

Functional Safety Concept Lane Assistance

**Document Version: 1.0**

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



# Document history

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Editor | Description |
| 21-Jun-18 | 1.0 | Nikhil Sinnarkar | Initial Draft |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# 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 functional safety concept is to describe the implementation of the independent safety solutions for a defined item.

# 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 additional steering torque shall end after a given time interval so the driver cannot misuse the system for autonomous driving. |

## Preliminary Architecture



### Description of architecture elements

|  |  |
| --- | --- |
| **Element** | **Description** |
| Camera Sensor | Capture road images and provide them to the Camera Sensor ECU. |
| Camera Sensor ECU | Analyze provided images to determine if the car is leaving the lane and if so, send a vibrational torque request to the power steering ECU. |
| Car Display | Provide feedback to the driver displaying warnings and the Lane Departure Assistance status. |
| Car Display ECU | An Electronic Control Unit that drives the Car Display component to show the Lane Keeping Assistance warning and Lane Departure Assistance status. |
| Driver Steering Torque Sensor | Measure the torque applied to the steering wheel by the driver. |
| Electronic Power Steering ECU | ECU responsible for measuring the torque provided by the driver and adding appropriate amount of torque based on a lane assistance system torque request (LKA) and vibrates the steering wheel when the driver drifts away from the center (LDW). |
| Motor | Actuator responsible for applying requested torque to the steering column by Electronic Power Steering ECU for either the LKA or LDW functions. |

# 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 lead 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 lane keeping item shall ensure that the lane departure oscillating torque amplitude is below Max\_Torque\_Amplitude | C | 50 ms | Vibration torque amplitude below Max\_Torque\_Amplitude. |
| Functional  Safety  Requirement  01-02 | The Lane Departure Warning item shall ensure that the lane departure oscillating torque frequency is below Max\_Torque\_Frequency. | C | 50 ms | Vibration frequency is below Max\_Torque\_Frequency. |

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 | Validate Max\_Torque\_Amplitude chosen is high enough to be detected by a driver while low enough not to cause loss of steering | Verify the system does turn off if the Lane Departure Warning exceeded Max\_Torque\_Amplitude. |
| Functional  Safety  Requirement  01-02 | Validate Max\_Torque\_Frequency chosen is adequate to be detected by the driver and not cause the loss of steering. | Verify the system does turn off if the Lane Departure Warning exceeded Max\_Torque\_Frequency. |

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 Lane Keeping Assistance torque is applied only 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 the Max\_duration chosen did dissuade drivers from using the car as self-driving car. | Verify that the system really does turn off if the lane keeping assistance ever 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 Lane Departure Warning item shall ensure that the lane departure oscillating torque amplitude is below Max\_Torque\_Amplitude. | **✓** |  |  |
| Functional  Safety  Requirement  01-02 | The Lane Departure Warning item shall ensure that the lane departure oscillating torque frequency is below Max\_Torque\_Frequency. | **✓** |  |  |
| Functional  Safety  Requirement  02-01 | The electronic power steering ECU shall ensure that the Lane Keeping Assistance torque is applied only Max\_Duration. | **✓** |  |  |

## Warning and Degradation Concept

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Degradation Mode** | **Trigger for Degradation Mode** | **Safe State invoked?** | **Driver Warning** |
| WDC-01 | Turn off Lane Departure Warning functionality | Malfunction\_01,  Malfunction\_02 | Yes | Lane Departure Warning Malfunction Warning on Car Display |
| WDC-02 | Turn off Lane Keeping Assistance functionality | Malfunction\_03 | Yes | Lane Keeping Assistance Malfunction Warning on Car Display |