

Functional Safety Concept Lane Assistance

**Document Version: V1.0**



# 

# Document history

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Editor | Description |
| 2020/09/15 | V1.0 | Mohamed Ayman | First 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 is looking at the item from a higher level; also it looks for the general functionality of the item. By identifying the higher level requirements and allocating them to the different parts of the architecture.

# Inputs to the Functional Safety Concept

## Safety goals from the Hazard Analysis and Risk Assessment

|  |  |
| --- | --- |
| **ID** | **Safety Goal** |
| Safety\_Goal\_01 | lane keeping assistance function shall be time limited |
| Safety\_Goal\_02 | Lane Departure warning function shall be less |
| Safety\_Goal\_03 | Lane keeping assistance shall be deactivated under some environmental conditions |
| Safety\_Goal\_04 | Lane Departure warning function shall be more |

## 

## Preliminary Architecture



### Description of architecture elements

|  |  |
| --- | --- |
| **Element** | **Description** |
| Camera Sensor | Take images for the road and provide it to the Camera ECU |
| Camera Sensor ECU | Determine the position of the car according to the center of the ego lane line |
| Car Display | Display information to the driver about the item and the status of the item |
| Car Display ECU | Turn on/off warning light based on the instructions from camera ECU |
| Driver Steering Torque Sensor | Measure the torque applied to steering wheel |
| Electronic Power Steering ECU | Receive the information from the camera and give the orders to motor and receive the measurements from the torque sensor |
| Motor | Apply the torque to 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 | 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 leads to misuse as an autonomous driving function |
| Malfunction\_04 | Lane Keeping Assistance (LKA) function shall be deactivated under some environmental conditions | Wrong | The camera sensor is not working under some environmental conditions |
| Malfunction\_05 | Lane Departure Warning (LDW) function shall apply an oscillating steering torque to provide the driver a haptic feedback | Less | The lane departure warning function applies an oscillating torque with very low torque frequency (under limit) |

## 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 Electronic power steering ECU shall ensure that the lane departure oscillating torque amplitude is below Max\_toruque\_amplitude | C | 50ms | the lane departure oscillating torque amplitude is below Max\_toruque\_amplitude |
| Functional  Safety  Requirement  01-02 | The Electronic power steering ECU shall ensure that the lane departure oscillating torque frequency is below Max\_toruque\_frequency | C | 50ms | the lane departure oscillating torque frequency is below Max\_toruque\_frequency |
| Functional  Safety  Requirement  01-03 | The Electronic power steering ECU shall ensure that the lane departure oscillating torque amplitude is upper Min\_toruque\_amplitude | A | 500ms | the lane departure oscillating torque amplitude is upper Min\_toruque\_amplitude |
| Functional  Safety  Requirement  01-04 | The Electronic power steering ECU shall ensure that the lane departure oscillating torque frequency is upper Min\_toruque\_frequency | A | 500ms | the lane departure oscillating torque frequency is upper Min\_toruque\_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 | ensure that the lane departure oscillating torque amplitude is at a level could be detected by a driver | Verify that the system don't turn off when exceeded the detected amplitude |
| Functional  Safety  Requirement  01-02 | ensure that the lane departure oscillating torque frequency is at a level could be detected by a driver | Verify that the system don't turn off when exceeded the detected frequency |
| Functional  Safety  Requirement  01-03 | ensure that the lane departure oscillating torque amplitude is not very low so the driver can't detect it | Verify that the system work at acceptable level of amplitude |
| Functional  Safety  Requirement  01-04 | ensure that the lane departure oscillating torque frequency is not very low so the driver can't detect it | Verify that the system work at acceptable level of frequency |

Lane Keeping Assistance (LKA) Requirements:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Functional Safety Requirement** | **ASIL** | **Fault Tolerant Time Interval** | **Safe State** |
| Functional  Safety  Requirement  02-01 | Electronic power steering ECU 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 | C | 50ms | lane keeping assistance function shall be time limited |
| Functional  Safety  Requirement  02-02 | Lane keeping assistance function shall be deactivated in case of the camera can't work under some environmental condition | C | 50ms | Lane keeping assistance function shall be deactivated in some environmental conditions |

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 duration chosen not allow the driver to use the car at autonomous mode | Verify the system stop if it exceeded the duration |
| Functional  Safety  Requirement  02-01 | Validate the system is stopping under some environmental conditions | Verify that the system stop under some environmental conditions |

## 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 departure item shall ensure that the oscillating torque amplitude is below Max\_toruque\_amplitude | **T** |  |  |
| Functional  Safety  Requirement  01-02 | The Lane departure item shall ensure that the oscillating torque frequency is below Max\_toruque\_frequency | **T** |  |  |
| Functional  Safety  Requirement  01-03 | The Lane departure item shall ensure that the oscillating torque amplitude is upper Min\_toruque\_amplitude | **T** |  |  |
| Functional  Safety  Requirement  01-04 | The Lane departure item shall ensure that the oscillating torque frequency is upper Min\_toruque\_frequency | **T** |  |  |
| 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 | **T** |  |  |
| Functional  Safety  Requirement  02-02 | Lane keeping assistance function shall be deactivated under some environmental condition |  | **T** |  |

## Warning and Degradation Concept

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Degradation Mode** | **Trigger for Degradation Mode** | **Safe State invoked?** | **Driver Warning** |
| WDC-01 | turn off the lane departure functionality | Malfunction\_1  Malfunction\_2  Malfunction\_5 | Yes | Lane departure warning work on car display |
| WDC-02 | turn off the lane keeping assistance functionality | Malfunction\_3  Malfunction\_4 | Yes | Lane keeping assistance warning work on car display |