

Functional Safety Concept Lane Assistance

**Document Version: 1.1**



# Document history

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Editor | Description |
| 12.01.2019 | 1.0 | Michael Ikemann | Initial definition of functional safety |
| 13.01.2019 | 1.1 | Michael Ikemann | Refinement |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# Table of Contents

[Document history](#_1t3h5sf)

[Table of Contents](#_ktt3lgighckp)

[Purpose of the Functional Safety Concept](#_fulgh8sf1ocg)

[Inputs to the Functional Safety Analysis](#_757cx6xm46zb)

[Safety goals from the Hazard Analysis and Risk Assessment](#_pi1c1upmo8jt)

[Preliminary Architecture](#_s0p6ihti6jgk)

[Description of architecture elements](#_cqb49updinx4)

[Functional Safety Concept](#_mx8us8onanqo)

[Functional Safety Analysis](#_mtn6qbhgsr36)

[Functional Safety Requirements](#_frlc9y84ede8)

[Refinement of the System Architecture](#_74udkdvf7nod)

[Allocation of Functional Safety Requirements to Architecture Elements](#_g2lqf7kmbspk)

[Warning and Degradation Concept](#_4w6r8buy4lrp)

# Purpose of the Functional Safety Concept

The purpose of the functional safety concept is to define the single functionalities from a high level perspective, how the the safety can be ensured as much as possible for each of it’s features and the functionality’s ASIL level.

# Inputs to the Functional Safety Concept

## Safety goals from the Hazard Analysis and Risk Assessment

|  |  |
| --- | --- |
| **ID** | **Safety Goal** |
| Safety\_Goal\_01 | The lane keeping item shall ensure that the lane departure oscillating torque amplitude is below Max\_Torque\_Amplitude |
| Safety\_Goal\_02 | Under bad weather conditions the LKA should deny activation to prevent this situation. The driver should be made aware that the LGA is no autonomous system and that majorly road work sites can lead to uncontrollable situations. |
| Safety\_Goal\_03 | If the user removes the hands from the steering wheel the driver should be informed audiovisual that the lane guidance will be deactivated because the system shall not be used in an autonomous manner. |
| Safety\_Goal\_04 | It shall be verified that the lane guidance system will be disabled when the vehicle is not driving. |

## Preliminary Architecture

### https://d17h27t6h515a5.cloudfront.net/topher/2017/July/5976aa23_02-advanced-driver-assistance-system-architecture-02-1/02-advanced-driver-assistance-system-architecture-02-1.png

### Description of architecture elements

|  |  |
| --- | --- |
| **Element** | **Description** |
| Camera Sensor | Captures the image. Is mounted at the top of the wind screen. |
| Camera Sensor ECU | Analyses the image – detects the lane and the detection certainty and decides if the user shall be warned about lane departure or follow the center of the lane if lane guidance is activated. |
| Car Display | Visualizes if lane guidance and departure features are activated and also informs the user when a lane departure occurs. |
| Car Display ECU | Is responsible for the visualization of the car’s dashboard. Needs to be extended for the visualization of LGA related features. |
| Driver Steering Torque Sensor | Detects with which amount of force the driver tries to steer. In case of the LGA a non-existing steering of the driver in a curve should lead to a warning so the driver will not use the LGA in an autonomous way. Also a counter-steering of the driver should be detected and disable the lane guide so the driver will regain control of the vehicle if required. |
| Electronic Power Steering ECU | The EPS ECU decides by the information provided by the DSTS and CS ECU which amount of torque to apply to the steering wheel. |
| Motor | Applies the amount of torque provided by the EPS ECU to the steering wheel so that the vehicle will (for example) follow the lane detected. |

# Functional Safety Concept

The functional safety concept consists of:

* Functional safety analysis
* Functional safety requirements
* Functional safety architecture
* Warning and degradation concept

## Functional Safety Analysis

|  |  |  |  |
| --- | --- | --- | --- |
| **Malfunction ID** | **Main Function of the Item Related to Safety Goal Violations** | **Guidewords (NO, WRONG, EARLY, LATE, MORE, LESS)** | **Resulting Malfunction** |
| Malfunction\_01 | Lane Departure Warning (LDW) function shall apply an oscillating steering torque to provide the driver a haptic feedback | The lane departure warning applies MORE oscillating torque than intended. | A too strong vibration of the steering wheel would distract the driver. |
| Malfunction\_02 | Lane Departure Warning (LDW) function shall apply an oscillating steering torque to provide the driver a haptic feedback | The computation of the camera ECU arrives too LATE at the EPS ECU. | The driver will be notified too late to still be able to react due to a delayed notification. |
| Malfunction\_03 | Lane Keeping Assistance (LKA) function shall apply the steering torque when active in order to stay in ego lane | The LKA steers WRONG within a road work site due to crossing lane markers which irritated the CS ESU. | The vehicle drives into a wrong direction and potentially causes an accident. |

