

Functional Safety Concept Lane Assistance

**Document Version: [Version]**

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



# Document history

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Editor | Description |
| Feb 28, 2019 | 1.0 | Junxun Luo | First submit |
| Mar 26, 2019 | 2.0 | Junxun Luo | Revised by review comments |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# 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

This document identifies the high-level system safety requirements which are allocated to different parts of the item architecture. Technical safety requirements will be derived from these safety concepts. It also presents instructions on how to validate and verify the requirements.

# 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 (LDW) function shall be limited. |
| Safety\_Goal\_02 | The Lane Keeping Assistance function shall be time limited. The additional steering torque shall end after a given time interval so that the driver cannot misuse the system for autonomous driving. |
| Safety\_Goal\_03 | The Lane Keeping Assistance function shall be deactivated when the camera sensor stops working. |

## Preliminary Architecture

**[Instructions: Provide a preliminary architecture for the lane assistance item. Hint: See Lesson 3: Item Definition]**

The following figure shows the architecture of the Lane Assistance item:



### Description of architecture elements

|  |  |
| --- | --- |
| **Element** | **Description** |
| Camera Sensor | Capture rod images and provide them to the Camera Sensor ECU |
| Camera Sensor ECU | Analyze provided images to calculate the vehicle position on the lane |
| Car Display | Provide warnings and the Lane Departure Assistance status to the driver |
| Car Display ECU | Drive 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 | Analyze how hard the driver is turning the steering wheel. When it receives a warning from Camera Sensor ECU, it decides the vibration required to alert the driver, and output a torque value to the motor |
| Motor | Applies the 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

**[Instructions: Fill in the functional safety analysis table below.]**

|  |  |  |  |
| --- | --- | --- | --- |
| **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. |
| Malfunction\_04 | The Lane Departure Warning (LDW) function shall be deactivated when the camera sensor stop working. | WRONG | The Lane Departure Warning start acting randomly when the camera sensor is not working. |
| Malfunction\_05 | The Lane Departure Warning (LDW) function shall be deactivated when the camera sensor stop working. | WRONG | The Lane Keeping Assistance start acting randomly when the camera sensor is not working. |

## 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 item shall ensure that the lane departure oscillating torque amplitude is below Max\_Torque\_Amplitude. | C | 50ms (Diagnostic Test Interval + Fault Reaction Time + Time in Safe State) | LDW torque request amplitude is set to zero |
| 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 | 50ms (Diagnostic Test Interval + Fault Reaction Time + Time in Safe State) | LDW torque request frequency is set to zero |
| Functional  Safety  Requirement  01-03 | The Lane Departure Warning function shall be deactivated when the camera sensor stops working. | C | 10ms (Diagnostic Test Interval + Fault Reaction Time + Time in Safe State) | Switch Off Lane Assistance System |

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 | when the torque amplitude crosses the limit, the lane assistance output is set to zero within the 50 ms fault tolerant time interval. |
| 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. | when the torque frequency crosses the limit, the lane assistance output is set to zero within the 50 ms fault tolerant time interval. |
| Functional  Safety  Requirement  01-03 | Validate Lane Departure Warning is off when the camera sensor is not working. | Verify the Lane Departure Warning is never on when the camera sensor is not working. |

**[Instructions: Fill in the functional safety requirements for the lane keeping assistance]**

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 for only Max\_Duration | B | 500 ms | LKA torque request amplitude and frequency is set to zero |
| Functional  Safety  Requirement  02-02 | The Lane Keeping assistance shall be deactivated when the electronic power steering ECU detects the camera sensor is not working. | C | 100 ms | Switch Off Lane Assistance System |

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 | Validate the Max\_Duration chosen not allows the driver to use the car as self-driving car. | Verify the system does deactivate if the Lane Keeping Assistance torque application exceeded Max\_Duration. |
| Functional  Safety  Requirement  02-02 | Validate the Lane Keeping assistance shall be deactivated when the camera sensor stops working. | Verify the system does deactivate the Lane Keeping Assistance if the camera sensor is not working. |

## 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. | **X** |  |  |
| Functional  Safety  Requirement  01-02 | The Lane Departure Warning item shall ensure that the lane departure oscillating torque frequency is below Max\_Torque\_Frequency. | **X** |  |  |
| Functional  Safety  Requirement  01-03 | The Lane Departure Warning function shall be deactivated when the camera sensor stops working. | **X** |  |  |
| Functional  Safety  Requirement  02-01 | The lane keeping item shall ensure that the lane keeping assistance torque is applied for only Max\_Duration | **X** |  |  |
| Functional  Safety  Requirement  02-02 | The Lane Keeping assistance shall be deactivated when the electronic power steering ECU detects the camera sensor is not working. | **X** |  |  |

## 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,  Malfunction\_04 | Yes | Lane Departure Warning Malfunction Warning on Car Display |
| WDC-02 | Turn off Lane Keeping Assistance functionality | Malfunction\_03,  Malfunction\_05 | Yes | Lane Keeping Assistance Malfunction Warning on Car Display |