A systematic approach based on STPA
for developing a dependable architecture for fully automated driving

ESW 2016, Zürich, September 24th 2016

Daniel Lammering and Asim Abdulkhaleq

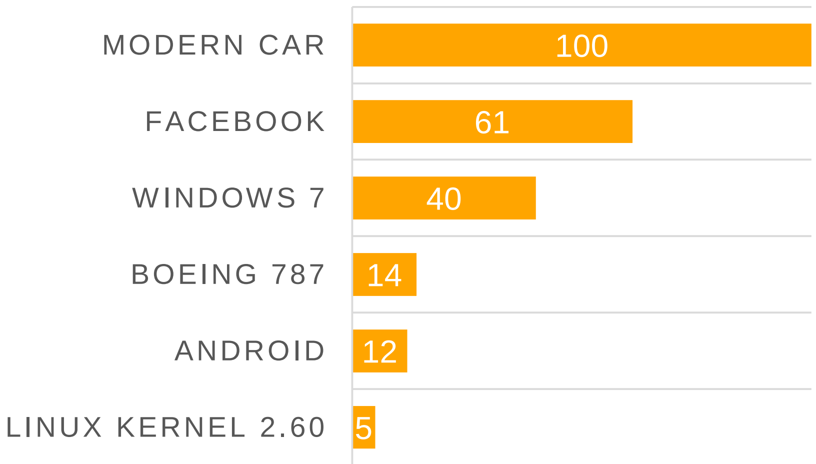
University of Stuttgart
Germany

Automated Driving Architecture
Agenda

1. **Motivation**
2. Challenges: Fully Automated Driving
3. Proposed Approach
4. Results
5. Conclusion & Future Work

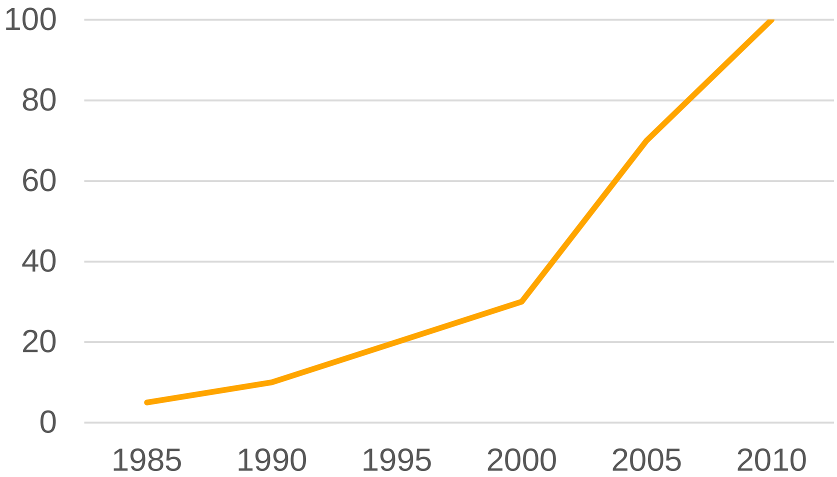
Motivation
Current and upcoming challenges

Million Lines of Code



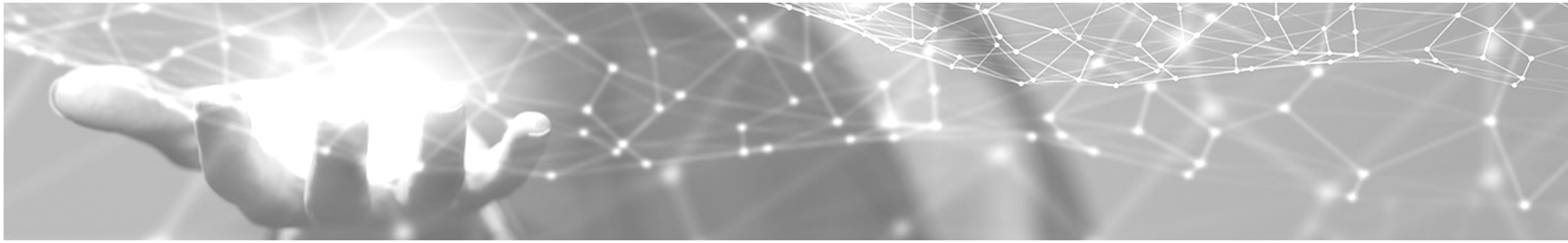
Numbers from 2014

Number of ECUs



Software and architecture complexity

Safety-driven Design



Why paradigm change?

- Old approaches becoming less effective
  (FTA / FMEA focus on component failures)
- New causes of accidents not handled
  (interaction accidents / complex software errors)

Component reliability
(component failures)

Systems thinking
(holistic View)

e.g. **Automated Driving**

- Many parallel interactions between components!

- Accidents happen with no component failures
  (Component Interaction Accidents)
- Complex, Software-intensive Systems
  (New Hazards: System functional **but** Process/Event is unsafe)

