

Technical Safety Concept Lane Assistance

**Document Version: 1.0**

**Released on 2018-06-22**



# Document history

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Editor | Description |
| 2018-06-22 | 1.0 | Deepak Kumar Singh | Technical Safety Document |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# 

# Table of Contents

[Purpose of the Technical Safety Concept 4](#_Toc517399549)

[Inputs to the Technical Safety Concept 4](#_Toc517399550)

[Functional Safety Requirements 4](#_Toc517399551)

[Refined System Architecture from Functional Safety Concept 5](#_Toc517399552)

[Functional overview of architecture elements 5](#_Toc517399553)

[Technical Safety Concept 6](#_Toc517399554)

[Technical Safety Requirements 6](#_Toc517399555)

[Refinement of the System Architecture 10](#_Toc517399556)

[Allocation of Technical Safety Requirements to Architecture Elements 10](#_Toc517399557)

[Warning and Degradation Concept 11](#_Toc517399558)

# 

# Purpose of the Technical Safety Concept

To convert functional safety requirements into technical safety requirements and assign the requirements to system architecture.

# Inputs to the Technical Safety Concept

## Functional Safety Requirements

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Functional Safety Requirement** | **ASIL** | **Fault Tolerant Time Interval** | **Safe State** |
| Functional  Safety  Requirement  01-01 | Lane departure warning system should limit the Oscillation of steering wheel below Max Torque Amplitude. | C | 50 ms | Torque amplitude set to 0 |
| Functional  Safety  Requirement  01-02 | The departure warning system shall ensure that the lane departure oscillating torque frequency is below Max Torque Frequency. | C | 50 ms | Torque frequency set to 0 |
| Functional  Safety  Requirement  02-01 | The lane keeping assistance system shall be time limited. | B | 500ms | Steering torque set to 0 |

## Refined System Architecture from Functional Safety Concept



### 

### Functional overview of architecture elements

|  |  |
| --- | --- |
| **Element** | **Description** |
| Camera Sensor | Sends captured images to camera sensor ECU |
| Camera Sensor ECU - Lane Sensing | Lane identification in camera images |
| Camera Sensor ECU - Torque request generator | Generates torque requests and sends to EPS ECU |
| Car Display | Displays warning messages |
| Car Display ECU - Lane Assistance On/Off Status | Sends display request to car display according to Lane Assistance system on/off status |
| Car Display ECU - Lane Assistant Active/Inactive | Sends display request to car display according to Lane Assistance system active/inactive status |
| Car Display ECU - Lane Assistance malfunction warning | Sends display request to car display according to Lane Assistance system malfunction status |
| Driver Steering Torque Sensor | Monitors torque applied by the driver |
| Electronic Power Steering (EPS) ECU - Driver Steering Torque | Receives and processes input from Driver steering torque sensor |
| EPS ECU - Normal Lane Assistance Functionality | Receives torque request from camera sensor, checks it with input from driver steering torque sensor and sends appropriate torque request to Lane Departure Warning Safety functionality |
| EPS ECU - Lane Departure Warning Safety Functionality | Checks if Lane Departure Warning functionality is malfunctioning or not and sends torque request based on that. |
| EPS ECU - Lane Keeping Assistant Safety Functionality | Checks if Lane Keeping Assistance functionality is malfunctioning or not and sends torque request based on that. |
| EPS ECU - Final Torque | Sends final torque to motor |
| Motor | Applies received final torque to steering wheel. |

# Technical Safety Concept

## Technical Safety Requirements

**Lane Departure Warning (LDW) Requirements:**

Functional Safety Requirement 01-01 with its associated system elements

(Derived in the functional safety concept)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Functional Safety Requirement** | **Electronic Power Steering ECU** | **Camera ECU** | **Car Display ECU** |
| Functional  Safety  Requirement  01-01 | Lane departure warning system should limit the Oscillation of steering wheel below Max Torque Amplitude. | X |  |  |

Technical Safety Requirements related to Functional Safety Requirement 01-01 are:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **ID** | **Technical Safety Requirement** | **ASIL** | **Fault Tolerant Time Interval** | **Architecture Allocation** | **Safe State** |
| Technical  Safety  Requirement  01 | The LDW safety component shall ensure that the amplitude of the 'LDW Torque Request' sent to the 'Final electronic power steering Torque' component is below 'Max Torque Amplitude’. | C | 50 ms | LDW safety block | LDW torque is zero |
| Technical  Safety  Requirement  02 | As soon as the LDW function deactivates the LDW feature, the 'LDW Safety' software block shall send a signal to the car display ECU to turn on a warning light. | C | 50 ms | LDW safety block | LDW torque is zero |
| Technical  Safety  Requirement  03 | As soon as a failure is detected by the LDW function, it shall deactivate the LDW feature and the 'LDW Torque Request' shall be set to zero. | C | 50 ms | LDW safety block | LDW torque is zero |
| Technical  Safety  Requirement  04 | The validity and integrity of the data transmission for 'LDW Torque Request' signal shall be ensured. | C | 50 ms | Data transmission integrity check block | LDW torque is zero |
| Technical  Safety  Requirement  05 | Memory test shall be conducted at startup of the EPS ECU to check for any faults in memory. | A | ignition cycle | Memory test block | LDW torque is zero |

