

Functional Safety Concept Lane Assistance

**Document Version: [Version]**

**Template Version 1.0, Released on 2017-06-21**



# Document history

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Editor | Description |
| 20/06/2018 | 1.0 | Aditya |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# 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 Functional Safety Concept documents the identified systems high level requirements. These requirements are allocated to different part of the item architecture. Technical safety requirements will be derived from the safety concept. The validation concept for these requirements are presented as well.

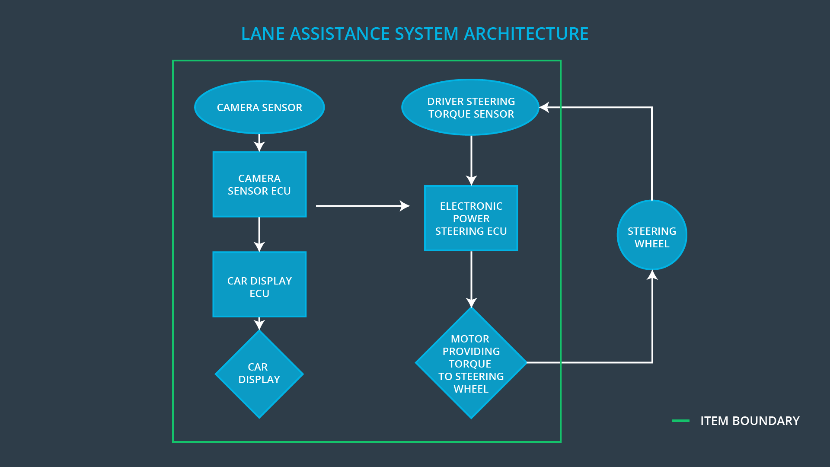
# Inputs to the Functional Safety Concept

## 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 system is not misused for autonomous driving. |
| Safety\_Goal\_03 | The lane keeping assistance function has to be deactivated if camera is not able to detect the lane lines correctly. |
| Safety\_Goal\_04 | The lane keeping assistance function shall have the ability to detect lane lines of different color, and reliably detect and react merging lanes in advance. |

## Preliminary Architecture

The Following figure shows the preliminary architecture of Lane Assistance System-



### Description of architecture elements

|  |  |
| --- | --- |
| **Element** | **Description** |
| Camera Sensor | Capture images of road lanes and send it to ECU. |
| Camera Sensor ECU | Process the images from camera and determine car position with respect to road lanes. |
| Car Display | Provides warnings and the Lane Departure Assistance status. |
| Car Display ECU | Controls the car display to show warnings and status of all functions. |
| Driver Steering Torque Sensor | Measures the torque applied to the steering wheel by the driver |
| Electronic Power Steering ECU | Receives the torque applied by the driver on the steering wheel from Driver Steering Torque Sensor and computes appropriate final torque which is transferred to steering wheel motor. |
| Motor | Receives the final torque computed by Electronic Power Steering ECU and applies it 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 LDW function applies an oscillating torque with very high torque amplitude. |
| Malfunction\_02 | Lane Departure Warning (LDW) function shall apply an oscillating steering torque to provide the driver a haptic feedback | MORE | The LDW function applies an oscillating torque with very high 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 LKA 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 | Vibration torque amplitude below Max\_Torque\_A mplitude. |
| Functional  Safety  Requirement  01-02 | The Electronic Power Steering ECU shall ensure that the lane departure warning oscillating torque amplitude is below Max\_Torque\_Frequency | C | 50 ms | Vibration frequency is below Max\_Torque\_Fr equency. |

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 and validate that Max\_Torque\_Amplitude chosen is low enough that driver does not lose control over the car. | Verify that the system does turn off in time if Max\_Torque\_Amplitude is exceeded. |
| Functional  Safety  Requirement  01-02 | Test and validate that Max\_Torque\_Frequency chosen is low enough that driver does not lose control over the car. | Verify that the system does turn off in time if Max\_Torque\_Frequency is exceeded. |

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 only for Max\_Duration. | B | 500 ms | Lane Keeping Assistance torque is zero. |

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 Max\_Duration chosen is low enough that driver does not lose control over the car | The system really does turn off if the LKA duration exceeds 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 warning oscillating torque amplitude is below MAX\_TORQUE\_AMPLITUDE. | **Yes** | **No** | **No** |
| Functional  Safety  Requirement  01-02 | The electronic power steering ECU shall ensure that the lane departure warning oscillating torque amplitude is below MAX\_TORQUE\_FREQUENCY. | **Yes** | **No** | **No** |
| Functional  Safety  Requirement  02-01 | The electronic power steering ECU shall ensure that the Lane Keeping Assistance torque is applied only for Max\_Duration. | **Yes** | **No** | **No** |

## Warning and Degradation Concept

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Degradation Mode** | **Trigger for Degradation Mode** | **Safe State invoked?** | **Driver Warning** |
| WDC-01 | Turn off system | Malfunction\_01 Malfunction\_02 | Yes | Warning light on dashboard |
| WDC-02 | Turn off system | Malfunction\_03 | Yes | Warning light on dashboard |