l

Functional Safety Concept Lane Assistance

**Document Version: [Version]**

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



# Document history

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Editor | Description |
| 12.02.2019 | 1.0 | Hiep Truong Cong | Draft |
| 15.02.2019 | 2.0 | Hiep Truong Cong | Release |

# 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 Technical Safety Concept defines how the subsystems interact at the message level and describes how the ECUs communicate with each other

# 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 function shall be time limited, and dditional steering torque shall end after a given time interval so the driver cannot misuse the system for autonomous driving |

## Preliminary Architecture



### Description of architecture elements

|  |  |
| --- | --- |
| **Element** | **Description** |
| Camera Sensor | Take images from the road |
| Camera Sensor ECU | Detecting lane lines and determining when the vehicle leaves the lane, request electronic power steering ECU to generate a demand torque, send appropriate messages to the car display ECU |
| Car Display | Display warning messages and system states |
| Car Display ECU | Process request from camera sensor ECU and prepare display information |
| Driver Steering Torque Sensor | Measure steering torque on the steering wheel, produced by the driver |
| Electronic Power Steering ECU | Receive requests from camera sensor ecu, control motor to generate torque to steering wheel, based on measured torque from driver steering torque sensor |
| Motor | Generate 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. |

## 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 oscillating torque amplitude is below Max\_Torque\_Amplitude | C | 50 ms | LDW will set the oscillating torque to 0. |
| Functional  Safety  Requirement  01-02 | The lane keeping item shall ensure that the lane departure oscillating torque frequency is below Max\_Torque\_Frequency | C | 50 ms | LDW will set the oscillating torque to 0. |

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 | Validate the Max\_Torque\_Amplitude is high enough to warn the driver but not too high, so that the driver loses control | Verify that the the lane assistance output is set to zero with within the 50 ms fault tolerant time interval, when when the torque amplitude crosses the limit |
| Functional  Safety  Requirement  01-02 | Validate the Max\_Torque\_Frequency is high enough to be detected by the driver but not too high, so that the driver loses control | Verify that the the lane assistance output is set to zero with within the 50 ms fault tolerant time interval, when when the torque frequency crosses the limit |

Lane Keeping Assistance (LKA) Requirements:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Functional Safety Requirement** | **ASIL** | **Fault Tolerant Time Interval** | **Safe State** |
| Functional  Safety  Requirement  02-01 | the electronic power steering ECU shall ensure that the lane keeping assistance torque is applied for only Max\_Duration | B | 500 ms | 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 chosen Max\_Duration not allow the driver to misuse the LKA as autonomous driving | Verify that the LKA will be deactivated if the active time 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 shall ensure that the lane departure warning oscillating torque amplitude is below Max\_Torque\_Amplitude | **x** |  |  |
| Functional  Safety  Requirement  01-02 | The electronic power steering ECU shall ensure that the lane departure warning oscillating torque frequency is below Max\_Torque\_Frequency | **x** |  |  |
| Functional  Safety  Requirement  02-01 | The electronic power steering ECU shall ensure that the lane keeping assistance torque is applied for only Max\_Duration | **x** |  |  |

## Warning and Degradation Concept

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Degradation Mode** | **Trigger for Degradation Mode** | **Safe State invoked?** | **Driver Warning** |
| WDC-01 | Lane departure warning shall be turned off | Malfunction\_01  Malfunction\_02 | yes | Warning on car display |
| WDC-02 | Lane keeping assistance shall be turned off | Malfunction\_03 | yes | Warning on car display |