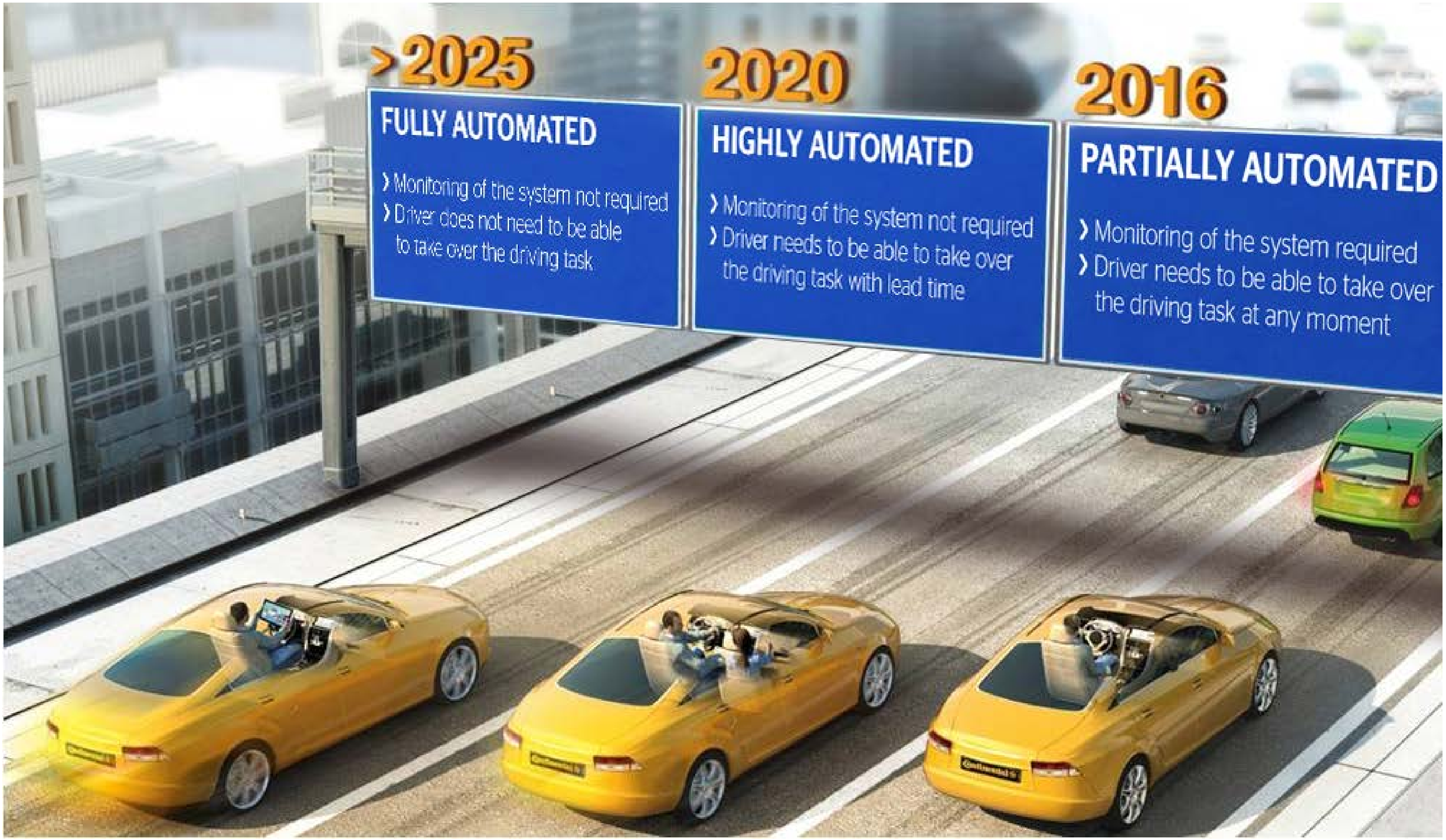
Automated Driving Architecture

Agenda

1. Motivation
2. **Challenges: Fully Automated Driving**
3. Proposed Approach
4. Results
5. Conclusion & Future Work

Automated Driving

A revolutionary approach in evolutionary steps



Automated and Autonomous Driving

SAE Definitions on Automation Levels

SAE level	SAE name	SAE narrative definition	Execution of steering and acceleration/ deceleration	Monitoring of driving environment	Fallback performance of *dynamic driving task*	System capability (*driving modes*)	BASt level
***Human driver* monitors the driving environment**							
0	**No Automation**	the full-time performance by the *human driver* of all aspects of the *dynamic driving task*, even when enhanced by warning or intervention systems	Human driver	Human driver	Human driver	n/a	Driver only
1	**Driver Assistance**	the *driving mode*-specific execution by a driver assistance system of either steering or acceleration/deceleration using information about the driving environment and with the expectation that the *human driver* perform all remaining aspects of the *dynamic driving task*	Human driver and system	Human driver	Human driver	Some driving modes	Assisted
2	**Partial Automation**	the *driving mode*-specific execution by one or more driver assistance systems of both steering and acceleration/deceleration using information about the driving environment and with the expectation that the *human driver* perform all remaining aspects of the *dynamic driving task*	**System**	Human driver	Human driver	Some driving modes	Partially automated
***Automated driving system* ("system") monitors the driving environment**							
3	**Conditional Automation**	the *driving mode*-specific performance by an *automated driving system* of all aspects of the *dynamic driving task* with the expectation that the *human driver* will respond appropriately to a *request to intervene*	System	**System**	Human driver	Some driving modes	Highly automated
4	**High Automation**	the *driving mode*-specific performance by an *automated driving system* of all aspects of the *dynamic driving task*, even if a *human driver* does not respond appropriately to a *request to intervene*	System	System	**System**	Some driving modes	Fully automated
5	**Full Automation**	the full-time performance by an *automated driving system* of all aspects of the *dynamic driving task* under all roadway and environmental conditions that can be managed by a *human driver*	System	System	System	**All driving modes**	

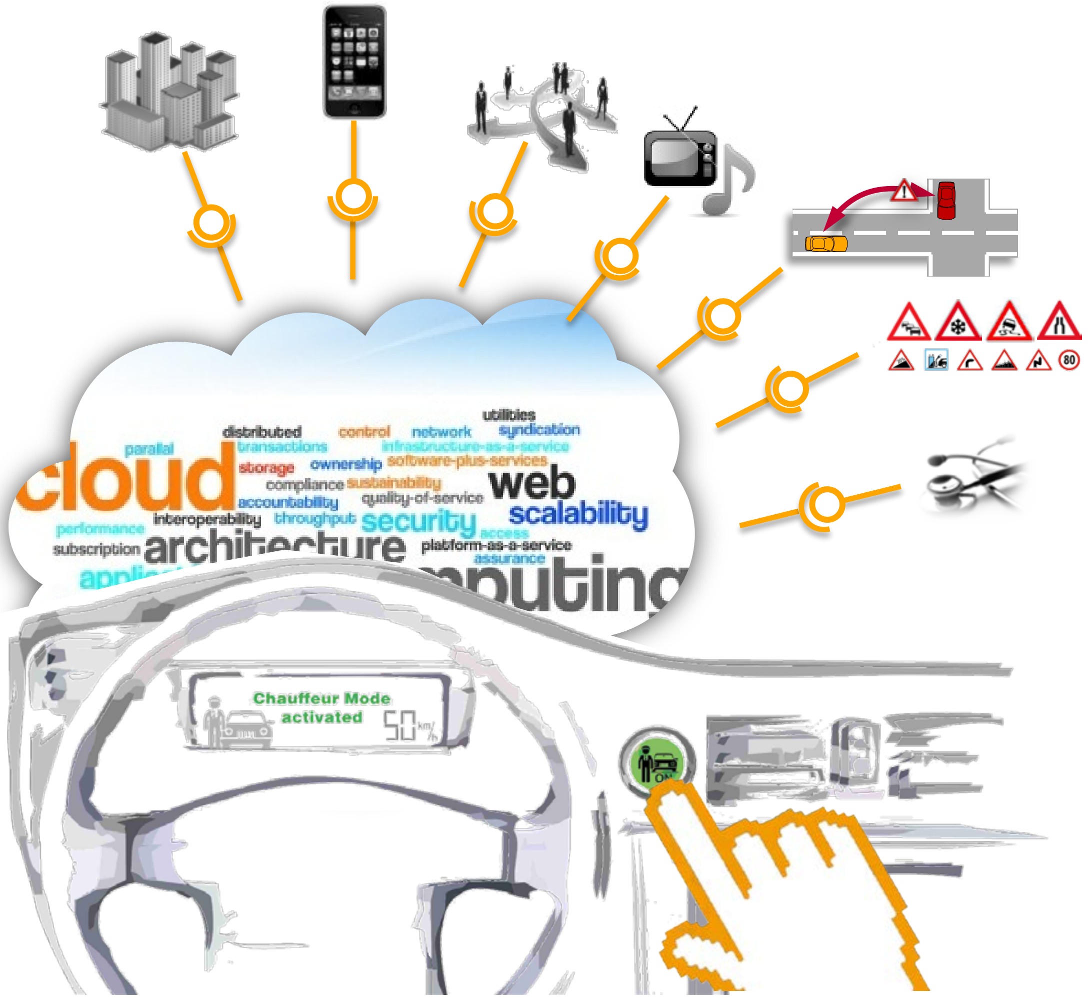
Automated Driving (levels 0–4)

