

Functional Safety Concept Lane Assistance

**Document Version: 1.0**

**Released on 2018-05-22**



# 

# Document history

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Editor | Description |
| 18-May-2018 | 0.1 | Carola | Initial Draft |
| 22-May-2018 | 1.0 | Carola | Updated the document after adding some point in “Hazard Analysis And Risk Assessment” document |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# 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 Functional Safety Concept document is to identify system high level requirements and allocate them to different parts of the item architecture without going into technical detail. Finally, to prove that a system actually meets requirements, they have to be verified and validated. The information in the functional safety analysis comes from the hazard analysis and risk assessment. The guide words help to analyze functions and malfunctions methodically. The malfunctions are then converted into functional safety requirements

# Inputs to the Functional Safety Concept

## Safety goals from the Hazard Analysis and Risk Assessment

|  |  |
| --- | --- |
| **ID** | **Safety Goal** |
| Safety\_Goal\_01 | Reduce the vibrating torque of steering wheel to bring to the acceptance level. |
| Safety\_Goal\_02 | Total functional time of the LKA should be reduced. |
| Safety\_Goal\_03 | While driving in the driving on *off road conditions*, the LDW function should be turned off. |
| Safety\_Goal\_04 | When there is no response from the camera sensors then the LKA function should be deactivated driver should be warned about the deactivation by displaying the issue on the car dashboard. |

## Preliminary Architecture



### Description of architecture elements

|  |  |
| --- | --- |
| **Element** | **Description** |
| Camera Sensor | This Sensor responsible for capturing road images and provide them to the Camera Sensor ECU |
| Camera Sensor ECU | Electronic Control Unit (ECU) responsible for calculates the deviation from center lane and request for oscillation torque(LDW) wherever required. |
| Car Display | Displays status of (active/inactive) LDW & LKA function, thus informing the driver about the current status so that driver is well informed before any mishap happens |
| Car Display ECU | Electronic Control Unit (ECU) responsible for displaying status of (active/inactive) LDW & LKA function on the Car Display. |
| Driver Steering Torque Sensor | Sensor responsible for measuring the torque applied on driver wheel, this calculation is based on the signals received. |
| Electronic Power Steering ECU | Electronic Control Unit (ECU) responsible for calculating extra torque need to be applied for LKA function and vibrates steering wheel when LDW is activated. |
| Motor | An electric motor that applies the torque indicated by the Electronic Power Steering ECU 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 | Above the limit an oscillating torque with very high torque amplitude is applied by the lane departure warning. |
| 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 which had a 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 misguiding the autonomous driving system. |
| Malfunction\_04 | Lane Keeping Assistance (LKA) function shall apply the steering torque when active in order to stay in ego lane | WRONG | When camera sensor is not working,  the lane keeping assistance function is activated randomly. |

## 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 should ensure that the lane departure oscillating torque amplitude is below Max\_Torque\_Amplitude value. | C | 50 ms | Turn Off System |
| Functional  Safety  Requirement  01-02 | The lane keeping item should ensure that the lane departure oscillating torque frequency is below Max\_Torque\_Frequency value | C | 50 ms | Turn Off System |

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 that the Max\_Torque\_Amplitude value chosen is low enough that the driver should not loss control over the car and high enough to be detected by driver, so that driver can act in given time frame | Verify that the system does turn off within a fault tolerant time interval, if Max\_Torque\_Amplitude is exceeded the given limit. |
| Functional  Safety  Requirement  01-02 | Validate that the Max\_Torque\_Frequency value chosen is low enough that the driver does not loss control over the car and high enough to be detected by driver, so that driver can act in given time frame | Verify that the system does turn off within a fault tolerant time interval, if Max\_Torque\_Frequency is exceeded the given 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 should ensure that the lane keeping assistance torque is applied for only Max\_Duration value | B | 500 ms | Turn Off System |
| Functional  Safety  Requirement  02-01 | The electronic power steering ECU should be deactivated​ ​when​ ​the​ ​electronic​ ​power steering​ ​ECU​ ​detects​ ​the no response (not working state)​ ​of the camera sensor. | B | 50 ms | Turn Off System |

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 that the value chosen for Max\_Duration dissuades drivers from taking their hands off the wheel. | Verify that the system should turn off within a fault tolerant time interval, if the lane keeping assistance ever exceeds Max\_Duration limit. |
| Functional  Safety  Requirement  02-02 | Validate​ ​that Lane​ ​Keeping assistance​ ​should​ ​be​ ​deactivated when​ ​the​ ​camera​ ​sensor​ ​stop working. | Verify that the system should turn off within a fault tolerant time interval, if the camera sensor stopped working. |

## 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 oscillating torque amplitude is below Max\_Torque\_Amplitude, this would be ensured by the lane keeping item. | **X** |  |  |
| Functional  Safety  Requirement  01-02 | The lane departure oscillating torque frequency is below Max\_Torque\_Frequency, this would be ensured by the lane keeping item. | **X** |  |  |
| Functional  Safety  Requirement  02-01 | The lane keeping assistance torque is applied for only Max\_Duration, this would be ensured by the electronic power steering ECU. | **X** |  |  |
| Functional  Safety  Requirement  02-02 | When the camera sensors are not responding then electronic power steering ECU should be deactivated. | **X** |  |  |

## Warning and Degradation Concept

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Degradation Mode** | **Trigger for Degradation Mode** | **Safe State invoked?** | **Driver Warning** |
| WDC-01 | Turn off LDW functionality | Malfunction\_01,  Malfunction\_02 | Yes | Turn on warning light of the LDW functionality |
| WDC-02 | Turn off LKA functionality | Malfunction\_03,  Malfunction\_04 | Yes | Turn on warning light of the LKA functionality |