

Functional Safety Concept Lane Assistance

**Document Version: 1.0.0**

**Released on 2017-12-19**



# Document history

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Editor | Description |
| 19.12.2017 | 1.0.0 | Bernhard Rode | Initial version of the safety concept |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# Table of Contents

Table of Contents

[Document history 2](#_Toc501461503)

[Table of Contents 2](#_Toc501461504)

[Purpose of the Functional Safety Concept 3](#_Toc501461505)

[Inputs to the Functional Safety Concept 3](#_Toc501461506)

[Safety goals from the Hazard Analysis and Risk Assessment 3](#_Toc501461507)

[Preliminary Architecture 3](#_Toc501461508)

[Description of architecture elements 4](#_Toc501461509)

[Functional Safety Concept 4](#_Toc501461510)

[Functional Safety Analysis 5](#_Toc501461511)

[Functional Safety Requirements 5](#_Toc501461512)

[Refinement of the System Architecture 7](#_Toc501461513)

[Allocation of Functional Safety Requirements to Architecture Elements 7](#_Toc501461514)

[Warning and Degradation Concept 7](#_Toc501461515)

# Purpose of the Functional Safety Concept

The technical safety concept involves:

* Turning functional safety requirements into technical safety requirements
* Allocating technical safety requirements to the system architecture

# 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 | 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 |

## Preliminary Architecture



### Description of architecture elements

|  |  |
| --- | --- |
| Element | Description |
| Camera Sensor | The camera sensor reads in images from the road |
| Camera Sensor ECU | The camera sensor ECU identifies when the vehicle has accidently departed its lane, and sends the appropriate messages to the car display and the electronic power steering ECU |
| Car Display | The car display shows messages to the driver |
| Car Display ECU | The car display ECU determines when to show messages |
| Driver Steering Torque Sensor | The driver steering torque sensor detects the steering input by the driver |
| Electronic Power Steering ECU | The electronic power steering ECU determines the amount of steering sent to the wheels |
| Motor | The steering motor provides force 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 EPS ECU shall ensure that the lane departure oscillating torque amplitude is below Max\_Torque\_Amplitude | C | 50ms | LDW will set the oscillating torque amplitude to zero |
| Functional  Safety  Requirement  01-02 | The EPS ECU shall ensure that the lane departure oscillating torque frequency is below Max\_Torque\_Frequency | C | 50ms | LDW will set the oscillating torque amplitude to 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 | test how drivers react to different torque amplitudes and frequencies to prove that we chose an appropriate value | software test inserting a fault into the system and seeing what happens |
| Functional  Safety  Requirement  01-02 | test how drivers react to different torque amplitudes and frequencies to prove that we chose an appropriate value | software test inserting a fault into the system and seeing what happens |

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 | LKA will set the oscillating torque amplitude to 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 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 shall ensure that the lane departure warning oscillating torque amplitude is below Max\_Torque\_Amplitude | **responsible** |  |  |
| Functional  Safety  Requirement  01-02 | The electronic power steering ECU shall ensure that the lane departure warning oscillating torque amplitude is below Max\_Torque\_Frequency | **responsible** |  |  |
| Functional  Safety  Requirement  02-01 | The functional safety requirement needs to only be allocated to the electronic power steering ECU. | **responsible** |  |  |

## Warning and Degradation Concept

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Degradation Mode** | **Trigger for Degradation Mode** | **Safe State invoked?** | **Driver Warning** |
| WDC-01 | turn off the functionality | Steering torque exceeds maximum levels | Yes | Warning light on dashboard |
| WDC-02 | turn off the functionality | Steering torque exceeds maximum levels | Yes | Warning light on dashboard |