Autonomous Driving (level 5)

The future of in-vehicle data management
Automotive part of the network

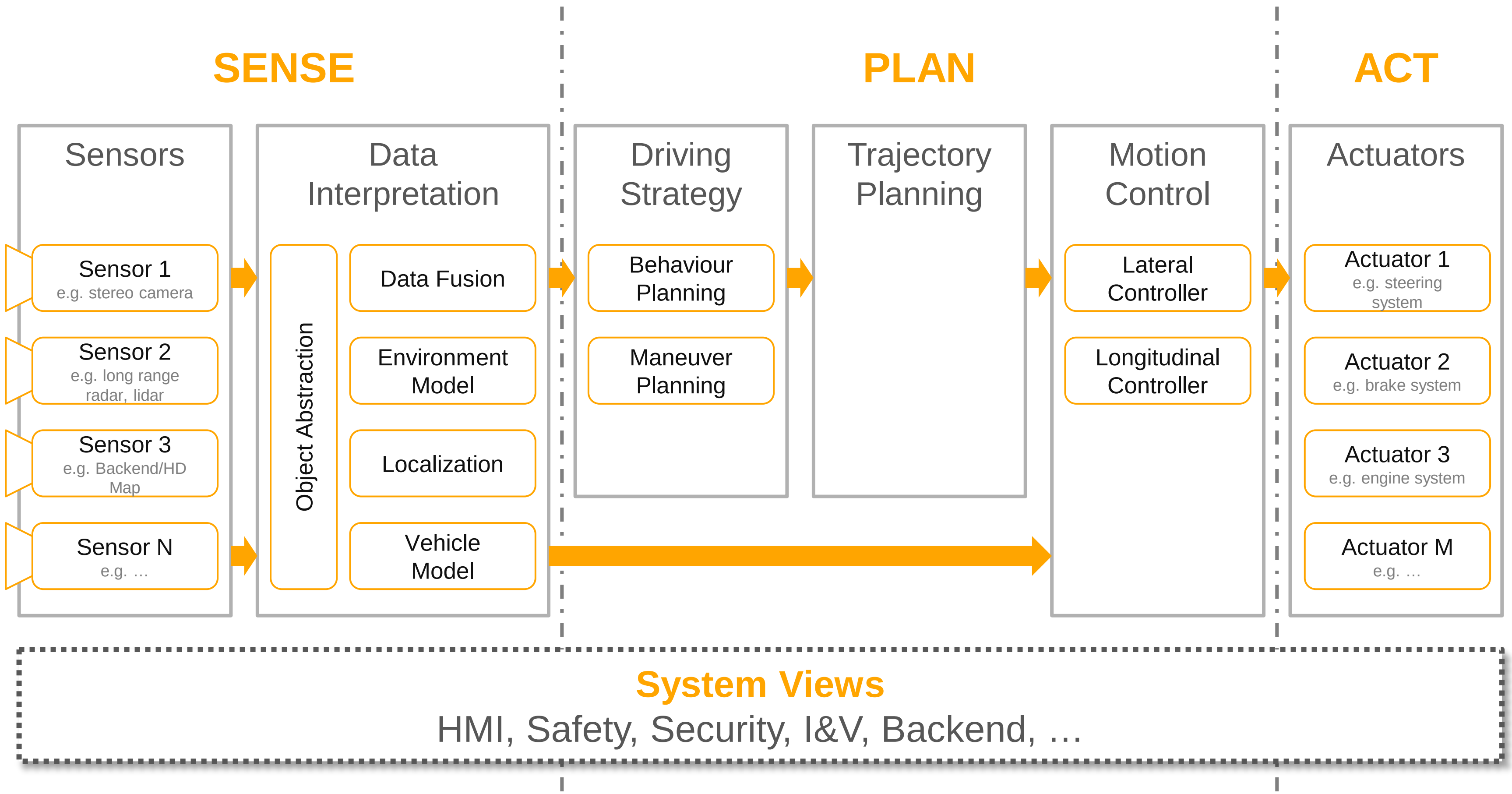
Vehicle E/E – Architecture
needs a holistic approach:

- Service Oriented Architectures
- Secure Connections
- Cloud services / Backend
- Software *Update over the Air*



