

Functional Safety Concept Lane Assistance

**Document Version: 1.3**

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



# Document history

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Editor | Description |
| 06/23/19 | 1.0 | Adam Gotlib | First draft |
| 06/23/19 | 1.1 | Adam Gotlib | Added explanation of document purpose |
| 06/23/19 | 1.2 | Adam Gotlib | Replaced refined architecture diagram |
| 06/23/19 | 1.3 | Adam Gotlib | Removed template-specific parts of the document |
|  |  |  |  |

# 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 serves the purpose of refining Safety Goals into Functional Safety Requirements and allocating them to appropriate places in the item architecture.

# 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 LDW function shall be limited. |
| Safety\_Goal\_02 | The LKA 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. |

## Preliminary Architecture



### Description of architecture elements

|  |  |
| --- | --- |
| **Element** | **Description** |
| Camera Sensor | Captures images in front of the vehicle. |
| Camera Sensor ECU | Analyses captured images and determines when the vehicle leaves the lane by mistake. |
| Car Display | Displays visual cues for the driver, informing them of functioning of the system. |
| Car Display ECU | Controls the Car Display based on inputs from other elements. |
| Driver Steering Torque Sensor | Measures the torque provided by the driver. |
| Electronic Power Steering ECU | Estimates the required amount of additional torque to be applied based on a lane assistance system torque request and the torque provided by the driver. |
| Motor | Applies additional 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). |
| 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 lane keeping item shall ensure that the lane departure oscillating torque amplitude is below Max\_Torque\_Amplitude. | C | 50 ms | The LDW function shall deactivate and display a visual warning to the driver. |
| Functional  Safety  Requirement  01-02 | The lane keeping item shall ensure that the lane departure oscillating torque frequency is below Max\_Torque\_Frequency. | C | 50 ms | The LDW function shall deactivate and display a visual warning to the driver. |

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 | The Max\_Torque\_Amplitude value shall be validated to be below acceptable level for most of the drivers. | The LDW function shall be verified to deactivate and display a visual warning to the driver within 50ms if the oscillating torque amplitude is above Max\_Torque\_Amplitude. |
| Functional  Safety  Requirement  01-02 | The Max\_Torque\_Frequency value shall be validated to be below acceptable level for most of the drivers. | The LDW function shall be verified to deactivate and display a visual warning to the driver within 50ms if the oscillating torque frequency is above 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 for Max\_Duratoin. | B | 500 ms | The LKA function shall deactivate and display a visual warning to the driver. |

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 | The Max\_Duration value shall be validated to be shorter than time needed for a driver to lose attention. | The LKA function shall be verified to deactivate and display a visual warning to the driver within 500ms if the lane keeping assistance torque is applied for more than Max\_Duratoin. |

## 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 keeping item shall ensure that the lane departure oscillating torque amplitude is below Max\_Torque\_Amplitude. | **YES** | **NO** | **NO** |
| Functional  Safety  Requirement  01-02 | The lane keeping item shall ensure that the lane departure oscillating torque frequency is below Max\_Torque\_Frequency. | **YES** | **NO** | **NO** |
| Functional  Safety  Requirement  02-01 | The lane keeping item shall ensure that the lane keeping assistance torque is applied only for Max\_Duratoin. | **YES** | **NO** | **NO** |

## Warning and Degradation Concept

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Degradation Mode** | **Trigger for Degradation Mode** | **Safe State invoked?** | **Driver Warning** |
| WDC-01 | Deactivate LDW function. | Malfunction\_01  Malfunction\_02 | YES | Visual display |
| WDC-02 | Deactivate LKA function. | Malfunction\_03 | YES | Visual display |