

Functional Safety Concept Lane Assistance

**Document Version: [Version]**

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



# Document history

**[Instructions: Fill in the date, version and description fields. You can fill out the Editor field with your name if you want to do so. Keep track of your editing as if this were a real world project.**

**For example, if this were your first draft or first submission, you might say version 1.0. If this is a second submission attempt, then you'd add a second line with a new date and version 2.0]**

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Editor | Description |
| 7/7/2018 | 1.0 | A. Zheng | First 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 functional safety concept documents the pertinent system high level requirements. These requirements are allocated to the various parts of the item architecture. The technical safety requirements are derived from the functional safety concept. The validation and verification method for these requirements are also included 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 provide a sufficient torque to the steering wheel. |
| Safety\_Goal\_02 | The LKA function shall be time limited so the driver cannot continuously use the system as an autonomous driving function |
| Safety\_Goal\_03 | The oscillating steering torque from the lane departure warning function shall be torque limited. |
| Safety\_Goal\_04 | The steering torque from the lane keeping function shall be torque limited. |

## Preliminary Architecture

### ../Architecture_Diagrams/graphic_asset_2.png

### 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 calculate the car position on the road with respect to the road lanes |
| Car Display | Provide feedback to the driver displaying warnings and the Lane Departure Assistance status |
| Car Display ECU | Controls 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 | Use the information received from the Driver Steering Torque Sensor and the torque requested by the Lane Keeping Assistance and Lane Warning and request the necessary torque to be applied by the motor actuator |
| Motor | Applies the torque indicated by the Electronic Power Steering ECU 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 a high torque amplitude. |
| Malfunction\_02 | Lane Departure Warning (LDW) function shall apply an oscillating steering torque to provide the driver a haptic feedback | LESS | The lane departure warning function applies an oscillating torque with a very low torque amplitude. |
| 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 results in a 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 stays below the max torque amplitude. | C | 50 mS | | Turn System off |
| Functional  Safety  Requirement  01-02 | The lane keeping item shall ensure that the oscillating torque amplitude stays above the minimum torque amplitude | C | | 50 mS | Turn System off |

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 the max torque amplitude chosen is small enough that the driver is able to maintain control of the vehicle | Verify that the system is in the off state if the max torque amplitude is exceeded |
| Functional  Safety  Requirement  01-02 | Test and validate that the max torque amplitude chosen is large enough that the driver is able to respond to the vehicle | Verify that the system is in the off state if the minimum torque amplitude 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 control unit shall ensure that the lane keeping assistance torque is applied only until a max duration. | B | 500 ms | Turn system off |

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 selected forces drivers to re-take control of the steering wheel | Verify that the system does turn off after the 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 keeping item shall ensure that the lane departure oscillating torque amplitude stays below the max torque amplitude. | **x** |  |  |
| Functional  Safety  Requirement  01-02 | The lane keeping item shall ensure that the oscillating torque amplitude stays above the minimum torque amplitude | **x** |  |  |
| Functional  Safety  Requirement  02-01 | The electronic power steering control unit shall ensure that the lane keeping assistance torque is applied only until a max duration. | **x** |  |  |

## Warning and Degradation Concept

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Degradation Mode** | **Trigger for Degradation Mode** | **Safe State invoked?** | **Driver Warning** |
| WDC-01 | Turn System off | Malfunction 01  Malfunction 02 | Yes | Dashboard warning light |
| WDC-02 | Turn System off | Malfunction 03 | Yes | Dashboard warning light |