A System View on Autonomous Driving

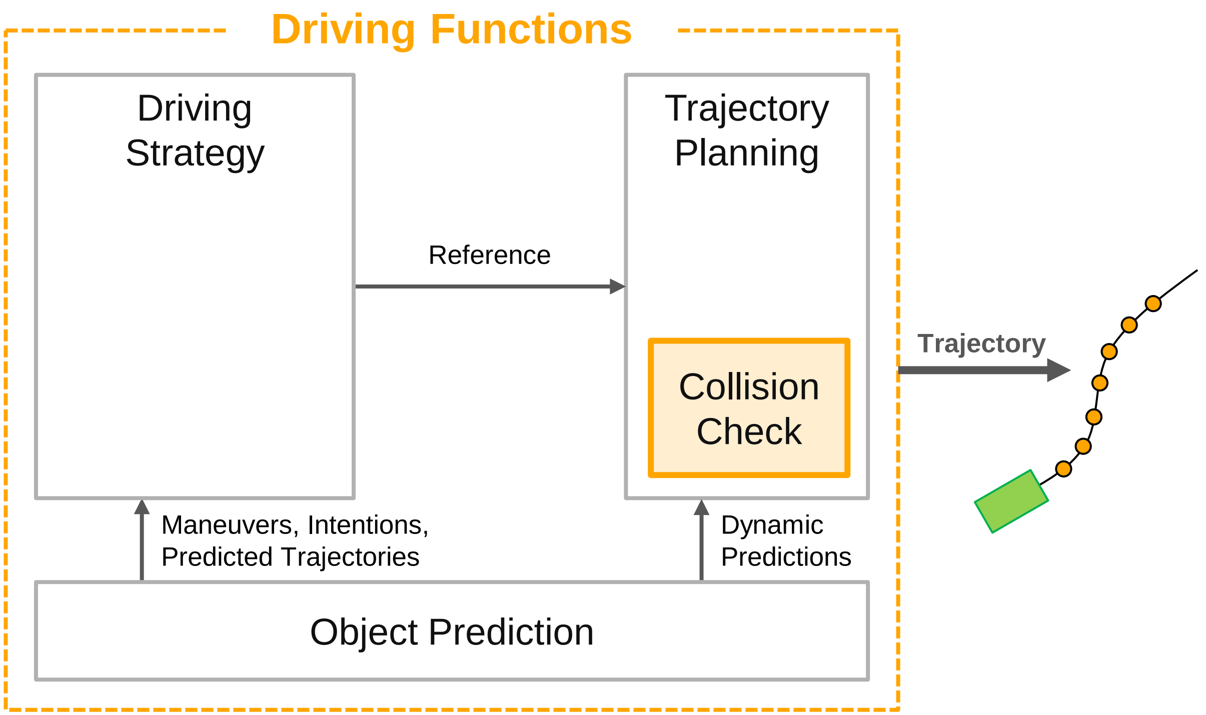
Functional Architecture



A System View on Automated Driving
Closer Look on Driving Functions

Environment Model
- Road Data
- Dynamic Objects
- Grid
- Map
- Situation

Vehicle Model
- Ego pose
- Ego dynamics
- Localization



Future Architecture Challenges

Growing Complexity – leads into stepwise change

Today
Component orientation

System orientation
Future

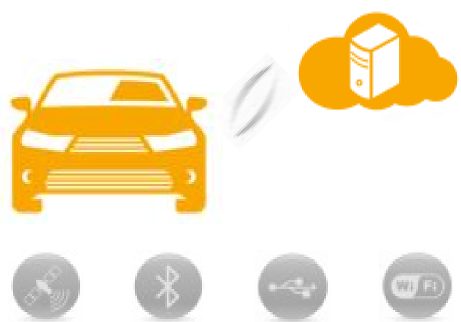
Distributed Architecture

Component Approach

Feature Update Rates
once a year [dealer's garage]

Domain Architecture

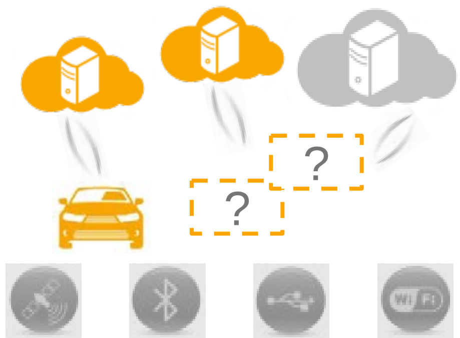
Multi Domain Approach



Feature Update Rates
monthly, weekly

Future Mobility Architectures

System Approach



Feature Update Rates
every time, everywhere

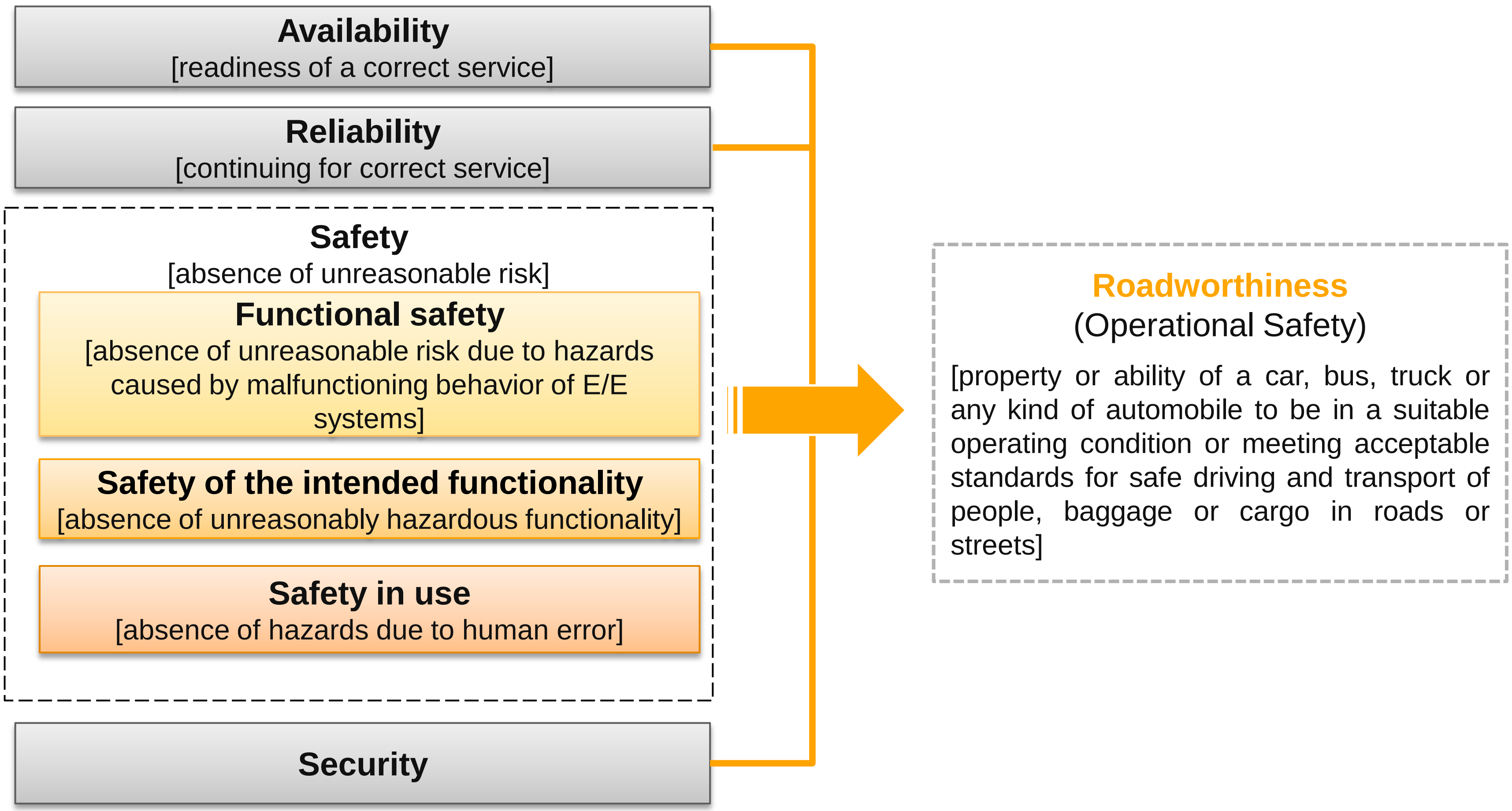
- Impact on customers and suppliers
- Impact on processes
- Impact on organizations
- Impact on business models…

