

Functional Safety Concept Lane Assistance

**Document Version: 1.0**

**Released on 2017-10-22**



# Document history

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Editor | Description |
| 2017-10-22 | 1.0 | Martin Hintz | Initial 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 of this functional safety concept is to avoid accidents by reducing risks involved in

the Lane Assistance functionality to acceptable levels.

# Inputs to the Functional Safety Concept

## Safety goals from the Hazard Analysis and Risk Assessment

|  |  |
| --- | --- |
| **ID** | **Safety Goal** |
| Safety\_Goal\_01 | The steering torque applied from the Lane Departure Warning functionality shall be limited. |
| Safety\_Goal\_02 | The Lane Assistance functionality shall be time limited and the additional  steering torque shall end after a pre-defined time interval so that the drive. |

## Preliminary Architecture

****

Figure 1: Preliminary Architecture of the Lane Assistance System

### Description of architecture elements

|  |  |
| --- | --- |
| **Element** | **Description** |
| Camera Sensor | One or more sensor(s) located at the front of  the vehicle that collect(s) visual data (image, video) |
| Camera Sensor ECU | A computer (electronic control unit) that interprets data collected by the camera sensor(s), detects lane lines, identifies and calculates steering corrections, triggers power steering ECU and triggers audio-visual warnings on the car display ECU. |
| Car Display | A physical display in front of the vehicle’s driver to provide audio-visual feedback. |
| Car Display ECU | A computer (ECU) that controls the car display and generates audio-visual warnings triggered from camera sensor ECU. |
| Driver Steering Torque Sensor | A sensor that measures the torque applied to the  steering wheel by the driver. |
| Electronic Power Steering ECU | A computer attached to the power steering of the vehicle that controls the torque applied to the steering wheel according to the commands of the camera sensor ECU. |
| Motor | An actuator responsible for applying torque to the steering wheel. |

# 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 Max\_Torque\_Amplitude). |
| 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 Max\_Torque\_Frequency). |
| 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 warning  oscillating torque amplitude is below  Max\_Torque\_Amplitude | C | 50 ms | Turn Off System |
| Functional  Safety  Requirement  01-02 | The Electronic Power Steering ECU shall  ensure that the lane departure warning  oscillating torque frequency is below  Max\_Torque\_Frequency | C | 50 ms | Turn 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 that the amplitude value chosen for  Max\_Torque\_Amplitude is balanced and does not trigger counter actions from the driver. | Verify that LDW is turned off when Max\_Torque\_Amplitude is exceeded and a warning is being generated. |
| Functional  Safety  Requirement  01-02 | Test that the amplitude value chosen for  Max\_Torque\_Frequency is balanced and does not trigger counter actions from the driver. | Verify that LDW is turned off when Max\_Torque\_Frequency is exceeded and a warning is being generated. |

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 | 500 ms | Turn 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 that the time value chosen for Max\_Duration discourages drivers from taking their hands off the steering wheel. | Verify that LKA is turned off when Max\_Duration is exceeded and a warning is being generated. |

## Refinement of the System Architecture



Figure 2: Refined Architecture of the Lane Assistance System

## 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 shall  ensure that the oscillating torque amplitude is below Max\_Torque\_Amplitude for the lane departure warning item. | **✓** |  |  |
| Functional  Safety  Requirement  01-02 | The electronic power steering  ECU shall ensure shall ensure that the oscillating torque frequency is below Max\_Torque\_Frequency for the lane departure warning item. | **✓** |  |  |
| Functional  Safety  Requirement  02-01 | The electronic power steering  ECU shall ensure that the lane  keeping assistance torque is  applied for only Max\_Duration. | **✓** |  |  |

## Warning and Degradation Concept

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Degradation Mode** | **Trigger for Degradation Mode** | **Safe State invoked?** | **Driver Warning** |
| WDC-01 | Turn off the  functionality. | Malfunction\_01  Malfunction\_02 | Yes | Audio-Visual Warning in Car Display |
| WDC-02 | Turn off the  functionality. | Malfunction\_03 | Yes | Audio-Visual Warning in Car Display |