

Technical Safety Concept Lane Assistance

**Document Version: [Version]**

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



# Document history

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Editor | Description |
| 5/23/2018 | 1.0 | Gireek Bansal | First Attempt |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# 

# 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 convert functional requirements into technical requirements and is an in-depth representation of the item’s technology. Functional safety concept was a part of concept phase but this is a part of 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 Departure Warning item shall ensure that the lane departure oscillating torque amplitude is below Max\_Torque\_Amplitude | C | 50 ms | 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 | 50 ms | Vibration frequency is below Max\_Torque\_Frequency. |
| Functional  Safety  Requirement  02-01 | The Lane Keeping Assistance function shall be time limited, and additional steering torque shall end after a given time interval so the driver cannot misuse the system for autonomous driving. | B | 500 ms | Lane Keeping Assistance torque is zero |

## Refined System Architecture from Functional Safety Concept



### 

### Functional overview of architecture elements

|  |  |
| --- | --- |
| **Element** | **Description** |
| Camera Sensor | Takes the photos of the external environment and passes them on to the Camera sensor ECU |
| Camera Sensor ECU - Lane Sensing | Analyzes the photos to calculate the car’s position w.r.t. the lane. |
| Camera Sensor ECU - Torque request generator | It calculates the torque required to re-center the car w.r.t. to the lane |
| Car Display | A display screen to let the driver know about the car’s status and for any type of warnings. |
| Car Display ECU - Lane Assistance On/Off Status | Knowledge about On/off status of lane assistance system is provided to car display by Car Display ECU - Lane Assistance On/Off Status |
| Car Display ECU - Lane Assistant Active/Inactive | Indicates if lane assistance functionality is functioning as required. |
| Car Display ECU - Lane Assistance malfunction warning | Indicates if a malfunction has hit the Lane assistance functionality |
| Driver Steering Torque Sensor | Gives the measure of the torque applied to the steering wheel by the driver. |
| Electronic Power Steering (EPS) ECU - Driver Steering Torque | Software which receives the driver’s torque request from the steering wheel. |
| EPS ECU - Normal Lane Assistance Functionality | Software receives the camera sensor ECU torque request. |
| EPS ECU - Lane Departure Warning Safety Functionality | Software ensures the torque amplitude and frequency are below specific maximum values. |
| EPS ECU - Lane Keeping Assistant Safety Functionality | Software keeps the check that LKA is not activated for more than a specific time duration. |
| EPS ECU - Final Torque | Combines the torque request from both LKA and LDW to send to motor |
| Motor | Responsible for applying the torque to the steering wheel after getting from EPS ECU - Final 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 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 | C | 50 ms | LDW\_safety | LDW\_Torque\_Request is set to zero. |
| Technical  Safety  Requirement  02 | On failure detection by LDW it shall be deactivated and LDW\_torque\_request reset to zero. | C | 50 ms | LDW\_safety | LDW\_Torque\_Request is set to zero. |
| Technical  Safety  Requirement  03 | When the LDW has been deactivated ‘LDW safety’ shall send a signal to car display ECU to turn on warning for the driver. | C | 50 ms | LDW\_safety | LDW\_Torque\_Request is set to zero. |
| Technical  Safety  Requirement  04 | Memory tests shall be conducted at start of EPS ECU for checking memory faults. | A | Ignition cycle | Safety start up | LDW\_Torque\_Request is set to zero. |
| Technical  Safety  Requirement  05 | The integrity of data transmission for LDW\_Torque\_Request signal shall be ensured. | C | 50 ms | Data transmission integrity check | 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 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\_Frequency | C | 50 ms | LDW\_safety | LDW\_Torque\_Request is set to zero. |
| Technical  Safety  Requirement  02 | On failure detection by LDW it shall be deactivated and LDW\_torque\_request reset to zero. | C | 50 ms | LDW\_safety | LDW\_Torque\_Request is set to zero. |
| Technical  Safety  Requirement  03 | When the LDW has been deactivated ‘LDW safety’ shall send a signal to car display ECU to turn on warning for the driver. | C | 50 ms | LDW\_safety | LDW\_Torque\_Request is set to zero. |
| Technical  Safety  Requirement  04 | Memory tests shall be conducted at start of EPS ECU for checking memory faults. | A | Ignition cycle | Safety start up | LDW\_Torque\_Request is set to zero. |
| Technical  Safety  Requirement  05 | The integrity of data transmission for LDW\_Torque\_Request signal shall be ensured. | C | 50 ms | Data transmission Integrity check | 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 LKA safety module shall keep the duration of LKA\_Torque\_Request sent to the steering component below Max\_Duration | B | 500 ms | LKA\_safety | LKA\_Torque\_Request is set to zero. |
| Technical  Safety  Requirement  02 | On failure detection by LKA it shall be deactivated and LKA\_torque\_request reset to zero. | B | 500 ms | LKA\_safety | LKA\_Torque\_Request is set to zero. |
| Technical  Safety  Requirement  03 | When the LKA has been deactivated ‘LKA safety’ shall send a signal to car display ECU to turn on warning for the driver. | B | 500 ms | LKA\_safety | LKA\_Torque\_Request is set to zero. |
| Technical  Safety  Requirement  04 | Memory tests shall be conducted at start of EPS ECU for checking memory faults. | A | Ignition cycle | Safety Start up | LKA\_Torque\_Request is set to zero. |
| Technical  Safety  Requirement  05 | The integrity of data transmission for LKA\_Torque\_Request signal shall be ensured. | B | 500 ms | Data transmission integrity check | LKA\_Torque\_Request is set to zero. |

## Refinement of the System Architecture



## Allocation of Technical Safety Requirements to Architecture Elements

All technical 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 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 |