Automated Driving Architecture
Agenda

1. Motivation
2. Challenges: Fully Automated Driving
3. **Proposed Approach**
4. Results
5. Conclusion & Future Work

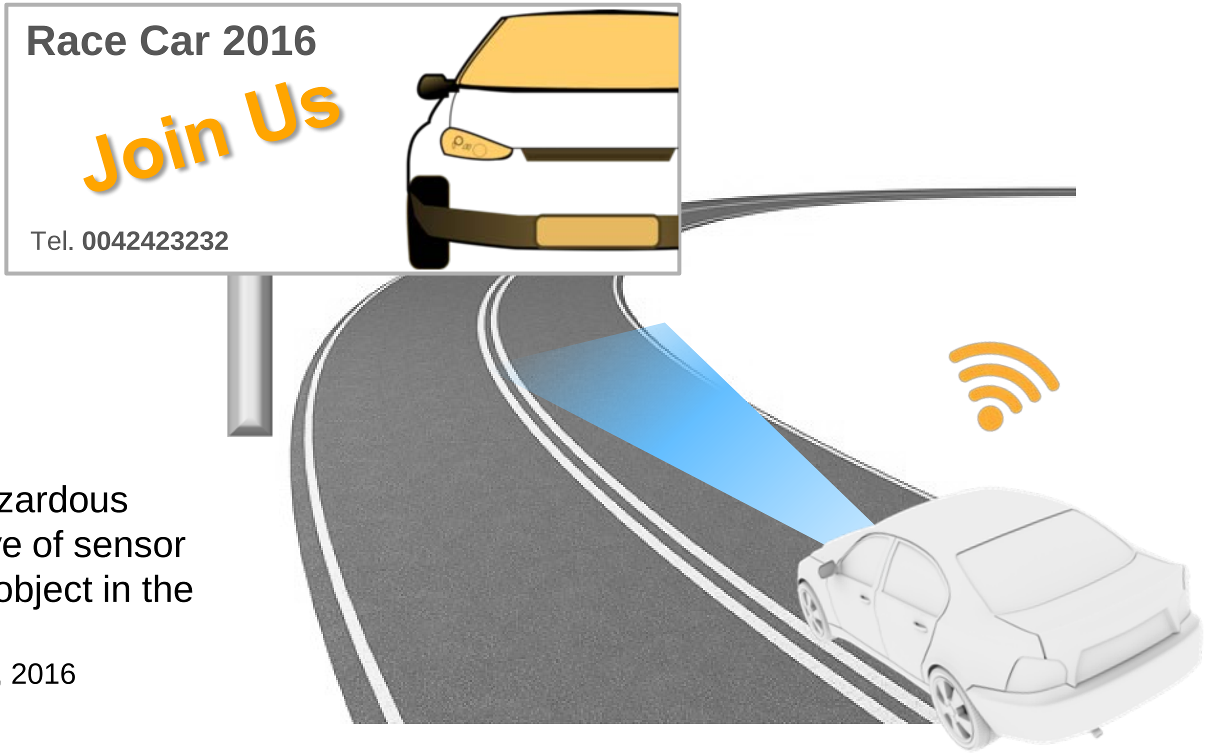
Operational Safety of The Fully Automated Vehicle

Ensuring a high level of operational safety of the fully automated vehicle



Safety of the intended functionality

A new aspect in safety of road vehicles



Definition

[absence of unreasonably hazardous functionality, e.g. false-positive of sensor performance to detect a real object in the lane]
working document at Continental AG, 2016

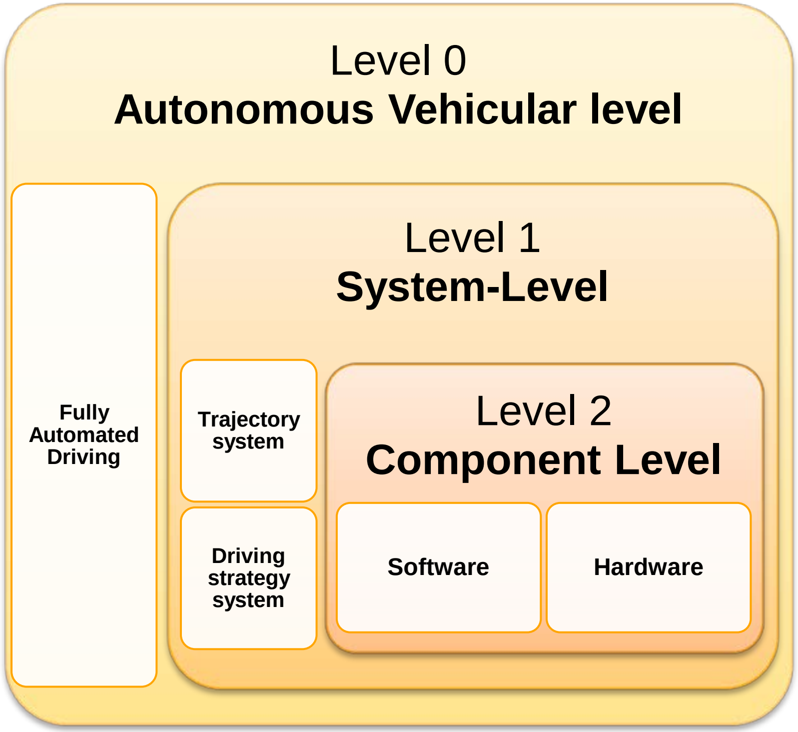
STPA-based Assessment Approach
Developing a dependable Architecture

