

Technical Safety Concept Lane Assistance

**Document Version: [Version]**

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



# Document history

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Editor | Description |
| 14.07.2018 | 1.1 | Ankith Manjunath |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# 

# Table of Contents

[Document history](#_1t3h5sf)

[Table of Contents](#_ktt3lgighckp)

[Purpose of the Technical Safety Concept](#_fulgh8sf1ocg)

[Inputs to the Technical Safety Concept](#_757cx6xm46zb)

[Functional Safety Requirements](#_2f9rjqxbsp2)

[Refined System Architecture from Functional Safety Concept](#_qp3s9pvua9mt)

[Functional overview of architecture elements](#_cqb49updinx4)

[Technical Safety Concept](#_mx8us8onanqo)

[Technical Safety Requirements](#_lnxjuovv6kca)

[Refinement of the System Architecture](#_74udkdvf7nod)

[Allocation of Technical Safety Requirements to Architecture Elements](#_g2lqf7kmbspk)

[Warning and Degradation Concept](#_4w6r8buy4lrp)

# Purpose of the Technical Safety Concept

The functional safety concept follows the ISO26262 standards to specifiy safety requirements on a system level ignoring the technical details. Technical safety concept introduces more technical specific requirements into the system.

# 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 | The lane keeping item shall ensure that the  torque amplitude by lane departure warning  system is below  MAX\_TORQUE\_AMPLITUDE | C | 50ms | Vibration torque amplitude below Max\_Torque\_Amplitude. |
| Functional  Safety  Requirement  01-02 | The lane keeping item shall ensure that the  torque frequency by the lane departure  warning is below  MAX\_TORQUE\_FREQUENCY | C | 50ms | Vibration torque amplitude below Max\_Torque\_Frequency. |
| Functional  Safety  Requirement  02-01 | The lane keeping item shall ensure that the  steering torque TIME\_FOR\_TORQUE is  applied for a limited period of time . | B | 500ms | Lane Keeping Assistance torque is zero. |

## Refined System Architecture from Functional Safety Concept

****

### 

### Functional overview of architecture elements

|  |  |
| --- | --- |
| **Element** | **Description** |
| Camera Sensor | Captures Frames of the road environment from a video feed |
| Camera Sensor ECU - Lane Sensing | Detects the lane on the road and the distance of the center of the car from the lane on either side |
| Camera Sensor ECU - Torque request generator | Estimates the amount of torque required to keep the car in the center of the lane |
| Car Display | HMI to the driver |
| Car Display ECU - Lane Assistance On/Off Status | HMI indication to indicate if Lane assistance is on or off |
| Car Display ECU - Lane Assistant Active/Inactive | HMI indicaion to indicate if Lane assistance item is working properly or not |
| Car Display ECU - Lane Assistance malfunction warning | HMI indication to alert the driver for a handover |
| Driver Steering Torque Sensor | Sensor to detect the amount of torque applied by the driver |
| Electronic Power Steering (EPS) ECU - Driver Steering Torque | ECU receiving the torque from the steering torque sensor |
| EPS ECU - Normal Lane Assistance Functionality | ECU calculating the amount of torque needed for lane assitance |
| EPS ECU - Lane Departure Warning Safety Functionality | ECU to provide driver with a haptic feedback(Vibration) to alert the driver of lane departure warning |
| EPS ECU - Lane Keeping Assistant Safety Functionality | ECU calculating the amount of extra torque needed to keep the vehicle in the lane |
| EPS ECU - Final Torque | ECU to send the torque request to the motor |
| Motor | Motor used to steer the 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 | The lane keeping item shall ensure that the lane departure oscillating torque amplitude is 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  01-01-01 | 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 | 50ms | LDW safety | Set LDW\_Torque\_request to zero |
| Technical  Safety  Requirement  01-01-02 | The validity and integrity of the data transmission for LDW\_Torque\_Request signal shall be ensured | C | 50ms | LDW safety | Set LDW\_Torque\_request to zero |
| Technical  Safety  Requirement  01-01-03 | 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 | 50ms | LDW safety | Set LDW\_Torque\_request to zero |
| Technical  Safety  Requirement  01-01-04 | 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 | 50ms | LDW safety | Set LDW\_Torque\_request to zero |
| Technical  Safety  Requirement  01-01-05 | Memory test shall be conducted at start up of the EPS ECU to check for any faults in memory | A | Ignition cycle | Data transmission Integrity check | Set LDW\_Torque\_request to 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 lane keeping item 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  01-02-01 | The lane departure warning safety subsyste ensures that the LDW\_Torque\_request is less than the Max\_Torque\_Frequency | C | 50ms | LDW safety | Set LDW\_Torque\_request to zero |
| Technical  Safety  Requirement  01-02-02 | On lane departure warning malfunction, the lane departure warning safety system shall deactivate and set Max\_Torque\_Frequency to zero | C | 50ms | LDW safety | Set LDW\_Torque\_request to zero |
| Technical  Safety  Requirement  01-02-03 | When LDW is deactivated the LDW safety module shall send a signal to car display ECU to display a warning | C | 50ms | LDW safety | Set LDW\_Torque\_request to zero |
| Technical  Safety  Requirement  01-02-04 | The integrity of LDW\_Torque\_request shall be ensured | C | 50ms | LDW safety | Set LDW\_Torque\_request to zero |
| Technical  Safety  Requirement  01-02-05 | Memory tests shall be conducted on EPS ECU to check for memory problems | A | Ignition cycle | Data transmission Integrity check | Set LDW\_Torque\_request to 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 item shall ensure that the lane keeping assistance torque is applied for only Max\_Duration | 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  02-01-01 | The lane keep assistance safety function shall apply lane keeping assistance torque for a duration less than Max\_Duration | B | 500ms | LKA safety | LKA\_Torque\_request set to zero |
| Technical  Safety  Requirement  02-01-02 | When lane keeping assitance is deactivated the LKA safety module shall send a signal to car display ECU to display a warning | B | 500ms | LKA safety | LKA\_Torque\_request set to zero |
| Technical  Safety  Requirement  02-01-03 | On lane keeping assistance malfunction, the lane keeping assistance safety system shall deactivate and set LKA\_Torque\_request to zero | B | 500ms | LKA safety | LKA\_Torque\_request set to zero |
| Technical  Safety  Requirement  02-01-04 | The integrity of LKA\_Torque\_request shall be ensured | B | 500ms | LKA safety | LKA\_Torque\_request set to zero |
| Technical  Safety  Requirement  02-01-05 | Memory tests shall be conducted on EPS ECU to check for memory problems | A | Ignition cycle | Data transmission Integrity check | LKA\_Torque\_request set to zero |