## Functional Safety Requirements

Lane Departure Warning (LDW) Requirements:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Functional Safety Requirement** | **ASIL** | **Fault Tolerant Time Interval** | **Safe State** |
| Functional  Safety  Requirement  01-01 | The lane keeping item shall ensure that the lane departure oscillating torque is amplitude is below Max\_Torque\_Amplitude. | C | 50ms | Disable LDW functionality |
| Functional  Safety  Requirement  01-02 | The lane keeping item shall ensure that the lane departure oscillating torque is oscillating frequency is below Max\_Torque\_Frequency. | C | 50ms | Disable LDW functionality |

Lane Departure Warning (LDW) Verification and Validation Acceptance Criteria:

|  |  |  |
| --- | --- | --- |
| **ID** | **Validation Acceptance**  **Criteria and Method** | **Verification Acceptance**  **Criteria and Method** |
| Functional  Safety  Requirement  01-01 | Acceptance:  Vibration amplitude is clearly detectable by the driver while not being too intense to be annoying.  Method: Vehicle testing | Acceptance:  Requested amplitude does not exceed defined maximum of Max\_Torque\_Amplitude.  Method: Fault test with measurement device |
| Functional  Safety  Requirement  01-02 | Acceptance:  Vibration frequency is clearly detectable by the driver while not being too intense to be annoying.  Method: Vehicle testing | Acceptance:  Requested amplitude does not exceed defined maximum of Max\_Torque\_Frequency  Method: Fault test with measurement device |

Lane Keeping Assistance (LKA) Requirements:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Functional Safety Requirement** | **ASIL** | **Fault Tolerant Time Interval** | **Safe State** |
| Functional  Safety  Requirement  02-01 | The lane keeping item shall ensure that the torque requested by the lane keeping assistant shall not exceed a given threshold (caused by a non-steering driver) for time span longer than Max\_Duration | B | 500ms | Disable LKA functionality |

Lane Keeping Assistance (LKA) Verification and Validation Acceptance Criteria:

|  |  |  |
| --- | --- | --- |
| **ID** | **Validation Acceptance**  **Criteria and Method** | **Verification Acceptance**  **Criteria and Method** |
| Functional  Safety  Requirement  02-01 | Validation:  The LKA automatically switches off when it detects that the driver did not steer at all for longer than Max\_Duration.  Method:  Vehicle testing | Validation:  LKA systems switches off if no activity of the driver, so no noteworthy level from the steering sensor could be received for Max\_Duration.  Method:  Fault test by verifying that the torque applied will be zeroed if the steering sensor does not send any signal above a minimum threshold for Max\_Duration |

## Refinement of the System Architecture



## Allocation of Functional Safety Requirements to Architecture Elements

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Functional Safety Requirement** | **Electronic Power Steering ECU** | **Camera ECU** | **Car Display ECU** |
| Functional  Safety  Requirement  01-01 | The lane keeping item shall ensure that the lane departure oscillating torque is amplitude is below Max\_Torque\_Amplitude. | **X** |  |  |
| Functional  Safety  Requirement  01-02 | The lane keeping item shall ensure that the lane departure oscillating torque is oscillating frequency is below Max\_Torque\_Frequency. | **X** |  |  |
| Functional  Safety  Requirement  02-01 | The lane keeping item shall ensure that the torque requested by the lane keeping assistant shall not exceed a given threshold (caused by a non-steering driver) for time span longer than Max\_Duration. | **X** |  |  |

## Warning and Degradation Concept

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Degradation Mode** | **Trigger for Degradation Mode** | **Safe State invoked?** | **Driver Warning** |
| WDC-01 | Disabled until next motor start. | When safety requirements for FSR 01-01 or FSR-01-02 are not met. | Yes | Error light in dashboard enabled and an acoustic warning sound played. |
| WDC-02 | Disabled temporarily till situation is safe again. | When safety requirements for FSR-01-01 are not met. | Yes | Error light in dashboard enabled and an acoustic warning sound played. |