- **Myth** *It's software—we can fix it later (add safety, security, other "-ilities")*
- **Fact** *"-ilities" must be architected in, and can't be easily added later*

[Boehm et al., 2002]

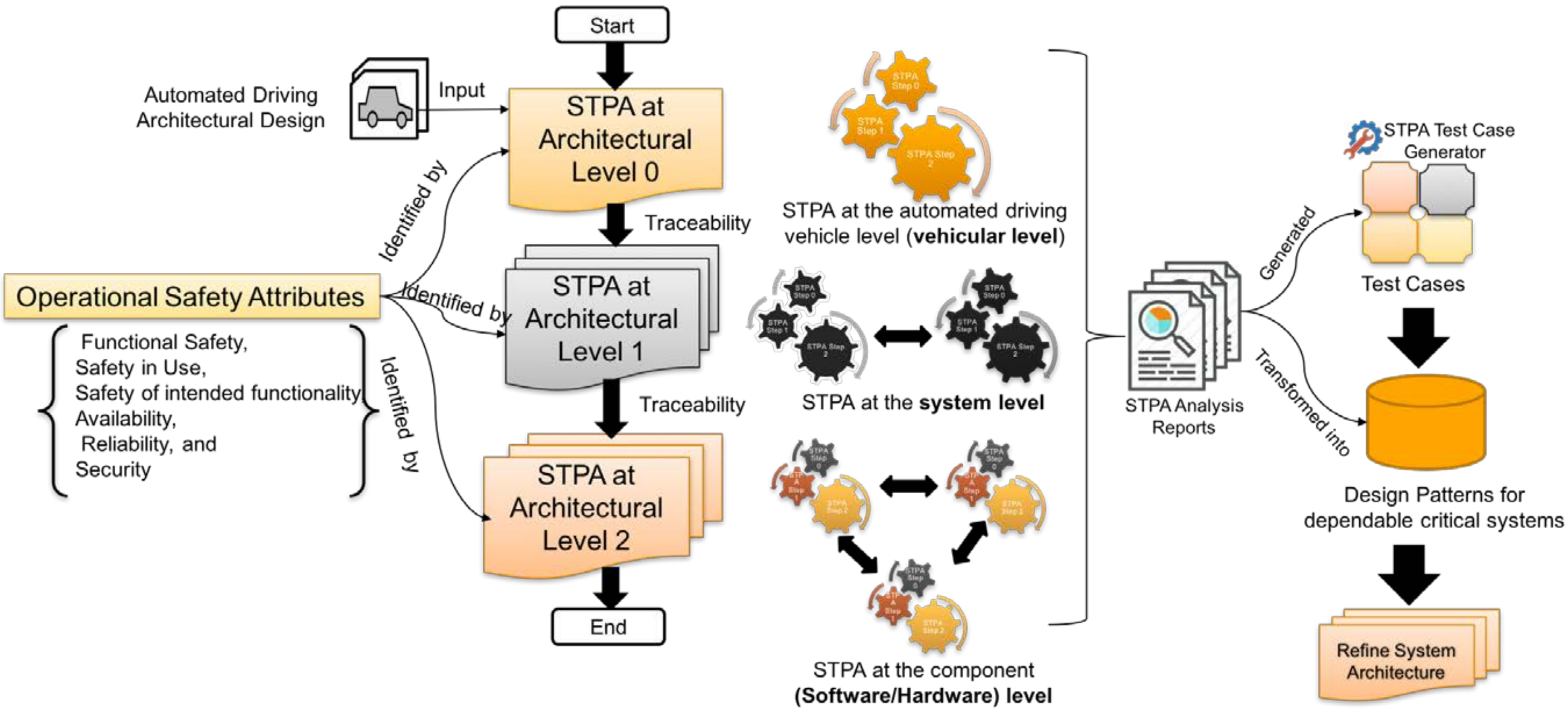
Our Approach

1. Decompose the architecture of fully automated driving
2. Apply STPA at each architecture levels
3. Develop an operational safety concept for fully automated driving
4. Generate test cases to evaluate the architectural design
5. Develop/Assign design patterns for dependable critical software systems



STPA-based Assessment Approach

Detailed View of the Proposed Approach



Automated Driving Architecture

Agenda

1. Motivation
2. Challenges: Fully Automated Driving
3. Proposed Approach
4. **Results**
5. Conclusion & Future Work

Operational Safety and Design Constraints

High Level Constraints for Fully Automated Driving Function

- We apply STPA to the autonomous vehicular level (Architectural level 0)
- We identify the operational safety and design constraints

ID	Operational Safety and Design Constraints
SR0.1	The AD vehicle shall be functional all the time, while it is active (**Reliability**)
SR0.2	The AD vehicle and its network shall be secured during driving task (**Security**)
SR0.3	The AD vehicle shall communicate with backend on a highly secure channel. (**Security**)
SR0.4	The AD vehicle data on the vehicle and backend should be available only to authorized personality (**Security**)
SR0.5	The AD vehicle shall drive safely and jerk optimized on the road (**Functional safety**)
SR0.6	The AD vehicle should react in all situations correct (**Safety of the intended functionality**)
SR0.7	The AD vehicle and its autonomous driving functions shall be ready for usage all the time (**Availability**)

Accidents
High Level Accidents which fully automated driving can lead to

- We identify 26 accidents which fully automated driving vehicle can lead to
- We assign the relevant operational safety attributes to each accidents

ID	Accident Description	Relevant Attributes**
ACC0.1	AD vehicle lost steering control and crashed into an object moving in front.	Sa, Su, Re
ACC0.2	AD vehicle lost steering control and crashed in the ego lane.	Sa, Su, Re, SIF
ACC0.3	AD vehicle made an accident while an object suddenly appeared in its lane in front.	Sa, Av, Re
ACC0.4	AD vehicle suddenly lost the steering/braking control while the vehicle moving up the hill and made an accident.	Sa, Re, Av
ACC0.5	AD vehicle made an accident due to fake data of sensors manipulated by an anonymous person.	Se
ACC0.6	AD vehicle made an accident due to loss of the communication signals from the Backend	Av, Se

