driver does not take over control of the vehicle … because the driver does not know the meaning of the warning."
  - "The intended behavior specified by the developer, while not representing unreasonable risk, might not match the driver's expectation of the system behavior."

- Methodological approach for level 2 is largely identical to level 4 approach:
  - Hazard identification with focus on **insufficiencies of driver performance** and **HMI**
  - Comprehensive HARA (SOTIF + functional safety)
  - System modifications and/or functional restrictions + **restrictions for presentation of systems**

Expected SOTIF requirements for ADAS

Considering current accidents with ADAS and subject to detailed further analyses, following SOTIF requirements can be expected for future development and approval of ADAS

- Suitable management of user expectations → in particular, avoidance of wrong expectations caused by unsuitable labelling or advertising promises
- Effective monitoring of user attention → active driver monitoring system vs. simple hands-off detection, also and especially for hands-off ADAS
- Timely and appropriate intervention by technical systems → warnings >>> takeover request >>> measures for hazard avoidance
- Clear HMI presentation → capabilities and limitations of the systems and required user interventions

Content

1. Introduction
2. SOTIF Requirements for Level 4 ADS for People & Goods Movers (Case Study)
3. Expected SOTIF Requirements for future ADAS Development
4. **Resume & Outlook**

Resume

- In recent years, problems have often been described rather than solutions offered by SOTIF standardization committees
- This lesson attempts to demystify the topic and provides practical solution for integration of SOTIF in a comprehensive safety consideration
- Regulation for level 3 and 4 ADS requires compliance with ISO 21448 and ISO 26262
- As an example, a comprehensive HARA - considering SOTIF & functional safety - was carried out for ADS of driverless level 4 vehicles
- It results in E/E architecture with
  - ASIL D capability
  - fail-operational design

Outlook

- Although there are no SOTIF requirements in recent level 2 regulations, the approach can be used for future ADAS development and approval, too
- Considering current accidents, requirements can be expected regarding
  - Avoidance of wrong expectations on the part of users
  - Effective monitoring of user attention
  - Timely and appropriate intervention by technical system and
  - Clear HMI presentation of system capabilities & limitations and required user interventions
- Further methodological development must deliver more practicable standards and guidelines to ensure that sufficient safe systems are developed and placed on the market
- Operational dependability must be demonstrated by improved approaches and methods in product monitoring and market surveillance

Thank you for your time.
Are there any questions?

WE MAKE FUTURE MOBILITY SAFE AND RELIABLE.

Udo Steininger

Managing Director

TESACO GmbH

Schloßlände 26

85049 Ingolstadt

+49 160 3601992

udo.steininger@tesaco.eu

www.tesaco.eu

Backup: Fault tolerance regimes

According to Stolte et al., the following definitions of fault tolerance regimes are relevant for automated driving systems: In the presence of a fault combination, a system is …

- **fail-safe** if it ceases its specified functionality and transitions to a well-defined condition to maintain a safe state,
- **fail-degraded** if it can provide its specified functionality with below nominal performance while maintaining a safe state,
- **fail-operational** if it can provide its specified functionality with nominal performance while maintaining a safe state.

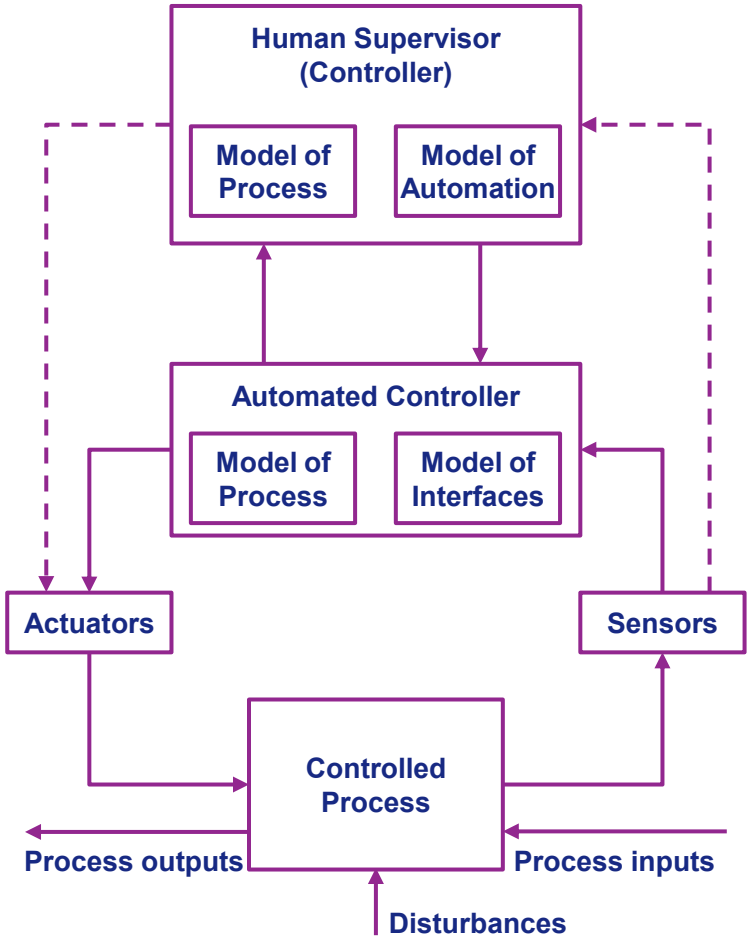
T. Stolte, S. Ackermann, R. Graubohm, I. Jatzkowski, B. Klamann, H. Winner, and M. Maurer (2022). A Taxonomy to Unify Fault Tolerance Regimes for Automotive Systems: Defining Fail-Operational, Fail-Degraded, and Fail-Safe. IEEE Transactions on Intelligent Vehicles, vol. 7, no. 2, pp. 251–262, DOI: 10.1109/TIV.2021.3129933

Backup: STPA Method

- The STPA (System Theoretical Process Analysis) is an analysis method based on the control flow of a system and can be applied for different purposes incl. SOTIF

- Benefits of the method:
  - Social and organizational factors can be included
  - First application even before the initial architecture is available
  - More emphasis on human errors compared to other methods
  - Supports deeper understanding of causal factors leading to a hazardous event

- For SOTIF specifically the STPA can be applied to identify misuse scenarios as well as triggering events leading to SOTIF hazards



Backup: Integration of STPA in the SOTIF lifecycle