

Functional Safety Concept Lane Assistance

**Document Version: 1.0**

**Released on 2018-06-22**



# Document history

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Editor | Description |
| 2018-06-22 | 1.0 | Deepak Kumar Singh | Functional Safety Docuent |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# Table of Contents

[Purpose of the Functional Safety Concept 4](#_Toc517399757)

[Inputs to the Functional Safety Concept 4](#_Toc517399758)

[Safety goals from the Hazard Analysis and Risk Assessment 4](#_Toc517399759)

[Preliminary Architecture 5](#_Toc517399760)

[Description of architecture elements 5](#_Toc517399762)

[Functional Safety Concept 6](#_Toc517399763)

[Functional Safety Analysis 6](#_Toc517399764)

[Functional Safety Requirements 7](#_Toc517399765)

[Refinement of the System Architecture 8](#_Toc517399766)

[Allocation of Functional Safety Requirements to Architecture Elements 9](#_Toc517399768)

[Warning and Degradation Concept 9](#_Toc517399769)

# 

# Purpose of the Functional Safety Concept

To identify functional safety requirement and assign those requirements to item’s subsystems and elements without getting into technical details.

# Inputs to the Functional Safety Concept

## Safety goals from the Hazard Analysis and Risk Assessment

|  |  |
| --- | --- |
| **ID** | **Safety Goal** |
| Safety\_Goal\_01 | Lane departure warning system should limit the Oscillation of steering wheel below Max Torque Amplitude. |
| Safety\_Goal\_02 | The departure warning system shall ensure that the lane departure oscillating torque frequency is below Max Torque Frequency. |
| Safety\_Goal\_03 | The lane keeping assistance system shall be time limited. |

## Preliminary Architecture

### 

### Description of architecture elements

|  |  |
| --- | --- |
| **Element** | **Description** |
| Camera Sensor | Sends camera images to camera sensor ECU |
| Camera Sensor ECU | Identifies lanes and sends torque request to electronic power steering ECU and warning request to car display ECU |
| Car Display | Shows warning |
| Car Display ECU | Sends warning to car display for driver |
| Driver Steering Torque Sensor | Monitors steering torque provided by driver and sends it to electronic power steering ECU |
| Electronic Power Steering ECU | Processes torque request from camera sensor ECU and calculate amount of torque to apply based on input from Driver steering torque sensor and sends it to Motor |
| Motor | Applies torque received from electronic power steering ECU to 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 MORE oscillation torque amplitude then the specified 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 MORE oscillation torque frequency then specified 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 system has NO time limit which results in misuse in case of autonomous vehicle. |

## 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 departure warning system shall ensure that oscillation torque amplitude applied to steering wheel is limited. | C | 50 ms | Torque amplitude set to 0 |
| Functional  Safety  Requirement  01-02 | The Lane departure warning system shall ensure that oscillation torque frequency applied to steering wheel is limited. | C | 50 ms | Torque frequency set to 0 |

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 | Have tests on driver’s reaction (applied torque) when different torque amplitude is applied and validates that appropriate max value is chosen. | Verify that system sets torque amplitude to 0 when torque amplitude greater than max torque amplitude is requested. |
| Functional  Safety  Requirement  01-02 | Have tests on driver’s reaction (applied torque) when different torque frequency is applied and validates that appropriate max value is chosen. | Verify that system sets torque frequency to 0 when torque frequency greater than max torque frequency is requested. |

Lane Keeping Assistance (LKA) Requirements:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Functional Safety Requirement** | **ASIL** | **Fault Tolerant Time Interval** | **Safe State** |
| Functional  Safety  Requirement  02-01 | Lane Keeping Assistance system shall apply the steering torque when active in order to stay in ego lane | B | 500ms | Steering torque set to 0 |

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 | Perform tests on time duration chosen to discourage taking off hands from steering wheel and prove that appropriate time duration is chosen. | Verify that system sets steering torque to 0 after time 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 | Lane departure warning system should limit the Oscillation of steering wheel below Max Torque Amplitude. | **x** |  |  |
| Functional  Safety  Requirement  01-02 | The departure warning system shall ensure that the lane departure oscillating torque frequency is below Max Torque Frequency. | **x** |  |  |
| Functional  Safety  Requirement  02-01 | The lane keeping assistance system shall be time limited. | **x** |  |  |

## Warning and Degradation Concept

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Degradation Mode** | **Trigger for Degradation Mode** | **Safe State invoked?** | **Driver Warning** |
| WDC-01 | Turn off lane assistance system | Malfunction\_01 | YES | Warning on Car display |
| WDC-02 | Turn off lane assistance system | Malfunction\_02 | YES | Warning on Car display |
| WDC-03 | Turn off lane assistance system | Malfunction\_03 | YES | Warning on Car display |