

Functional Safety Concept Lane Assistance

**Document Version: 1.0**



# 

# Document history

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Editor | Description |
| 15.08.2018 | 1.0 | Reuss | First version |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# 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 is to avoid accidents by reducing risk to acceptable levels. The functional safety concept helps contributing to that, by decomposing safety goals into functional safety requirements and allocating them to the corresponding subsystems.

# Inputs to the Functional Safety Concept

## Safety goals from the Hazard Analysis and Risk Assessment

|  |  |
| --- | --- |
| **ID** | **Safety Goal** |
| Safety\_Goal\_01 | The oscillating steering torque from the lane departure warning function shall be limited. |
| Safety\_Goal\_02 | The lane keeping assistance function shall be time limited and the additional steering torque shall end after a given time interval so that the driver cannot misuse the system for autonomous driving. |
| Safety\_Goal\_03 | The steering torque from the lane keep assistance function shall steer the car back to the center of the lane. |
| Safety\_Goal\_04 | The steering torque from the lane keep assistance function shall be limited. |

## 

## Preliminary Architecture



### Description of architecture elements

|  |  |
| --- | --- |
| **Element** | **Description** |
| Camera Sensor | Takes images of the road. |
| Camera Sensor ECU | Processing images taken by the camera sensor and outputs information to the Electronic Power Steering ECU. |
| Car Display | Display used to share information with the driver. |
| Car Display ECU | Responsible ECU to control the car display. |
| Driver Steering Torque Sensor | Measures torque applied by the driver the steering wheel. |
| Electronic Power Steering ECU | Processing information from Camera Sensor ECU and Torque Sensor and controls motor to add additional torque to the steering wheel, depending on the situation. |
| Motor | Adds additional torque to the steering wheel, if requested. |

# 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 | MORE | The lane departure warning function applies an oscillating torque with very high torque amplitude (above limit). |
| Malfunction\_02 | Lane Departure Warning (LDW) function shall apply an oscillating steering torque to provide the driver a haptic feedback | MORE | The lane departure warning function applies an oscillating torque with very high torque frequency (above limit). |
| Malfunction\_03 | Lane Keeping Assistance (LKA) function shall apply the steering torque when active in order to stay in ego lane | NO | The lane keeping assistance function is not limited in time duration which leads to misuse as an autonomous driving function. |

## 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 electronic power steering ECU shall ensure that the lane departure oscillating torque amplitude is below Max\_Torque\_Amplitude. | C | 50ms | Set torque to zero and shut off system |
| Functional  Safety  Requirement  01-02 | The electronic power steering ECU shall ensure that the lane departure oscillating torque frequency is below Max\_Torque\_Frequency. | C | 50ms | Set torque to zero and shut off system |

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 | Test how drivers react to different torque amplitudes and frequencies to prove that the chosen value is apprpriate | Software test with fault injection |
| Functional  Safety  Requirement  01-02 | Test how drivers react to different torque amplitudes and frequencies to prove that the chosen value is apprpriate | Software test with fault injection |

Lane Keeping Assistance (LKA) Requirements:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Functional Safety Requirement** | **ASIL** | **Fault Tolerant Time Interval** | **Safe State** |
| Functional  Safety  Requirement  02-01 | The electronic power steering ECU shall ensure that the lane keeping assistance torque is applied for only Max\_Duration. | B | 500ms | Set torque to zero and shut off system |

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 | Test and validate, that the chosen parameter Max\_Duration really dissuade drivers from taking their hands off the wheel. | Vehicle test to verify that the system turns off, if the lane keeping assistance has exceeded 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 electronic power steering ECU shall ensure that the lane departure oscillating torque amplitude is below Max\_Torque\_Amplitude. | **x** |  |  |
| Functional  Safety  Requirement  01-02 | The electronic power steering ECU shall ensure that the lane departure oscillating torque frequency is below Max\_Torque\_Frequency. | **x** |  |  |
| Functional  Safety  Requirement  02-01 | The electronic power steering ECU shall ensure that the lane keeping assistance torque is applied for only Max\_Duration. | **x** |  |  |

## Warning and Degradation Concept

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Degradation Mode** | **Trigger for Degradation Mode** | **Safe State invoked?** | **Driver Warning** |
| WDC-01 | Turn off functionality | Torque amplitude over Max\_Torque\_Amplitude  OR  Torque frequency over Max\_Torque\_Frequency | Yes | Play alarm sound. Display warning “Lane assistance system is shut off due to malfunction.” |
| WDC-02 | Turn off functionality | Driver did not put hands on the steering wheel for time longer than Max\_Duration | Yes | Display warning “Lane assistance system is not designed for autonomous driving. Driver is responsible to control the car at all times. System is shut off.” |