

Functional Safety Concept Lane Assistance

**Document Version: [Version]**

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



# Document history

**[Instructions: Fill in the date, version and description fields. You can fill out the Editor field with your name if you want to do so. Keep track of your editing as if this were a real world project.**

**For example, if this were your first draft or first submission, you might say version 1.0. If this is a second submission attempt, then you'd add a second line with a new date and version 2.0]**

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Editor | Description |
| 03.06.2018 | 1.1 | Ankith Manjunath | Functional safety concept first version |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# 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 main higher view of functional safety concept for a system under test is to make the system functionally safe. Functionally safe system has to reduce the impact of occuring hazardous situations.

# Inputs to the Functional Safety Concept

## Safety goals from the Hazard Analysis and Risk Assessment

|  |  |
| --- | --- |
| **ID** | **Safety Goal** |
| Safety\_Goal\_01 | The lane departure warning subsystem shall apply an oscillating torque less than the limit |
| Safety\_Goal\_02 | The lane keeping assistance shall be time limited and shall apply steering torque for a limited period of time |

## Preliminary Architecture

****

### Description of architecture elements

**[**

|  |  |
| --- | --- |
| **Element** | **Description** |
| Camera Sensor | Provide video feed of the road in front of the vehicle |
| Camera Sensor ECU | Detect lane markings from the video feed. Detect the position of the vehicle from the center of the lane. |
| Car Display | Display to the driver if functionality is on/off. Display the driver for a gradual degradation |
| Car Display ECU | Receive data about function on/off and also for function gradual degradation |
| Driver Steering Torque Sensor | Sense the steering wheel torque from the driver |
| Electronic Power Steering ECU | Determine the amount of steering torque needed for the functionality and normal operation mode |
| Motor | Provide the required torque from the software torque input |

# 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 lead 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 torque amplitude by lane departure warning system is below MAX\_TORQUE\_AMPLITUDE | C | 50ms | Vibration torque amplitude below Max\_Torque\_Amplitude. |
| Functional  Safety  Requirement  01-02 | The lane keeping item shall ensure that the torque frequency by the lane departure warning is below MAX\_TORQUE\_FREQUENCY | C | 50ms | Vibration torque amplitude below Max\_Torque\_Frequency. |

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 | Choose a suitable value for MAX\_TORQUE\_AMPLITUDE | Verify the FTTI and safe state degradation using the validated MAX\_TORQUE\_AMPLITUDE |
| Functional  Safety  Requirement  01-02 | Choose a suitable value for MAX\_TORQUE\_FREQUENCY | Verify the FTTI and safe state degradation using the validated MAX\_TORQUE\_FREQUENCY |

Lane Keeping Assistance (LKA) Requirements:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Functional Safety Requirement** | **ASIL** | **Fault Tolerant Time Interval** | **Safe State** |
| Functional  Safety  Requirement  02-01 | The lane keeping item shall ensure that the steering torque TIME\_FOR\_TORQUE is applied for a limited period of time . | B | 500ms | Lane Keeping Assistance 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 the TIME\_FOR\_TORQUE such that the system is not misinterpreted as an autonomous function | The FTTI and safe state is verfied using the validated TIME\_FOR\_TORQUE |

## 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 torque amplitude by lane departure warning system is below MAX\_TORQUE\_AMPLITUDE | **x** | **-** | **-** |
| Functional  Safety  Requirement  01-02 | The lane keeping item shall ensure that the torque frequency by the lane departure warning is below MAX\_TORQUE\_FREQUENCY | **x** | **-** | **-** |
| Functional  Safety  Requirement  02-01 | The lane keeping item shall ensure that the steering torque TIME\_FOR\_TORQUE is applied for a limited period of time . | **x** | **-** | **-** |

## Warning and Degradation Concept

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Degradation Mode** | **Trigger for Degradation Mode** | **Safe State invoked?** | **Driver Warning** |
| WDC-01 | Turn off functionality | Malfunction\_01  Malfunction\_02 | Yes | LDW warning on the screen |
| WDC-02 | Turn off functionality | Malfunction\_03 | Yes | LKA warning on the screen, Driver to take over the car |