

Functional Safety Concept Lane Assistance

**Document Version: [Version]**

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



# Document history

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Editor | Description |
| 2018-06-17 | 1.0 | H. Kube | Initial version |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# 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 purpose of the functional safety concept is to refine safety goals in functional safety requirements and then allocate these requirements to sub-systems in the high-level 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 | The lane keeping assistance 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 autonomous driving. |
| Safety\_Goal\_03 | The lane keeping assistance shall be able to detect yellow lane markings and prefer them over white lane markings. |
| Safety\_Goal\_04 | The lane departure warning shall not apply any torque to the wheel in case the lane markings are not clearly visible. |

## Preliminary Architecture

The figure below describes the Lane Assistance item architecture.



### Description of architecture elements

|  |  |
| --- | --- |
| **Element** | **Description** |
| Camera Sensor | Captures road images and provide them to the Camera Sensor ECU |
| Camera Sensor ECU | Analyzes the road images, detect the lane markings positions, and calculates the verhicle position in respect to the ego lane. |
| Car Display | Shows the driver the lane keeping assistance warning and status. |
| Car Display ECU | Generates warning and status signals and show them on the Car Display. |
| Driver Steering Torque Sensor | Measures the torque applied by the driver to the wheel. |
| Electronic Power Steering ECU | Compares the torque measured by the Driver Steering Torque Sensor, compares this with the torque requested by the lane keeping assistance and drives the motor to apply the missing torque. |
| Motor | Applies the torque requested by the Electronic Power Steering ECU to the 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 amplitude (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 apply the steering torque when active in order to stay in ego lane | WRONG | The camera sensor might detect the wrong lane markings in road construction zones |
| Malfunction\_05 | Lane Departure Warning (LDW) function shall apply an oscillating steering torque to provide the driver a haptic feedback | WRONG | The camera sensor might detect the lane markings wrong in situation with degraded view (e. G. dense fog). |

## 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 | Lane assistance functionality is deactivated. |
| 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 | Lane assistance functionality is deactivated. |
| Safety Requirement 01-03 | The lane keeping item shall not apply any torque to the wheel if the contrast of the road images is below Min\_Image\_Contrast. | B | 50 ms | Lane assistance functionality is deactivated. |

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 | The how different drivers react to different torque value to prove that an appropriate value is chosen. | Verify that the system is turned off if the torque exceeds Max\_Torque\_Amplitude |
| Functional  Safety  Requirement  01-02 | The how different drivers react to different torque frequency to prove that an appropriate value is chosen. | Verify that the system is turned off if the torque exceeds Max\_Torque\_Frequency |
| Functional Safety Requirement 01-03 | Validate the contrast level of the road images at which the camera is just able to detect the lane markings properly. | Verify that the no torque is applied if the contrast level is below Min\_Image\_Contrast |

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 function is deactivated |
| Functional Safety Requirement 02-02 | The lane keeping assistance shall detect the color of the line markings and prefer yellow markings over white markings | C | 50 ms | Yellow lines are detected |

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 Max\_Duration chosen does not allow the driver to use the car as self-driving car. | Verify that the lane keeping assistance is deactivated after the driver does not apply any torque to the wheel for more than Max\_Duration |
| Functional Safety Requirement 02-02 | Validate that the camera can clearly distinguish yellow lines from white lines. | Verify that the yellow lines are recognized and used if they are present in the camera image. |

## 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 keeping item shall ensure that the lane departure oscillating torque amplitude is below Max\_Torque\_Amplitude. | **X** |  |  |
| Functional  Safety  Requirement  01-02 | The lane keeping item shall ensure that the lane departure oscillating torque frequency is below Max\_Torque\_Frequency. | **X** |  |  |
| Functional  Safety  Requirement  01-03 | Validate the contrast level of the road images at which the camera is just able to detect the lane markings properly. |  | **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 lane keeping assistance shall detect the color of the line markings and prefer yellow markings over white markings |  | **X** |  |

## Warning and Degradation Concept

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Degradation Mode** | **Trigger for Degradation Mode** | **Safe State invoked?** | **Driver Warning** |
| WDC-01 | Turn off Lane Departure Warning functionality | Malfunction\_01,  Malfunction\_02,  Malfunction\_05 | Yes | Lane Departure Warning indicator on car display |
| WDC-02 | Turn off Lane Keeping Assistance functionality | Malfunction\_03,  Malfunction\_04 | Yes | Lane Keeping Assistance Malfunction indicator on car display |