

Technical Safety Concept Lane Assistance

**Document Version: 1.0**

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



# Document history

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Editor | Description |
| 22/05/2018 | 0.1 | Kapil Saini | Initial draft |
| 23/05/2018 | 1.0 | Kapil Saini | Finalized version |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# 

# 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 specify the roadmap for implementation of the defined functional safety concept. This includes concrete information on 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 keeping item shall ensure that the lane departure warning torque **amplitude** is below **Max\_Torque\_Amplitude** | C | 50ms | Turn off LDW |
| Functional  Safety  Requirement  01-02 | The lane keeping item shall ensure that the lane departure warning torque **frequency** is below **Max\_Torque\_Frequency** | C | 50ms | Turn off LDW |
| Functional  Safety  Requirement  02-01 | Ensure that LKA torque is applied only for a limited time not more than **Max\_Duration** | B | 500ms | Turn off LKA setting torque to zero |

## Refined System Architecture from Functional Safety Concept

### 

Figure Refined System Architecture

### Functional overview of architecture elements

|  |  |
| --- | --- |
| **Element** | **Description** |
| Camera Sensor | Sensors to capture environmental information as images and provide them to the camera sensor ECU continuously. |
| Camera Sensor ECU - Lane Sensing | A processor unit to process acquired images by camera sensors to detect Lane Lines and calculate car positions w.r.t. to lane lines. |
| Camera Sensor ECU - Torque request generator | A processor unit to generate Torque request to the car for the Electronic Power Steering ECU |
| Car Display | Display device to display system status and warnings during system malfunctions to driver. |
| Car Display ECU - Lane Assistance On/Off Status | A control function to display on/off status of lane assistance system. |
| Car Display ECU - Lane Assistant Active/Inactive | A control function to display active/inactive status of lane assistance system. |
| Car Display ECU - Lane Assistance malfunction warning | Function to display any malfunction in the Lane Assistance system |
| Driver Steering Torque Sensor | Sensor to measures the torque applied to the steering wheel. |
| Electronic Power Steering (EPS) ECU - Driver Steering Torque | The Processing unit to process input from driver Steering Torque Sensor. |
| EPS ECU - Normal Lane Assistance Functionality | A function to process the data from the torque request generator |
| EPS ECU - Lane Departure Warning Safety Functionality | A function to ensure the LDW safety functionality |
| EPS ECU - Lane Keeping Assistant Safety Functionality | Function to check for any malfunction in the Lane Keeping Assistance system. |
| EPS ECU - Final Torque | Combine the inputs from LDW and LKA and deliver the final torque request to the motor |
| Motor | An electric motor that interpret the EPS ECU data to control 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 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 | Torque\_Request=0 |
| 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 | Torque\_Request=0 |
| 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 | Torque\_Request=0 |
| Technical  Safety  Requirement  04 | The validity and integrity of the data transmission for 'LDW\_Torque\_Request' signal shall be ensured | C | 50ms | Data Transmission Integrety Check | Torque\_Request=0 |
| Technical  Safety  Requirement  05 | Memory test shall be conducted at startup of the EPS ECU to check for any faults in memory. | A | 50ms | Memory test | Torque\_Request=0 |

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 Frequency of the 'LDW\_Torque\_Request' sent to the 'Final electronic power steering Torque' component is below 'Max\_Torque\_Frequency. | C | 50ms | LDW safety | Torque\_Request=0 |
| 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 | Torque\_Request=0 |
| 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 | Torque\_Request=0 |
| Technical  Safety  Requirement  04 | The validity and integrity of the data transmission for 'LDW\_Torque\_Request' signal shall be ensured | c | 50ms | Data Transmission Integrety Check | Torque\_Request=0 |
| Technical  Safety  Requirement  05 | Memory test shall be conducted at startup of the EPS ECU to check for any faults in memory. | A | 50ms | Memory Check | Torque\_Request=0 |

**Lane Departure Warning (LDW) Verification and Validation Acceptance Criteria:**

**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 LKA safety component shall ensure that the Duration of LKA Torque application is less than Max\_Duration. | B | 500ms | LKA Safety | Torque\_Request=0 |
| 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. | B | 500ms | LKA Safety | Torque\_Request=0 |
| 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. | B | 500ms | LKA Safety | Torque\_Request=0 |
| Technical  Safety  Requirement  04 | The validity and integrity of the data transmission for 'LDW\_Torque\_Request' signal shall be ensured | B | 500ms | Data Transmission Integrety Check | Torque\_Request=0 |
| Technical  Safety  Requirement  05 | Memory test shall be conducted at startup of the EPS ECU to check for any faults in memory. | A | 500ms | Memory Check | Torque\_Request=0 |

**Lane Keeping Assistance (LKA) Verification and Validation Acceptance Criteria:**

## Refinement of the System Architecture

****

Figure Refined Lane System Architecture

## Allocation of Technical Safety Requirements to Architecture Elements

## Warning and Degradation Concept

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **ID** | **Degradation Mode** | **Trigger for Degradation Mode** | **Safe State invoked?** | | **Driver Warning** |
| WDC-01 | Turn off the functionality | **Malfunction\_01**  Is\_Max\_Torque\_ Exceeded  “Lane Departure Warning (LDW) function shall apply an oscillating steering torque to provide the driver a haptic feedback” | | Yes | Turn on warning light on car display and dashboard. |
| WDC-02 | Turn off the functionality | **Malfunction\_02**  Is\_Max\_Duration \_Exceeded  “Lane Departure Warning (LDW) function shall apply an oscillating steering torque to provide the driver a haptic feedback” | | Yes | Turn on warning light on car display and dashboard |