

Technical Safety Concept Lane Assistance

**Document Version: [Version]**

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



# Document history

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Editor | Description |
| 20-06-2018 | 1.0 | Shubham | Final Draft |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# 

# 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 turn the functional safety requirements for the Lane Assistance item into technical safety requirements and allocating technical safety requirements to the system architecture.

# The technical safety requirements shall be derived taking into consideration:

# detecting faults within a system

# detecting faults in an external device interacting with the system –

# reaching a safe state

# implementing a warning and degradation concept

# preventing latent faults

# 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 | 1. The lane keeping item shall ensure that the lane departure oscillating torque amplitude is below Max\_Torque\_Amplitude | C | 50ms | Set lane departure Warning torque request amplitude to zero |
| Functional  Safety  Requirement  01-02 | 1. The lane keeping item shall ensure that the lane departure oscillating torque frequency is below Max\_Torque\_Frequency | C | 50ms | Set lane departure Warning torque request frequency to zero |
| Functional  Safety  Requirement  02-01 | Lane Keeping Assistance Function will be active for a limited time Max\_Duration | B | 500ms | Set Lane Keeping Assistance torque amplitude to zero |

## Refined System Architecture from Functional Safety Concept

****

Figure 1: Refined System Architecture

### 

### Functional overview of architecture elements

|  |  |
| --- | --- |
| **Element** | **Description** |
| Camera Sensor | Captures images and feed them to Camera Sensor ECU. |
| Camera Sensor ECU - Lane Sensing | Process the images provided by camera. Detect lane lines and in case of lane departure warn Car display ECU. |
| Camera Sensor ECU - Torque request generator | Generate torque request to Electronic Power Steering ECU. |
| Car Display | Display warnings and status of the System. |
| Car Display ECU - Lane Assistance On/Off Status | Displays the status of the Lane Assistance system that is whether the system is On or Off. |
| Car Display ECU - Lane Assistant Active/Inactive | Displays the status of the Lane Assistance system that is whether the system is Active or Inactive. |
| Car Display ECU - Lane Assistance malfunction warning | Displays any malfunction or warnings in the Lane Assistance system. |
| Driver Steering Torque Sensor | Measures torque applied to the steering wheel. |
| Electronic Power Steering (EPS) ECU - Driver Steering Torque | Takes input from Driver steering torque sensor and process that. |
| EPS ECU - Normal Lane Assistance Functionality | It takes input from Camera ECU and driver steering torque sensor and passes it to the lane assistance functionality. |
| EPS ECU - Lane Departure Warning Safety Functionality | It checks for any malfunction in the Lane Departure warning function and takes appropriate action in case of any malfunction. |
| EPS ECU - Lane Keeping Assistant Safety Functionality | It checks for any malfunction in the Lane Keeping Assistance function and takes appropriate action in case of any malfunction |
| EPS ECU - Final Torque | It merges the input from LKA,LDW and driver steering torque to deliver the final torque request to the motor |
| Motor | Provide torque 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 | As soon as any malfunction occurs LDW function, it shall cut off the LDW feature and the ‘LDW\_Torque\_Request’ shall be set to zero. | C | 50ms | LDW safety block | Lane Departure Warning Torque Request Amplitude shall be set to zero. |
| Technical  Safety  Requirement  02 | At the time when LDW feature turns off the LDW function, ‘LDW safety’ software block shall send a signal to the car display ECU to turn on a warning light. | C | 50ms | LDW Safety block | Lane Departure Warning Torque Request Amplitude shall be set to zero. |
| Technical  Safety  Requirement  03 | Memory test shall be conducted at startup of the EPS ECU to check for potential malfunction in memory. | A | The length of ignition cycle | Data Transmission Integrity Check | Lane Departure Warning Torque Request Amplitude shall be set to zero. |
| Technical  Safety  Requirement  04 | The validity and integrity of the data transmission for LDW\_Torque\_Request signal shall be ensured. | C | 50ms | LDW safety block | Lane Departure Warning Torque Request Amplitude shall be 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 | 50ms | LDW safety block | Lane Departure Warning Torque Request Amplitude shall be 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 | As soon as the 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 block | Lane Departure Warning Torque Request Frequency shall be set to zero. |
| Technical  Safety  Requirement  02 | As soon as the LDW function deactivates the LDW feature , ‘LDW safety’ software block shall send a signal to the car display ECU to turn on a warning light. | C | 50ms | LDW safety block | Lane Departure Warning Torque Request Frequency shall be set to zero. |
| Technical  Safety  Requirement  03 | Memory test shall be conducted at startup of the EPS ECU to check for potential malfunction in memory. | A | The length of ignition cycle | Data Transmission Integrity Check | Lane Departure Warning Torque Request Frequency shall be set to zero. |
| Technical  Safety  Requirement  04 | The validity and integrity of the data transmission for LDW\_Torque\_Request signal shall be ensured | C | 50ms | LDW safety block | Lane Departure Warning Torque Request Frequency shall be 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 | 50ms | LDW Safety block | Lane Departure Warning Torque Request Frequency shall be 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 | At the time a malfunction is detected by the LKA function, it shall cut off the LKA feature and the ‘LKA\_Torque\_Request’ shall be set to zero | B | 500ms | LKA safety block | Lane Keeping Assistance Torque Request shall be set to zero |
| Technical  Safety  Requirement  02 | At the time LKA function deactivates the LKA feature , ‘LKA safety’ software block shall send a signal to the car display ECU to turn on a warning light | B | 500ms | LKA safety block | Lane Keeping Assistance Torque Request shall be set to zero |
| Technical  Safety  Requirement  03 | Memory test shall be conducted at startup of the EPS ECU to check for potential malfunction in memory. | A | The length of ignition cycle | Data Transmission Integrity Check | Lane Keeping Assistance Torque Request shall be set to zero |
| Technical  Safety  Requirement  04 | The validity and integrity of the data transmission for LKA\_Torque\_Request signal shall be ensured. | B | 500ms | LKA safety block | Lane Keeping Assistance Torque Request shall be set to zero |
| Technical  Safety  Requirement  05 | The LKA safety component shall ensure that duration of the 'LKA\_Torque\_Request' sent to the 'Final electronic power steering Torque' component is below 'Max\_Duration’. | B | 500ms | LKA safety block | Lane Keeping Assistance Torque Request shall be set to zero |

## Refinement of the System Architecture

****

Figure 2: Refined Lane Assistance system architecture

## Allocation of Technical Safety Requirements to Architecture Elements

All The Technical Safety Requirements like LDW (Lane Departure Warning) Safety, LKA (Lane Keeping Assistance) Safety and memory are assigned to the EPS ECU (Fig. 2]

## Warning and Degradation Concept

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Degradation Mode** | **Trigger for Degradation Mode** | **Safe State invoked?** | **Driver Warning** |
| WDC-01 | Turn OFF the functionality | Malfunction\_01  Malfucntion\_02 | Yes | Warning Light on Dashboard, and warnings displayed on car display |
| WDC-02 | Turn OFF the functionality | Malfunction\_03 | Yes | Warning Light on Dashboard, and warnings displayed on car display |