

Technical Safety Concept Lane Assistance

**Document Version: [Version]**

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



# Document history

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Editor | Description |
| 22/05/2018 | 1.0 | Ashith Raghunath | Compiled Technical Safety Concept |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# 

# 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 purpose of the technical safety concept is to be a more concrete version of the Functional Safety Concept and get into the details of the item's technology. While the functional safety concept is in the concept phase, the technical safety concept is part of the product development phase.

# 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 lane departure oscillating torque max amplitude is below Max\_Torque\_Amplitude | C | 50ms | Limit the torque below Max\_Torque\_Amplitude |
| Functional  Safety  Requirement  01-02 | The lane keeping item shall ensure that the lane departure oscillating torque max frequency is below Max\_Torque\_Frequency | C | 50ms | Limit the torque below Max\_Torque\_Frequency |
| Functional  Safety  Requirement  02-01 | lane keeping assistance function shall be time limited and the additional steering torque shall end after a given timer interval (MAX\_DURATION)so that the driver cannot misuse the system for autonomous driving | B | 500ms | Turn off the lane keeping assistance function |

## Refined System Architecture from Functional Safety Concept



### 

### Functional overview of architecture elements

|  |  |
| --- | --- |
| **Element** | **Description** |
| Camera Sensor | It is used to capture the images of the road ahead and pass it on to the Camera Sensor ECU |
| Camera Sensor ECU - Lane Sensing | Use OpenCV methods to analyze the input images and Localize the car with respect to the lane lines. |
| Camera Sensor ECU - Torque request generator | It calculates the torque necessary to center the vehicle in the lane. |
| Car Display | Provide visual display for warnings related to any of the functions such as lane departure warning. |
| Car Display ECU - Lane Assistance On/Off Status | Indicate whether the Lane Assistance Functionality is turned on or off. |
| Car Display ECU - Lane Assistant Active/Inactive | Indicate if the Lane Assistance Functionality is currently activated or not. |
| Car Display ECU - Lane Assistance malfunction warning | Indicate if the Lane Assistance Functionality is malfunctioning. |
| Driver Steering Torque Sensor | Measures the amount of torque applied to the steering wheel by the driver. |
| Electronic Power Steering (EPS) ECU - Driver Steering Torque | Receives the driver steering torque measured by the Driver Steering Torque Sensor |
| EPS ECU - Normal Lane Assistance Functionality | Receives the torque request from camera ECU and implements the Lane Keeping assist and Lane Departure Warning Functionalities |
| EPS ECU - Lane Departure Warning Safety Functionality | Safety module that makes sure that the applied torque amplitude and frequency are within the threshold values. |
| EPS ECU - Lane Keeping Assistant Safety Functionality | Safety module that makes sure that the torque is applied only for a Max\_Duration time interval and automatically switches off Lane Keeping Assistant |
| EPS ECU - Final Torque | Combines the torque requests from Lane Keeping Assist and Lane Departure Warning to generate the appropriate torque and sends them to the Motor |
| Motor | Applies the required torque received from the Electronic Power Steering ECU to 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 | The validity and integrity for the data transmission for ‘LDW\_Torque\_Request’ signal shall be ensured | C | 50 ms | Data Transmission Integrity Check | LDW\_Torque\_Request is set to zero. |
| Technical  Safety  Requirement  02 | As soon as 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 | LDW\_Torque\_Request is set to zero. |
| Technical  Safety  Requirement  03 | 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 | LDW\_Torque\_Request is set to zero. |
| Technical  Safety  Requirement  04 | Memory test shall be conducted at startup of the EPS ECU to check for any faults in memory | A | ignition cycle | Safety Startup | LDW\_Torque\_Request is set to zero. |
| Technical  Safety  Requirement  05 | 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 | LDW\_Torque\_Request is set 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 | The validity and integrity for the data transmission for ‘LDW\_Torque\_Request’ signal shall be ensured | C | 50 ms | Data Transmission Integrity Check | LDW\_Torque\_Request is set to zero. |
| Technical  Safety  Requirement  02 | As soon as 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 | LDW\_Torque\_Request is set to zero. |
| Technical  Safety  Requirement  03 | 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 | LDW\_Torque\_Request is set to zero. |
| Technical  Safety  Requirement  04 | Memory test shall be conducted at startup of the EPS ECU to check for any faults in memory | A | ignition cycle | Safety Startup | LDW\_Torque\_Request is set to zero. |
| Technical  Safety  Requirement  05 | 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 | LDW\_Torque\_Request is set 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  01 | The validity and integrity for the data transmission for ‘LKA\_Torque\_Request’ signal shall be ensured | B | 500 ms | Data Transmission Integrity Check | LKA\_Torque\_Request is set to zero. |
| Technical  Safety  Requirement  02 | The LKA safety component shall ensure that the duration of the ‘LKA\_Torque\_Request’ sent to the ‘Final electronic power steering Torque’ component is below ‘Max\_DURATION’ | B | 500 ms | LKA\_Safety | LKA\_Torque\_Request is set to zero. |
| Technical  Safety  Requirement  03 | Memory test shall be conducted at startup of the EPS ECU to check for any faults in memory | A | ignition cycle | Safety Startup | LKA\_Torque\_Request is set to zero. |
| Technical  Safety  Requirement  04 | As soon as the LKA function deactivates the LKA feature, the ‘LKA Safety’ software block shall send a signal to the car display ECU to turn on a warning light | B | 500 ms | LKA\_Safety | LKA\_Torque\_Request is set to zero. |
| Technical  Safety  Requirement  05 | As soon as 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 | LKA\_Torque\_Request is set to zero. |

## Refinement of the System Architecture

****

## Allocation of Technical Safety Requirements to Architecture Elements

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 the functionality | Malfunction\_01  Malfunction\_02 | Yes | Display a Lane Departure Warning Malfunction warning on Car Display |
| WDC-02 | Turn off the functionality | Malfunction\_03 | Yes | Display a Lane Keeping Assistance Malfunction warning on Car Display |