Overview of Working Packages

- Functional & Safety Requirements for automated driving
- Specification and harmonization of functional and system architecture
- Definition of a fail-operational & resilient system architecture:
  - Duo Duplex Architecture with fault detection selected and advantages evaluated
- Specification of harmonized driving strategies for minimum risk maneuver & lane change maneuver
System Architecture Design

Logical Architecture
Solution independent structuring of features

Network Architecture
Electric infrastructure of the system and partitioning of SW functions and I/Os

Functional Architecture
Functional description of logical features & their interfaces

Wiring Harness Architecture
ECU placement and the electrical & physical connections
Initial System Architecture
Technical Architecture Design

Safety Goals

Functional Safety Requirements

Technical Safety Requirements

DOORS

Hazard & Risk Assessment

Imported Requirements

Functional Safety Concept

Technical Safety Concept

Item Definition

DOORS

RIF import

Concept

Requirements

Imported Requirements
Technical Architecture Design

Imported Requirements

- 1.5.5 Perception Requirements / -0 (Requirement)
  - 1.5.5.2 SYS_AD_4605 / -0 (Requirement)
  - 1.5.5.3 SYS_AD_4696 / -0 (Requirement)
  - 1.5.5.4 SYS_AD_5311 / -0 (Requirement)
  - 1.5.5.5 SYS_AD_5210 / -0 (Requirement)
  - 1.5.5.6 Traffic sign/rules detection / -0 (Requirement)
  - 1.5.5.6.1 SYS_AD_2504 / -0 (Requirement)

Functional Safety Concept

Technical Safety Concept
Functional Safety and Redundancy Concept

- Vehicle E/E - Architecture needs a holistic approach
e.g. Service Oriented Architectures, Cloud services, Update over the air

- Safety & system architecture/interface must be defined together
- Safety, reliability and availability has important implications for analyzing
- Fail Operational Behavior - fail silent
A method for functional safety analysis is developed and applied to the representative case of ‘Lane Change’.

Relevant impact for the definition of a fault tolerant architecture.

A structured approach is established regarding the implementation of the sensor system.

The work addresses aspects:
- redundancy,
- data fusion
- specific demands to bring the vehicle to a safe state in case of failure.
Functional Safety and Redundancy Concept

› Fault Tolerant System Architecture
  › Proposal for **Error Detection** and **Recovery Mechanisms**
  › Detection of:
    › Sensor Fault
    › Data Fusion Failure
    › Actuator Failure
  › **Fault Handling** and **Reconfiguration** of the system's functionality
Harmonization of Driving Maneuvers

The MRM is a manoeuvre to bring the vehicle into a minimal risk condition only if:

- driver does not react on a planned and initiated by automation system (with sufficient take-over time) take-over-request
  - upcoming situation cannot be handled by automation system (e.g. infrastructural reasons, technical limitations like heavy rain, fog,...)
    -> foreseeable situation
- an unplanned automation system related failure appears (take-over time may be limited to zero in worst case);
Harmonization of Driving Maneuvers

The minimal risk condition depends strongly on the situation and the characteristic of the system failure. For automated driving on highway, urban or close distance scenarios a safe stop shall be achieved.

- The MRM is not:
  - a degradation of the automation system
  - a collision avoidance functionality
Harmonization of Driving Maneuvers

A Lane Change is a short term driving manoeuvre with a clearly defined start and end condition to bring the host vehicle from the current driving lane to an adjacent driving lane, either to the left or right. Before starting and after finishing a Lane Change manoeuvre the host vehicle is in Lane Following.

- A Lane Change shall be clearly identifiable by the surrounding traffic participants and driver of host vehicle
- Conditions harmonized
- Reasons to trigger a Lane Change defined
- Sequence of an automated lane change harmonized
Conclusion

Key Drivers

- eMobility
- Automated Driving
- Mobility Services
- Connectivity

- Market
- User experience

Challenges

- Updatable
- Upgradable
- Dependable (reliable, available, safe & secure)

- Technology
- Function
- Costs
- Quality

System orientation enables us to handle the challenges
Thank you.

Daniel Lammering
Vehicle System Architect
Corporate Systems and Technology
Daniel.Lammering@continental-corporation.com

Carolin Hilbert
Vehicle System Architect
Corporate Systems and Technology
Carolin.Hilbert@continental-corporation.com