

Technical Safety Concept Lane Assistance

**Document Version: [Version]**

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



# Document history

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Editor | Description |
| 23/05/2018 | 1.0 | Sanchit Agrawal | First Submission |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# 

# 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

In this document, new requirements are defined and assigned to the system architecture. Technical safety concept is part of the product development phase. The technical safety concept is more concrete and gets into the details of the item's technology.

# 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 Departure Warning item shall ensure that the lane departure oscillating torque amplitude is below Max\_Torque\_Amplitude. | C | 50ms | Vibration torque amplitude below Max\_Torque\_Amplitude. |
| Functional  Safety  Requirement  01-02 | The Lane Departure Warning item shall ensure that the lane departure oscillating torque frequency is below Max\_Torque\_Frequency. | C | 50ms | Vibration frequency is below Max\_Torque\_Frequency. |
| Functional  Safety  Requirement  02-01 | The electronic power steering ECU shall ensure that the Lane Keeping Assistance torque is applied only Max\_Duration. | B | 500ms | Lane Keeping Assistance torque is zero. |

## Refined System Architecture from Functional Safety Concept



### Functional overview of architecture elements

|  |  |
| --- | --- |
| **Element** | **Description** |
| Camera Sensor | Provides images of road to Camera Sensor ECU. |
| Camera Sensor ECU - Lane Sensing | Software module detecting lane line position from the camera images. |
| Camera Sensor ECU - Torque request generator | Software module calculating the necessary torque to be requested to the Electronic Power Steering ECU. |
| Car Display | Shows warning to driver. |
| Car Display ECU - Lane Assistance On/Off Status | Indicate status of Lane Assistance functionality. |
| Car Display ECU - Lane Assistant Active/Inactive | Indicate Lane Assistance functionality is properly working or not. |
| Car Display ECU - Lane Assistance malfunction warning | Indicate malfunction in Lane Assistance functionality. |
| Driver Steering Torque Sensor | Senses how much torque already been applied by driver. |
| Electronic Power Steering (EPS) ECU - Driver Steering Torque | Software module receiving the driver’s torque request from the steering wheel. |
| EPS ECU - Normal Lane Assistance Functionality | Software module receiving the Camera Sensor ECU torque request. |
| EPS ECU - Lane Departure Warning Safety Functionality | Ensuring the torque amplitude is below Max\_Torque\_Amplitude and torque frequency is below Max\_Torque\_Frequency. |
| EPS ECU - Lane Keeping Assistant Safety Functionality | Ensuring the Lane Keeping Assistance functionality application is not activate more than Max\_duration time. |
| EPS ECU - Final Torque | Combining the torque request from the Lane Keeping and Lane Departure Warning functionalities and sends them to the Motor. |
| Motor | Applies the torque. |

# 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 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 Lane Departure Warning torque to 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 | 50ms | LDW Safety | Set Lane Departure Warning torque to 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 | 50ms | LDW Safety | Set Lane Departure Warning torque 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 | Set Lane Departure Warning torque to zero. |
| Technical  Safety  Requirement  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 Lane Departure Warning torque 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 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\_Frequency. | C | 50ms | LDW Safety | Set Lane Departure Warning torque to 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 | 50ms | LDW Safety | Set Lane Departure Warning torque to 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 | 50ms | LDW Safety | Set Lane Departure Warning torque 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 | Set Lane Departure Warning torque to zero. |
| Technical  Safety  Requirement  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 Lane Departure Warning torque 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** | **Architecture Allocation** | **Safe State** |
| Technical  Safety  Requirement  01 | The Lane Keeping Assistance safety component shall ensure the duration of the lane keeping assistance torque is applied for less than Max\_Duration | C | 500ms | LKA Safety | Set Lane Departure Warning torque to zero. |
| Technical  Safety  Requirement  02 | As soon as the LKS function deactivates the LKS feature, the 'LKA Safety' software block shall send a signal to the car display ECU to turn on a warning light. | C | 500ms | LKA Safety | Set Lane Departure Warning torque to zero. |
| Technical  Safety  Requirement  03 | As soon as a failure is detected by the LKS function, it shall deactivate the LKA feature and the 'LKA\_Torque\_Request' shall be set to zero. | C | 500ms | LKA Safety | Set Lane Departure Warning torque to zero. |
| Technical  Safety  Requirement  04 | The validity and integrity of the data transmission for 'LKA\_Torque\_Request' signal shall be ensured. | C | 500ms | LKA Safety | Set Lane Departure Warning torque to zero. |
| Technical  Safety  Requirement  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 Lane Departure Warning torque 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 Lane Departure Warning 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.’ | **YES** | **NO** | **NO** |
| Technical  Safety  Requirement  01-01-02 | When the Lane Departure Warning is deactivated, the ‘LDW Safety’ software module shall send a signal to the Car Display ECU to turn on a warning signal. | **YES** | **NO** | **NO** |
| Technical  Safety  Requirement  01-01-03 | When a failure is detected by the Lane Departure Warning functionality, it shall deactivate the Lane Departure Warning feature and set ‘LDW\_Torque\_Request’ to zero. | **YES** | **NO** | **NO** |
| Technical  Safety  Requirement  01-01-04 | The validity and integrity of the data transmission for ‘LDW\_Torque\_Request’ signal shall be ensured. | **YES** | **NO** | **NO** |
| Technical  Safety  Requirement  01-01-05 | Memory test shall be conducted at start up of the EPS ECU to check for any memory problems | **YES** | **NO** | **NO** |
| Technical  Safety  Requirement  01-02-01 | The Lane Departure Warning safety component shall ensure the frequency of the ‘LDW\_Torque\_Reques’ sent to the ‘Final electronic power steering Torque’ component is below ‘Max\_Torque\_Frequency.’ | **YES** | **NO** | **NO** |
| Technical  Safety  Requirement  02-01-01 | The Lane Keeping Assistance safety component shall ensure the duration of the lane keeping assistance torque is applied for less than Max\_Duration | **YES** | **NO** | **NO** |
| Technical  Safety  Requirement  02-01-02 | When the Lane Keeping Assistance function deactivates, the ‘LKA Safety’ shall send a signal to the Car Display ECU to turn on a warning light. | **YES** | **NO** | **NO** |
| Technical  Safety  Requirement  02-01-03 | When a failure is detected, the Lane Keeping Assistance function shall deactivate and the ‘LKA\_Torque\_Request’ shall be zero. | **YES** | **NO** | **NO** |
| Technical  Safety  Requirement  02-01-04 | The validity and integrity of the data transmission for ‘LKA\_Torque\_Request’ signal shall be ensured. | **YES** | **NO** | **NO** |
| Technical  Safety  Requirement  02-01-05 | Memory test shall be conducted at start up of the EPS ECU to check for any memory problems | **YES** | **NO** | **NO** |

## Warning and Degradation Concept

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Degradation Mode** | **Trigger for Degradation Mode** | **Safe State invoked?** | **Driver Warning** |
| WDC-01 | Turn off Lane Departure Warning functionality | Malfunction\_01,  Malfunction\_02 | Yes | Lane Departure Warning Malfunction Warning on Car Display |
| WDC-02 | Turn off Lane Keeping Assistance functionality | Malfunction\_03 | Yes | Lane Keeping Assistance Malfunction Warning on Car Display |