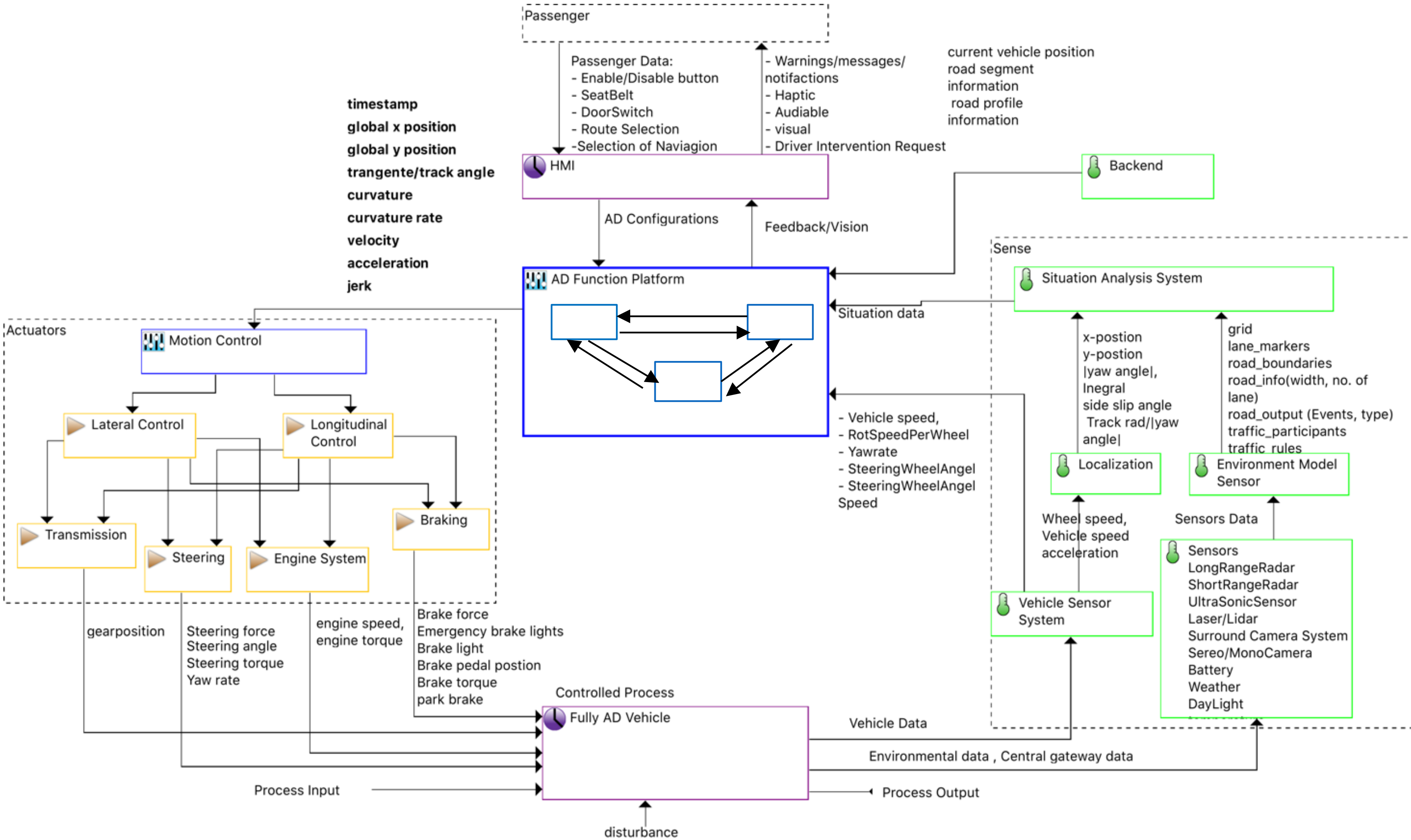
** **Sa**: Functional safety, **Su**: Safety in use, **Re**: Reliability, **SIF**: Safety of intended functionality, **Av** : Availability, **Se**: Security.

Hazard Categories
of fully Automated Driving

- We identify 9 hazard categories at the Autonomous Vehicular level to facilitate developing operational safety concepts
- We identify 176 hazards which are grouped into the nine hazard categories

ID	Hazard Categories	Operational Safety Attributes *	No. of Hazard	Linked Accidents
HG1	Road Surface Detection	Sa, Re, SIF, Av	4	**1-12, 16-19**
HG2	Object Detection	Sa, Re, Av, SIF	23	**1-13, 15-20**
HG3	Control Hazard	Sa, Su, Re	47	**1,2, 12, 15, 24-26**
HG4	Localization & Mapping	Sa, Se, Av	8	**1-21, 24-26**
HG5	Environmental Model Hazards	Sa, Av, Se, SIF	34	**1-13, 14-21**
HG6	Decision Making Hazards	Sa	30	**1-21**
HG7	Data Communication Hazards	Se, Av	10	**1-19, 21**
HG8	Individual ECU Defect	Re	5	**1-19**
HG9	Security Hazards	Se	15	**20-23**
Total			**176**	

Safety Control Structure Diagram
at Level 0



Developing Operational Safety Concepts

- We evaluate each control actions to determine the hazardous events
- We identify **29** hazardous control actions

HCA-0.1{Sa, Av, Re, SIF, Su}

The AD function platform does not provide a valid trajectory to motion control while the AD vehicle is approaching too fast in the lane ➲ [**H-31, H-46, H-54**], Hazard Category: **control hazards**

