

Functional Safety Concept Lane Assistance

**Document Version: [1.0]**

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



# Document history

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Editor | Description |
| 20 June, 2018 | 1.0 | Akhil Suri | Initial Submission |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# 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 documents the identified system high level requirements. These requirements are allocated to different parts of the item architecture. Technical safety requirements will be derived from the safety concepts. The validation and verification concepts for these requirements are presented as well.

# 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 shall be time limited and the additional steering torque shall end after a given time interval so that the driver cannot misuse the system for autonomous driving. |

## Preliminary Architecture



### Description of architecture elements

|  |  |
| --- | --- |
| **Element** | **Description** |
| Camera Sensor | To provide the images captured from camera to the camera Sensor ECU. |
| Camera Sensor ECU | Images will be analyzed and will calculate the car position and detect the lane lines. |
| Car Display | It will display warning to the driver. |
| Car Display ECU | It will show the lane departure and lane keeping assistance warning status, by controlling the car display component. |
| Driver Steering Torque Sensor | It measures the torque applied to the steering wheel. |
| Electronic Power Steering ECU | It will process the inputs from Driver steering torque sensor, Camera Sensor ECU and request  the required torque which will be applied by the motor. |
| Motor | The component is responsible for applying the work required to produce the torque required to execute actions delivered to the 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 oscillating amplitude is too high. |
| Malfunction\_02 | Lane Departure Warning (LDW) function shall apply an oscillating steering torque to provide the driver a haptic feedback | MORE | The oscillating frequency is too high. |
| Malfunction\_03 | Lane Keeping Assistance (LKA) function shall apply the steering torque when active in order to stay in ego lane | NO | The lane departure oscillating torque amplitude is below Max\_Torque\_Amplitude |

## 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 departure oscillating torque amplitude is below Max\_Torque\_Amplitude | C | 50 ms | Turn off the functionality or system |
| Functional  Safety  Requirement  01-02 | The lane departure oscillating torque frequency is below Max\_Torque\_Frequency | C | 50 ms | Turn off the functionality or system |

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 | Validating the Max\_Torque\_Amplitude and check if it is low which will not cause the steering loss. | To verify that the system goes turn off when the Max\_Torque\_Amplitude is exceeded. |
| Functional  Safety  Requirement  01-02 | Validating the Max\_Torque\_Frequency and check if it is low which will not cause the steering loss. | To verify that the system goes turn off when the Max\_Torque\_Frequency is exceeded. |

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 shall be time limited and the additional steering torque shall end after a given timer interval so that the driver cannot misuse the system for autonomous driving | B | 500 ms | Turn the system off |

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 | The max\_duration chosen really did dissuade drivers from taking their hands off the wheel | The system really does turn off if the lane keeping assistance every exceeded max\_duration. |

## 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 should be ensuring that the lane departure oscillating torque frequency is below Max\_Torque\_Frequency | **x** |  |  |
| Functional  Safety  Requirement  01-02 | The electronic power steering ECU should be ensuring that the lane departure oscillating torque Amplitude is below Max\_Torque\_Amplitude | **x** |  |  |
| Functional  Safety  Requirement  02-01 | The electronic power steering ECU should be ensuring that the lane keeping torque is applied for less than the Max\_Duration. | **x** |  |  |

## Warning and Degradation Concept

WDC-01 is for Lane Departure Warning function

WDC-02 is for Lane Keeping assistance function

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Degradation Mode** | **Trigger for Degradation Mode** | **Safe State invoked?** | **Driver Warning** |
| WDC-01 | Turn off the functionality | Malfunction\_01  Malfunction\_02 | Yes | a warning light on the dashboard |
| WDC-02 | Turn off the functionality | Malfunction\_03 | Yes | a warning light on the dashboard |