

Functional Safety Concept Lane Assistance

**Document Version: 1.0**

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



# Document history

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Editor | Description |
| 2018-03-04 | 1.0 | Maximilian Wenger | Initial version |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# Table of Contents

[Document history 2](#_Toc507925136)

[Table of Contents 2](#_Toc507925137)

[Purpose of the Functional Safety Concept 3](#_Toc507925138)

[Inputs to the Functional Safety Concept 3](#_Toc507925139)

[Safety goals from the Hazard Analysis and Risk Assessment 3](#_Toc507925140)

[Preliminary Architecture 3](#_Toc507925141)

[Description of architecture elements 4](#_Toc507925142)

[Functional Safety Concept 4](#_Toc507925143)

[Functional Safety Analysis 5](#_Toc507925144)

[Functional Safety Requirements 6](#_Toc507925145)

[Refinement of the System Architecture 8](#_Toc507925146)

[Allocation of Functional Safety Requirements to Architecture Elements 9](#_Toc507925147)

[Warning and Degradation Concept 10](#_Toc507925148)

# Purpose of the Functional Safety Concept

This document specifies how the subsystems of the lane assistance item will be used to achieve functional safety goals by implementing the identified functional safety requirements.

# 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 LDW function shall be limited. |
| Safety\_Goal\_02 | The LKA function 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. |
| Safety\_Goal\_03 | The oscillating steering torque from the LDW function shall be over a certain threshold. |
| Safety\_Goal\_04 | The LKA shall warn the driver when it's sensor cannot see lane markings due to poor visibility. |

## Preliminary Architecture



### Description of architecture elements

|  |  |
| --- | --- |
| **Element** | **Description** |
| Camera Sensor | Provide images of the road to the ECU. |
| Camera Sensor ECU | Detect lane markings and position of vehicle in relation to them. |
| Car Display | Show visual information to the driver (e.g. warning light). |
| Car Display ECU | Receive information from the Camera ECU and trigger the appropriate visualization in the display. |
| Driver Steering Torque Sensor | Measure the torque applied to the steering wheel by the driver. |
| Electronic Power Steering ECU | Calculate the steering torque the motor should apply to the steering wheel from the camera and torque sensor inputs. |
| Motor | Apply 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 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 not enough torque amplitude (below driver’s sensation threshold) |
| 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 not enough torque frequency (below driver’s sensation threshold) |
| Malfunction\_06 | 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 does not work due to low visibility. |

## 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 oscillating torque amplitude is below Max\_Torque\_Amplitude. | C | 50ms | LA off (torque zero) |
| Functional  Safety  Requirement  01-02 | The electronic power steering ECU shall ensure that the oscillating torque frequency is below Max\_Torque\_Frequency. | C | 50ms | LA off (torque zero) |
| Functional  Safety  Requirement  01-03 | The electronic power steering ECU shall ensure that the oscillating torque amplitude is above Min\_Torque\_Amplitude. | B | 50ms | LA off (torque zero) |
| Functional  Safety  Requirement  01-04 | The electronic power steering ECU shall ensure that the oscillating torque frequency is above Min\_Torque\_Frequency. | B | 50ms | LA off (torque zero) |

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 | When applying the chosen Max\_Torque\_Amplitude value, over 95% of drivers must be able to sustain control over the vehicle. | If the requested torque is above Max\_Torque\_Amplitude, the commanded torque is zero. |
| Functional  Safety  Requirement  01-02 | When applying the chosen Max\_Torque\_Frequency value, over 95% of drivers must be able to sustain control over the vehicle. | If the requested torque is above Max\_Torque\_Frequency, the commanded torque is zero. |
| Functional  Safety  Requirement  01-03 | When applying the chosen Min\_Torque\_Amplitude value, over 95% of drivers must be able to feel the vibration easily. | If the requested torque is below Min\_Torque\_Amplitude, the commanded torque is zero. |
| Functional  Safety  Requirement  01-04 | When applying the chosen Min\_Torque\_Frequency value, over 95% of drivers must be able to feel the vibration easily. | If the requested torque is below Min\_Torque\_Frequency, the commanded torque is zero. |

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 | 500ms | LA off (torque zero) |
| Functional  Safety  Requirement  02-02 | The camera ECU shall warn the driver that the lane keeping assistance function is not available by setting the Low\_Visibility flag. | QM | 500ms | LA off (torque 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 | The chosen value of Max\_Duration must be sufficiently short to dissuade drivers to assume the vehicle is fully autonomous. | If the duration of applying torque is above Max\_Duration, the commanded torque is zero. |
| Functional  Safety  Requirement  02-02 | The camera ECU sets the Low\_Visibility flag if it’s lane detections are not confident enough. | If the Low\_Visibility flag is set, the commanded torque is zero. |

## 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 oscillating torque amplitude is below Max\_Torque\_Amplitude. | **x** |  |  |
| Functional  Safety  Requirement  01-02 | The electronic power steering ECU shall ensure that the oscillating torque frequency is below Max\_Torque\_Frequency. | **x** |  |  |
| Functional  Safety  Requirement  01-03 | The electronic power steering ECU shall ensure that the oscillating torque amplitude is above Min\_Torque\_Amplitude. | **x** |  |  |
| Functional  Safety  Requirement  01-04 | The electronic power steering ECU shall ensure that the oscillating torque frequency is above Min\_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** |  |  |
| Functional  Safety  Requirement  02-02 | The car display shall warn the driver that the lane keeping assistance function is not available in a low visibility environment. |  | **x** |  |

## Warning and Degradation Concept

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Degradation Mode** | **Trigger for Degradation Mode** | **Safe State invoked?** | **Driver Warning** |
| WDC-01 | Turn LA off (additional torque set to zero) | Malfunction\_01  Malfunction\_02  Malfunction\_04  Malfunction\_05 | Yes | LA malfunction warning light |
| WDC-02 | Turn LA off (additional torque set to zero) | Malfunction\_03 | Yes | LA malfunction warning light |
| WDC-03 | Turn LA off (additional torque set to zero) | Malfunction\_06 | Yes | LA malfunction warning light |