

Functional Safety Concept Lane Assistance

**Document Version: [RC1]**

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



# Document history

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Editor | Description |
| 09/10/2017 | 0.1 | Gustavo Espindola | First draft |
| 11/10/2017 | 1 | Gustavo Espindola | Release candidate |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# Table of Contents

Inhalt

[Document history 2](#_Toc495527311)

[Table of Contents 2](#_Toc495527312)

[Purpose of the Functional Safety Concept 3](#_Toc495527313)

[Inputs to the Functional Safety Concept 3](#_Toc495527314)

[Safety goals from the Hazard Analysis and Risk Assessment 3](#_Toc495527315)

[Preliminary Architecture 3](#_Toc495527316)

[Description of architecture elements 4](#_Toc495527317)

[Functional Safety Concept 4](#_Toc495527318)

[Functional Safety Analysis 4](#_Toc495527319)

[Functional Safety Requirements 5](#_Toc495527320)

[Refinement of the System Architecture 7](#_Toc495527321)

[Allocation of Functional Safety Requirements to Architecture Elements 7](#_Toc495527322)

[Warning and Degradation Concept 8](#_Toc495527323)

# Purpose of the Functional Safety Concept

This document is intended to map the safety goals to a specific ECU, sub-system or system**.**

# Inputs to the Functional Safety Concept

## Safety goals from the Hazard Analysis and Risk Assessment

|  |  |
| --- | --- |
| **ID** | **Safety Goal** |
| Safety\_Goal\_01 | The vibration applied to the steering wheel shall be limited. |
| Safety\_Goal\_02 | The function lane keep assistance shall be limited in time. The additional torque shall end after the configured time. |

## Preliminary Architecture



### Description of architecture elements

|  |  |
| --- | --- |
| **Element** | **Description** |
| Camera Sensor | Obtains the image as raw data. |
| Camera Sensor ECU | Processes the image and extracts the lines of the lane.  With that information requests the correction torque needed to stay on the lane. |
| Car Display | Shows information about the state of the system |
| Car Display ECU | Interprets the signals from other ECU’s and sends the command to the Car display to show them. |
| Driver Steering Torque Sensor | This sensor gives feedback on the force applied to the steering wheel, either by the driver or by the LKA system. |
| Electronic Power Steering ECU | This ECU is responsible of controlling the signals sent to the motor and its correct behavior. |
| Motor | Is the actuator which applies the torque to steering wheel which finally corrects the trajectory of the vehicle. |

# 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 LDW applies an oscillating torque which amplitude is above the limit and thus very high. |
| Malfunction\_02 | Lane Departure Warning (LDW) function shall apply an oscillating steering torque to provide the driver a haptic feedback | MORE | The LDW warning applies an oscillating torque at a frequency above the limit and thus very high. |
| Malfunction\_03 | Lane Keeping Assistance (LKA) function shall apply the steering torque when active in order to stay in ego lane | NO | The LKA functionality is not limited in duration, this leads to abuse from the user which uses it as a full autonomous car. |

## 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 electronic power steering ECU shall limit the alert for the LDW, so the amplitude of the oscillating torque is less than Max\_Torque\_Amplitude | C | 50ms | LDW requested torque is set to zero.  The failure is shown in the car display and recorded. |
| Functional  Safety  Requirement  01-02 | The electronic power steering ECU shall limit the alert for the LDW, so the frequency of the oscillating torque is less than Max\_Torque\_Frequency | C | 50ms | LDW requested torque is set to zero.  The failure is shown in the car display and recorded. |

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 if a driver is capable of perceive the torque at the nominal amplitude. | Verify that the torque goes to zero after requesting a value above the limit, and the lamp goes on, This within 50ms after the failure. |
| Functional  Safety  Requirement  01-02 | Validate if a driver is capable of perceive the torque at the nominal frequency. | Verify that the torque goes to zero after requesting a value above the limit, and the lamp goes on, This within 50ms after the failure. |

Lane Keeping Assistance (LKA) Requirements:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Functional Safety Requirement** | **ASIL** | **Fault Tolerant Time Interval** | **Safe State** |
| Functional  Safety  Requirement  02-01 | The power steering ECU shall limit the duration of the functionality up to a period of Max\_Duration | B | 500ms | LKA requested 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 | Validate that the active period for the functionality is short enough to make the driver alert. | Verify the deactivation of the system after Max\_duraton. |

## 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 electronic power steering ECU shall ensure that the lane departure oscillating torque amplitude is below Max\_Torque\_Amplitude | **X** |  |  |
| Functional  Safety  Requirement  01-02 | The electronic power steering ECU shall ensure that the lane departure oscillating torque frequency 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 | LDW functionality is deactivated and lamp turned on. | Requested oscillation amplitude is > Max\_Torque\_Amplitude OR Requested oscillation frequency is > Max\_Torque\_Frequency | Yes | Yes, through lamp in the dash board. |
| WDC-02 | LKA functionality is deactivated and lamp turned on. | LKA functionality is active after Max\_Duration | Yes | Yes, through lamp in the dash board. |