Functional Safety Requirement 01-2 with its associated system elements

(Derived in the functional safety concept)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Functional Safety Requirement** | **Electronic Power Steering ECU** | **Camera ECU** | **Car Display ECU** |
| Functional  Safety  Requirement  01-02 | The departure warning system shall ensure that the lane departure oscillating torque frequency is below Max Torque Frequency. | X |  |  |

Technical Safety Requirements related to Functional Safety Requirement 01-02 are:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **ID** | **Technical Safety Requirement** | **ASIL** | **Fault Tolerant Time Interval** | **Architecture Allocation** | **Safe State** |
| Technical  Safety  Requirement  01 | The LDW safety component shall ensure that the frequency of the 'LDW Torque Request' sent to the 'Final electronic power steering Torque' component is below 'Max Torque Frequency. | C | 50 ms | LDW safety block | LDW torque is zero |
| Technical  Safety  Requirement  02 | As soon as the LDW feature is deactivated, the 'LDW Safety' software block will send a signal to the car display ECU to turn on a warning light and message. | C | 50 ms | LDW safety block | LDW torque is zero |
| Technical  Safety  Requirement  03 | As soon as a failure is detected by the LDW function, it shall deactivate the LDW feature and the 'LDW Torque Request' shall be set to zero. | C | 50 ms | LDW safety block | LDW torque is zero |
| Technical  Safety  Requirement  04 | The validity and integrity of the data transmission for 'LDW Torque Request' signal shall be ensured. | C | 50 ms | Data transmission integrity check block | LDW torque is zero |
| Technical  Safety  Requirement  05 | Memory test shall be conducted at startup of the EPS ECU to check for any faults in memory. | A | Ignition cycle | Memory test block | LDW torque is zero |

**Lane Keeping Assistance (LKA) Requirements:**

Functional Safety Requirement 02-1 with its associated system elements

(derived in the functional safety concept)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Functional Safety Requirement** | **Electronic Power Steering ECU** | **Camera ECU** | **Car Display ECU** |
| Functional  Safety  Requirement  02-01 | The lane keeping assistance system shall be time limited. | X |  |  |

Technical Safety Requirements related to Functional Safety Requirement 02-01 are:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **ID** | **Technical Safety Requirement** | **ASIL** | **Fault Tolerant Time Interval** | **Allocation to Architecture** | **Safe State** |
| Technical  Safety  Requirement  01 | The LKA safety component should ensure that the torque sent to the 'Final electronic power steering Torque' component is only for 'Max Duration’. | B | 500 ms | LKA safety block | LKA torque is zero |
| Technical  Safety  Requirement  02 | As soon as LKA feature is deactivated, the 'LKA Safety' software block shall send a signal to the car display ECU to turn on a warning light on display. | B | 500 ms | LKA safety block | LKA torque is zero |
| Technical  Safety  Requirement  03 | As soon as a failure is detected by the LKA function, it shall deactivate the LKA feature and the 'LKA Torque Request' shall be set to zero. | B | 500 ms | LKA safety block | LKA torque is zero |
| Technical  Safety  Requirement  04 | The validity and integrity of the data transmission for 'LKA Torque Request' signal shall be ensured. | B | 500 ms | Data transmission integrity check block | LKA torque is zero |
| Technical  Safety  Requirement  05 | Memory test shall be conducted at startup of the EPS ECU to check for any faults in memory. | A | Ignition cycle | Memory test block | LKA torque is zero |

## Refinement of the System Architecture

****

## Allocation of Technical Safety Requirements to Architecture Elements

For this item, all technical safety requirements are allocated to the Electronic Power Steering ECU.

## Warning and Degradation Concept

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Degradation Mode** | **Trigger for Degradation Mode** | **Safe State invoked?** | **Driver Warning** |
| WDC-01 | Turn off lane assistance system | Malfunction\_01 | YES | Warning on Car display |
| WDC-02 | Turn off lane assistance system | Malfunction\_02 | YES | Warning on Car display |
| WDC-03 | Turn off lane assistance system | Malfunction\_03 | YES | Warning on Car display |