

Functional Safety Concept Lane Assistance

**Document Version: [Version]**

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



# Document history

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Editor | Description |
| 20-06-2018 | 1.0 | Shubham | 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 looks at the item from a higher level. We don’t dive into technical details when working with Functional Safety concept. It looks at the general functionality of the item. The objective here is to reduce the identified risks to the acceptable levels.

# Inputs to the Functional Safety Concept

## Safety goals from the Hazard Analysis and Risk Assessment

|  |  |
| --- | --- |
| **ID** | **Safety Goal** |
| Safety\_Goal\_01 | Oscillating torque should be below a given limit |
| Safety\_Goal\_02 | Lane assistance system should be active for some time interval |

## Preliminary Architecture



Figure 1: Lane Assistance System Architecture

### Description of architecture elements

|  |  |
| --- | --- |
| **Element** | **Description** |
| Camera Sensor | Captures images and feed them to Camera Sensor ECU. |
| Camera Sensor ECU | Process the images provided by camera. Detect lane lines and in case of lane departure warn Car display ECU and send message to Electronic Power Steering ECU. |
| Car Display | Display the status of the systems and warnings in case of lane departure or any potential malfunction |
| Car Display ECU | It takes the input from the Camera and other sensors and controls the things displayed on the Car display |
| Driver Steering Torque Sensor | It measures the torque applied to the steering wheel. |
| Electronic Power Steering ECU | It takes input from Camera ECU and Driver steering Torque sensor and then decides what amount of torque should be applied on the steering wheel. |
| Motor | It is actuated by the input provided by the Electronic power steering ECU. |

# 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 item applies an oscillating torque with very high amplitude which is above threshold |
| 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 item applies an oscillating torque with very high frequency which is above threshold |
| Malfunction\_03 | Lane Keeping Assistance (LKA) function shall apply the steering torque when active in order to stay in ego lane | NO | The Lane assistance system is active all the time, the user might use it incorrectly as 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 | 1. The lane keeping item shall ensure that the lane departure oscillating torque amplitude is below Max\_Torque\_Amplitude | C | 50ms | Set lane departure Warning torque request amplitude to zero |
| Functional  Safety  Requirement  01-02 | 1. The lane keeping item shall ensure that the lane departure oscillating torque frequency is below Max\_Torque\_Frequency | C | 50ms | Set lane departure warning torque request frequency to zero |

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 | Value of Max\_Torque\_Amplitude should be such that it is high enough to warn the driver and it is low enough so that driver won’t lose control | Validate whether the system turns off in case value of torque amplitude exceeds the value of Max\_Torque\_Amplitude. |
| Functional  Safety  Requirement  01-02 | Value of Max\_Torque\_Frequency should be such that it is high enough to warn the driver and it is low enough so that driver won’t lose control | Validate whether the system turns off in case value of torque frequency exceeds the value of Max\_Torque\_Frequency. |

**[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 | Lane Keeping Assistance Function will be active for a limited time Max\_Duration | B | 500ms | Set Lane Keeping Assistance torque amplitude to 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 | Value of Max\_Duration should be such that it is high enough to bring vehicle back in the center of ego lane and small enough to discourage driver taking his hands off the steering wheel | Verify that the function turns off after the Max\_Duration is exceeded |

## Refinement of the System Architecture

## **C:\Users\shubham08\CarND-Functional-Safety-Project\Architecture_Diagrams\graphic_asset_3.png**

Figure 2: Refined Architecture of Lane Assistance System

## 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 make sure that the oscillation amplitude generated by the Lane departure warning system should be below Max\_Torque\_Amplitude | **Responsible** | **Not Responsible** | **Not Responsible** |
| Functional  Safety  Requirement  01-02 | The Electronic Power Steering ECU shall make sure that the oscillation frequency generated by the Lane departure warning system should be below Max\_Torque\_Frequency | **Responsible** | **Not Responsible** | **Not Responsible** |
| Functional  Safety  Requirement  02-01 | The Electronic Power Steering shall ensure that the torque applied by the lane keeping system is being applied for a maximum duration of Max\_Duration not more than that. | **Responsible** | **Not Responsible** | **Not Responsible** |

## Warning and Degradation Concept

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Degradation Mode** | **Trigger for Degradation Mode** | **Safe State invoked?** | **Driver Warning** |
| WDC-01 | Turn OFF the functionality | Malfunction\_01  Malfucntion\_02 | Yes | Warning Light on Dashboard, and warnings displayed on car display |
| WDC-02 | Turn OFF the functionality | Malfunction\_03 | Yes | Warning Light on Dashboard, and warnings displayed on car display |