

Functional Safety Concept Lane Assistance

**Document Version: 1.0**

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



# Document history

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Editor | Description |
| 21/5/2018 | 0.1 | Kapil Saini | Initial draft |
| 23/5/2018 | 1.0 | Kapil Saini | Finalized document |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# 

# 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

Purpose of functional safety concept is to describe the implementation of the independent safety solutions for a defined item from a higher level without delving into the technical details of the system. The primary focus here is to reduce the risks below than acceptable levels.

# 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 function shall be limited. |
| Safety\_Goal\_02 | The Lane Keeping Assistance system shall be time limited, thus after a lane keeping maneuvers, the control is given back to the driver so that it can’t be misused. |
| Safety\_Goal\_03 | The Lane detection system shall not be activated if the detection for a certain environment is not available. |

## Preliminary Architecture

### 

Figure Lane Assistance System Architecture

### Description of architecture elements

|  |  |
| --- | --- |
| **Element** | **Description** |
| Camera Sensor | Sensors to capture environmental information as images and provide them to the camera sensor ECU continuously. |
| Camera Sensor ECU | A processor unit to process acquired images by camera sensors to detect Lane Lines and calculate car positions w.r.t. to lane lines. |
| Car Display | Display device to display system status and warnings during system malfunctions to driver. |
| Car Display ECU | A processor chip controlling car displays by processing data from the camera sensor ECU. |
| Driver Steering Torque Sensor | Sensor to measures the torque applied to the steering wheel. |
| Electronic Power Steering ECU | A processor chip for processing data from camera sensor ECU and torque sensor. |
| Motor | An electric motor that interpret the EPS ECU data to control 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 | LDW function applies oscillating torque of a very high (above limit) **amplitude**. |
| Malfunction\_02 | Lane Departure Warning (LDW) function shall apply an oscillating steering torque to provide the driver a haptic feedback | MORE | LDW function applies oscillating torque of a very high (above limit) **frequency**. |
| Malfunction\_03 | Lane Keeping Assistance (LKA) function shall apply the steering torque when active in order to stay in ego lane | NO | The LKA doesn’t have a time limiting function resulting in its 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 warning torque **amplitude** is below **Max\_Torque\_Amplitude** | C | 50ms | Turn off LDW |
| Functional  Safety  Requirement  01-02 | The lane keeping item shall ensure that the lane departure warning torque **frequency** is below **Max\_Torque\_Frequency** | C | 50ms | Turn off LDW |

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 | Set the value of Max\_Torque\_Amplitude such that it is adequate enough to warn the driver without causing steering loss. | Validate whether the system turns off when Max\_Torque\_Amplitude is exceeded within 50ms of fault tolerant. |
| Functional  Safety  Requirement  01-02 | Set the value of Max\_Torque\_Frequency such that it is enough to warn the driver without causing steering loss. | Validate whether the system turns off when Max\_Torque\_Amplitude exceeds fault tolerant limits. |

Lane Keeping Assistance (LKA) Requirements:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Functional Safety Requirement** | **ASIL** | **Fault Tolerant Time Interval** | **Safe State** |
| Functional  Safety  Requirement  02-01 | Ensure that LKA torque is applied only for a limited time not more than Max\_Duration | B | 500 ms | Turn off LKA setting torque 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 | Test if LKA is active until the Max\_Duration is reached and post warning light turns on. | LKA is turned off when Max\_Duration is reached |

## Refinement of the System Architecture

## D:\CnD\Projects\CarND-Functional-Safety-Project-master\Architecture_Diagrams\graphic_asset_3.png

Figure 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 warning torque **amplitude** is below **Max\_Torque\_Amplitude** | **X** |  |  |
| Functional  Safety  Requirement  01-02 | The lane keeping item shall ensure that the lane departure warning torque **frequency** is below **Max\_Torque\_Frequency** | **X** |  |  |
| Functional  Safety  Requirement  02-01 | Test if LKA is active until the Max\_Duration is reached and post warning light turns on. | **X** |  |  |

## Warning and Degradation Concept

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Degradation Mode** | **Trigger for Degradation Mode** | **Safe State invoked?** | **Driver Warning** |
| WDC-01 | Turn off the functionality | **Malfunction\_01**  Is\_Max\_Torque\_ Exceeded  “Lane Departure Warning (LDW) function shall apply an oscillating steering torque to provide the driver a haptic feedback” | Yes | Turn on warning light on car display and dashboard. |
| WDC-02 | Turn off the functionality | **Malfunction\_02**  Is\_Max\_Duration \_Exceeded  “Lane Departure Warning (LDW) function shall apply an oscillating steering torque to provide the driver a haptic feedback” | Yes | Turn on warning light on car display and dashboard |