

Functional Safety Concept Lane Assistance

**Document Version: [Version]**

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



# Document history

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Editor | Description |
| 2019.07.20 | 1.0 | Zhilong Lu | First Submission |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# 

# Table of Contents

Contents

[Document history 2](#_Toc16474013)

[Table of Contents 3](#_Toc16474014)

[Purpose of the Functional Safety Concept 4](#_Toc16474015)

[Inputs to the Functional Safety Concept 4](#_Toc16474016)

[Safety goals from the Hazard Analysis and Risk Assessment 4](#_Toc16474017)

[Preliminary Architecture 4](#_Toc16474018)

[Description of architecture elements 5](#_Toc16474019)

[Functional Safety Concept 6](#_Toc16474020)

[Functional Safety Analysis 6](#_Toc16474021)

[Functional Safety Requirements 7](#_Toc16474022)

[Refinement of the System Architecture 8](#_Toc16474023)

[Allocation of Functional Safety Requirements to Architecture Elements 8](#_Toc16474024)

[Warning and Degradation Concept 9](#_Toc16474025)

# Purpose of the Functional Safety Concept

The functional safety concept looks at the general functionality of the Lane Assistance item.

This document refines the safety goals into functional safety requirements. These functional safety requirements have the following attributes:

* the ASIL level
* the fault tolerant time interval, which measures how quickly a system needs to react to a hazardous situation
* the safe state, which discusses what a system looks like after it has avoided an accident

The functional safety concept also includes verification and validation.

# Inputs to the Functional Safety Concept

## Safety goals from the Hazard Analysis and Risk Assessment

|  |  |
| --- | --- |
| **ID** | **Safety Goal** |
| Safety\_Goal\_01 | The oscillating torque to the steering wheel from the lane departure warning function shall be limited. |
| Safety\_Goal\_02 | The lane keeping assistance function shall be time limited and the additional steering |
| Safety\_Goal\_03 | The electronic power steering ECU shall check that the actuator provided steering torque is only a few ms behind the demanded torque. If the actual torque is provided too late the steering support torque shall end. |
| Safety\_Goal\_04 | The electronic power steering ECU shall check whether the indicated driver steering torque from the sensor is plausible (e.g. with a model-based approach). If the indicated driver steering torque is not plausible the support torque shall end. |

## Preliminary Architecture

****

### Description of architecture elements

|  |  |
| --- | --- |
| **Element** | **Description** |
| Camera Sensor | The camera sensor reads in images from the road. |
| Camera Sensor ECU | The Camera Sensor ECU identifies when the vehicle has accidentally departed its lane and sends the appropriate messages to the Car Display ECU and the Electronic Power Steering ECU. |
| Car Display | The Car Display shows a warning light to the driver, when the vehicle leaves the lane. |
| Car Display ECU | The Car Display ECU turns on the warning light on the Car Display when it receives information from the Camera Sensor ECU that the vehicle is leaving the lane. |
| Driver Steering Torque Sensor | The Driver Steering Torque Sensor provides the torque that the driver puts on the steering wheel to the Electronic Power Steering ECU. |
| Electronic Power Steering ECU | The Electronic Power Steering ECU reads the info from the Driver Steering Torque Sensor and commands a support torque from the Motor, based on the lane info from the Camera Sensor ECU. |
| Motor | The Motor applies the demanded torque that is demanded by the Electronic Power Steering ECU onto 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 | Turn off the functionality – Set torque request to 0 |
| 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 | Turn off the functionality – Set torque request 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 | Make a study to test how drivers react to different torque amplitudes to prove that we chose an appropriate value. | Do a software test by inserting a fault into the system. When the demanded torque amplitude crosses the limit, the lane assistance output must be set to zeros within 50 ms. |
| Functional  Safety  Requirement  01-02 | Make a study to test how drivers react to different torque frequencies to prove that we chose an appropriate value. | Do a software test by inserting a fault into the system. When the demanded torque frequency crosses the limit, the lane assistance output must be set to zeros within 50 ms. |

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 ECU shall ensure that the lane keeping assistance torque is applied for only ‘Max\_Duration’. | B | 500 ms | Turn off the functionality – Set torque request 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 | Make a study to test that the time ‘Max\_Duration’ chosen really dissuades drivers from taking their hands off the wheel. | Make car or software tests 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 keeping item shall ensure that the lane departure oscillating torque amplitude is below Max\_Torque\_Amplitude. | **x** |  |  |
| Functional  Safety  Requirement  01-02 | The Electronic Power Steeriing ECU shall ensure that the oscillating torque frequency requested by the LDW function is below Max\_Torque\_Frequency. | **x** |  |  |
| Functional  Safety  Requirement  02-01 | The electronic power steering ECU shall ensure that the lane keeping assistance torque is applied for only Max\_Duration. | **x** |  |  |

## Warning and Degradation Concept

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Degradation Mode** | **Trigger for Degradation Mode** | **Safe State invoked?** | **Driver Warning** |
| WDC-01 | Turn off the funcionality – Set torque request to 0 | The lane departure warning function applies an oscillating torque with very high torque amplitude or torque frequency (above limit). | Yes | A message on the car display shows the driver, that the lane departure warning function is not available. |
| WDC-02 | Turn off the funcionality – Set torque request to 0 | The lane keeping assistance function is not limited in time duration which leads to misuse as an autonomous driving function. | Yes | A message on the car display shows the driver, that the lane keeping assistance function is not available. |