

Functional Safety Concept Lane Assistance

**Document Version: [Version]**

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



# Document history

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Editor | Description |
| 9/18/2017 | 1.0 | Dr. Martin Pfeifle | First Version of the Functional Safety Concept for Lane Assistance |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# Table of Contents

Contents

[Document history 1](#_Toc493614044)

[Table of Contents 2](#_Toc493614045)

[Purpose of the Functional Safety Concept 3](#_Toc493614046)

[Inputs to the Functional Safety Concept 3](#_Toc493614047)

[Safety goals from the Hazard Analysis and Risk Assessment 3](#_Toc493614048)

[Preliminary Architecture 4](#_Toc493614049)

[Description of architecture elements 4](#_Toc493614050)

[Functional Safety Concept 5](#_Toc493614051)

[Functional Safety Analysis 5](#_Toc493614052)

[Functional Safety Requirements 6](#_Toc493614053)

[Refinement of the System Architecture 8](#_Toc493614054)

[**** 8](#_Toc493614055)

[Allocation of Functional Safety Requirements to Architecture Elements 8](#_Toc493614056)

[Warning and Degradation Concept 9](#_Toc493614057)

# Purpose of the Functional Safety Concept

The functional safety concept describes the high-level safety functionality of the system.

# Inputs to the Functional Safety Concept

## Safety goals from the Hazard Analysis and Risk Assessment

|  |  |
| --- | --- |
| **ID** | **Safety Goal** |
| Safety\_Goal\_01 | Limit the magnitude and frequency of the oscillating torque |
| Safety\_Goal\_02 | System must switch off if lanes are not corrected by the camera. Responsibility needs to be passed to the driver. |
| Safety\_Goal\_03 | System must inform the driver that the sensors are not working properly anymore, slow down and pass the responsibility to the driver |
| Safety\_Goal\_04 | The controlling unit / execution model needs to publish steering and acceleration values at least values every 30ms |

## 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 information to the driver which reflect the status of the system, i.e. whether it is working normally or whether an error situation occurred and the driver needs to take over. |
| Car Display ECU | The Car Display ECU does the graphical rendering of the information which are depicted. It activates lamps or other display modules according to the current status of the system. Basically, it prepared the information so that it can be shown on the Car Display element. |
| Driver Steering Torque Sensor | A sensor that outputs the torque applied by the driver to the steering wheel |
| Electronic Power Steering ECU | A control module that fuses the driver steering torque signal, requested steering wheel torque from the camera sensor ECU, and the motor information to create an actuator output signal. |
| Motor | An actuator that adds torque to the steering system in either direction (clockwise or counterclockwise) |

# 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 applying the steering torque as the lanes are not detected properly by the camera system |

## 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 | 50ms | Lane keeping item output torque = 0 |
| Functional  Safety  Requirement  01-02 | The lane keeping item shall ensure that the lane departure oscillating torque amplitude is below Max\_Torque\_Frequency | C | 50ms | Lane keeping item output torque = 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 | Acceptance Criteria  100% of drivers are able to regain steering control  Event  Software produce a torque signal which exceeds the maximum  1.5 \* Max\_Torque\_Amplitude  Method  Vehicle on test track with test driver | Criteria  Lane\_Keep\_Torque = 0 within 50ms of event  Event  Fault injection by RAM address write, requested torque amplitude exceeds limit  Method  Hardware-in-the-loop verification |
| Functional  Safety  Requirement  01-02 | Acceptance Criteria  100% of drivers are able to regain steering control  Event  Software produce a torque signal which exceeds the maximum  1.5 \* Max\_Torque\_Frequency  Method  Vehicle on test track with test driver | Criteria  Lane\_Keep\_Torque = 0 within 50ms of event  Event  Fault injection by RAM address write, requested torque frequency exceeds limit  Method  Hardware-in-the-loop verification |

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 | 500ms | Lane keeping item output torque = 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 | Criteria  100% of drivers are able to regain steering control  Event  Driver removes hands from wheel with system active, retakes control after system is disabled by functional safety feature  Method  Vehicle on test track with driving coaches and various drivers | Criteria  Lane\_Keep\_Torque = 0 within 500ms of event  Event  Fault injection by RAM address write, requested lane keep assistance torque remains active indefinitely  Method  Hardware-in-the-loop verification |

## Refinement of the System Architecture

## **C:\Martin\Udacity\Term3\FunctionalSafety\CarND-Functional-Safety-Project\Architecture_Diagrams\graphic_asset_3.png**

## 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 lane keeping item shall ensure that the lane departure oscillating torque amplitude 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 | Functionality is turned off | Malfunction\_01 | Yes,  immediately | audible warning signal combined with a pop-up message on instrument cluster |
| WDC-02 | Functionality is turned off | Malfunction\_02 | Yes,  immediately | audible warning signal combined with a pop-up message on instrument cluster |