Control Hazard

loss of steering or braking or acceleration

Operational Safety Requirements

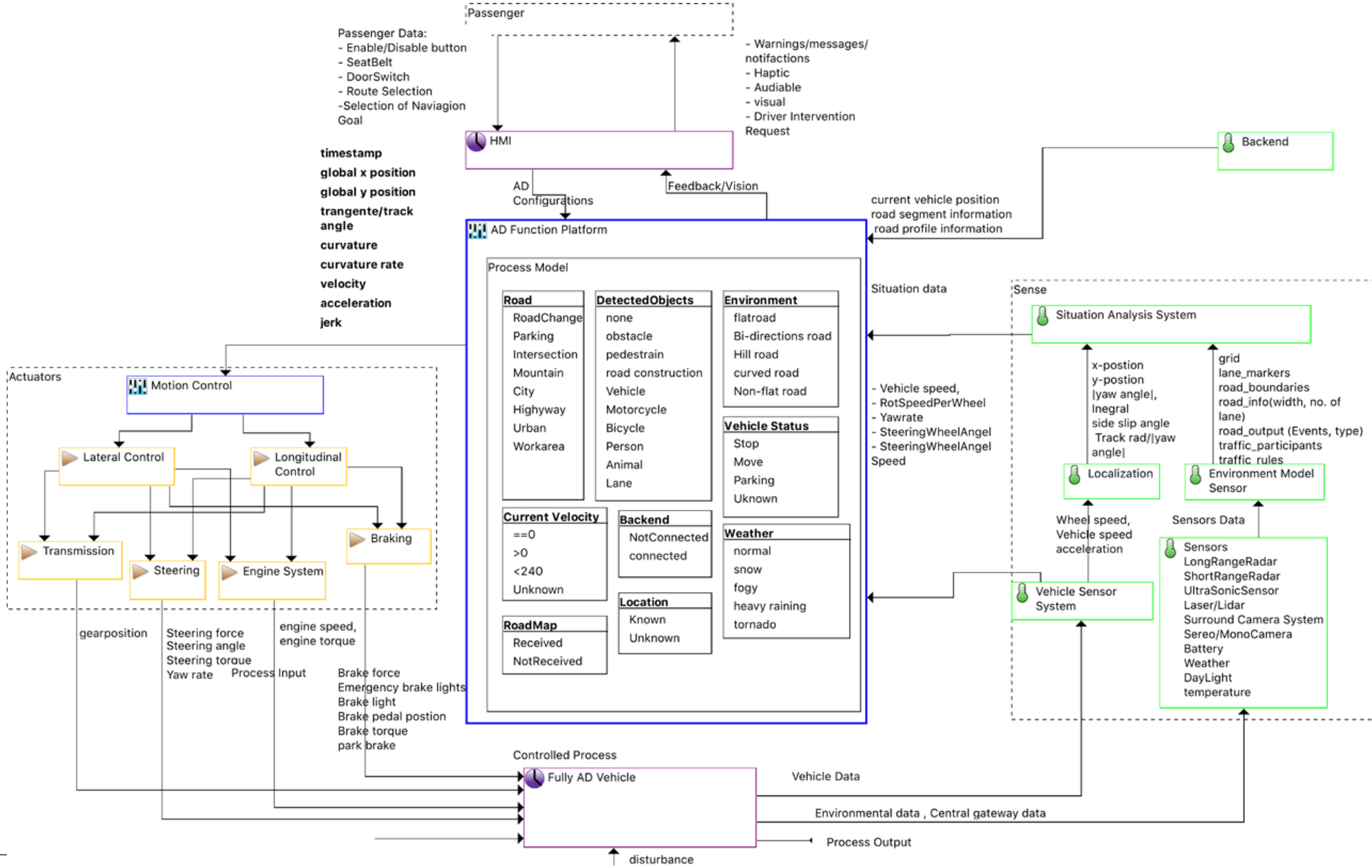
OSR 0.1: The AD function platform shall always provide a trajectory to motion control

Operational Safety Concept

OSC 0.1: Unintended absence of a vehicle trajectory shall be avoided

Refine Operational Safety Concepts

› We identify the process model variables of the fully automated driving at the level **0**



Refine Operational Safety Concepts

- We use XSTAMPP to generate the context table and provide a minimal set of combination between the process model variable and refine hazardous control actions and operational safety concepts
- We identify **229** hazardous scenarios
- We identify the accident causes (STPA Step 2) for each hazardous control action

---

Operational Safety Requirements

OSR 0.1: The AD function platform shall always provide a trajectory to motion control

Refine Operational Safety Requirements

ROSR 0.1: : the AD function platform shall always provide the trajectory to enable motion control to adjust throttle and apply brake friction when the vehicle is moving and there is traffic ahead to avoid the potential collision

Refine Operational Safety Concept

ROSC 0.1: Unintended absence of a vehicle trajectory shall be avoided when the vehicle is moving and there is traffic ahead.

Automated Driving Architecture

Agenda

1 Motivation

2 Challenges: Fully Automated Driving

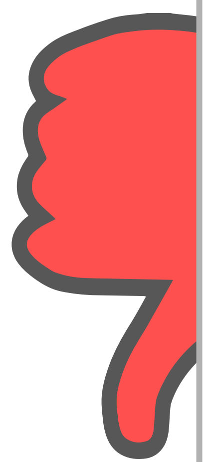
3 Proposed Approach

4 Results

5 Conclusion & Future Work

A systematic approach based on STPA
Conclusion

- We used STPA approach as a risk assessment approach of functional arictecutrue of fully automated driving function.
- We applied STPA to complex functional architecture of fully automated driving at early stage of development process.
- We provide a systematic guidance on deriving operational safety requirements and develop operational safety concepts.
- We address different attributes to develop operational safety concepts.



- Ensuring completeness of hazards list.
- Linking between different control structure diagram at multiple levels of functional architecture.
- XSTAMPP does not support multi-levels of control structure diagram and multi-STPA process for one project.
- Directly mapping between our results to the safety standard like ISO 26262.

A systematic approach based on STPA
Future Work

- We plan to apply STPA to other levels (level 1 and level 2) to identify the hazardous scenarios of each system or component
- We plan to generate the test cases based on the results of STPA to test the prototype of the fully automated driving (**STPA SwISs approach**)
- We plan to explore the use of STPA approach in compliance with **ISO 26262**
- We plan to use **CAST** approach to analyse the accidents which are occurred during the simulation phase to get a better understanding why these accidents occurred
- We plan to link between **XSTAMPP** platform which is an extensible safety engineering platform with architectural tool such **PREEVision** to link the results of STPA safety analysis directly to the architecture element

Thank you for your attention

Q&A

Joint work with:
Prof. Dr. Stefan Wagner, University of Stuttgart, Stuttgart, Germany
Jürgen Röder, Norbert Balbierer and Ludwig Ramsauer, *Continental AG, Regensburg, Germany*
Thomas Raste and Hagen Boehmert, *Continental Teves AG & Co. oHG, Frankfurt am Main, Germany*