## Refinement of the System Architecture

****

## Allocation of Technical Safety Requirements to Architecture Elements

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Technical Safety Requirement** | **Electronic Power Steering ECU** | **Camera ECU** | **Car Display ECU** |
| Technical  Safety  Requirement  01-01-01 | 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 | X |  |  |
| Technical  Safety  Requirement  01-01-02 | The validity and integrity of the data transmission for LDW\_Torque\_Request signal shall be ensured | x |  |  |
| Technical  Safety  Requirement  01-01-03 | 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 | x |  |  |
| Technical  Safety  Requirement  01-01-04 | 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 | x |  |  |
| Technical  Safety  Requirement  01-01-05 | Memory test shall be conducted at start up of the EPS ECU to check for any faults in memory | x |  |  |
| Technical  Safety  Requirement  01-02-01 | The lane departure warning safety subsyste ensures that the LDW\_Torque\_request is less than the Max\_Torque\_Frequency | x |  |  |
| Technical  Safety  Requirement  01-02-02 | On lane departure warning malfunction, the lane departure warning safety system shall deactivate and set Max\_Torque\_Frequency to zero | x |  |  |
| Technical  Safety  Requirement  01-02-03 | When LDW is deactivated the LDW safety module shall send a signal to car display ECU to display a warning | x |  |  |
| Technical  Safety  Requirement  01-02-04 | The integrity of LDW\_Torque\_request shall be ensured | x |  |  |
| Technical  Safety  Requirement  01-02-05 | Memory tests shall be conducted on EPS ECU to check for memory problems | x |  |  |
| Technical  Safety  Requirement  02-01-01 | The lane keep assistance safety function shall apply lane keeping assistance torque for a duration less than Max\_Duration | x |  |  |
| Technical  Safety  Requirement  02-01-02 | When lane keeping assitance is deactivated the LKA safety module shall send a signal to car display ECU to display a warning | x |  |  |
| Technical  Safety  Requirement  02-01-03 | On lane keeping assistance malfunction, the lane keeping assistance safety system shall deactivate and set LKA\_Torque\_request to zero | x |  |  |
| Technical  Safety  Requirement  02-01-04 | The integrity of LKA\_Torque\_request shall be ensured | x |  |  |
| Technical  Safety  Requirement  02-01-05 | Memory tests shall be conducted on EPS ECU to check for memory problems | x |  |  |

## Warning and Degradation Concept

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