

Technical Safety Concept Lane Assistance

**Document Version: 1.0**

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



# Document history

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Editor | Description |
| 20/10/2018 | 1.0 | L.R | First Submission |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# 

# Table of Contents

[Document history](#_Toc527941817)

[Table of Contents](#_Toc527941818)

[Purpose of the Technical Safety Concept](#_Toc527941819)

[Inputs to the Technical Safety Concept](#_Toc527941820)

[Functional Safety Requirements](#_Toc527941821)

[Refined System Architecture from Functional Safety Concept](#_Toc527941822)

[Functional overview of architecture elements](#_Toc527941823)

[Technical Safety Concept](#_Toc527941824)

[Technical Safety Requirements](#_Toc527941825)

[Refinement of the System Architecture](#_Toc527941826)

[Allocation of Technical Safety Requirements to Architecture Elements](#_Toc527941827)

[Warning and Degradation Concept](#_Toc527941828)

# Purpose of the Technical Safety Concept

This document refines functional safety requirements into technical safety requirements and determines the components these requirements should be allocated to. This is a lower level look at requirements and applying them to actual system components. Technical safety requirements describe what a system will do when a malfunction violates a safety goal.

# 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 amplitude is below Max\_Torque\_Amplitude | C | 50ms | Turn system off |
| Functional  Safety  Requirement  01-02 | The lane keeping item shall ensure that the lane departure oscillating torque frequency is below Max\_Torque\_Frequency | C | 50ms | Turn system off |
| Functional  Safety  Requirement  02-01 | The lane keeping item shall ensure that the lane keeping assistance torque is applied for only Max\_Duration | B | 500ms | Turn system off |

## Refined System Architecture from Functional Safety Concept



Figure - Refined system architecture diagram for Lane Assistance System

### 

### Functional overview of architecture elements

|  |  |
| --- | --- |
| **Element** | **Description** |
| Camera Sensor | Takes images of the road and passes them to the Camera Sensor ECU. |
| Camera Sensor ECU - Lane Sensing | Detects lane lines and determines car position relative to center of lane. |
| Camera Sensor ECU - Torque request generator | Sends warnings to Car Display and torque commands to EPS ECU. |
| Car Display | Displays feedback to the driver about lane departure warnings and other system status. |
| Car Display ECU - Lane Assistance On/Off Status | Control display to indicate LAS status |
| Car Display ECU - Lane Assistant Active/Inactive | Control display to indicate LAS active/inactive |
| Car Display ECU - Lane Assistance malfunction warning | Control display to indicate malfunction |
| Driver Steering Torque Sensor | Measure torque applied to steering wheel by driver and sends measurement to EPS ECU |
| Electronic Power Steering (EPS) ECU - Driver Steering Torque | Receive driver torque request, send to Final torque |
| EPS ECU - Normal Lane Assistance Functionality | Receive camera torque request, send to safety functionality |
| EPS ECU - Lane Departure Warning Safety Functionality | Ensure torque amplitude and frequency limits are obeyed. |
| EPS ECU - Lane Keeping Assistant Safety Functionality | Ensure LKA time limit is obeyed. |
| EPS ECU - Final Torque | Combine torque requests and command the motor. |
| Motor | Applies torque to steering wheel as commanded by 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 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 | LDW\_Torque\_Request amplitude shall be set to zero. |
| Technical  Safety  Requirement  02 | The validity and integrity of the data transmission for LDW\_Torque\_Request signal shall be ensured | C | 50ms | LDW safety | LDW\_Torque\_Request amplitude shall be set to zero. |
| Technical  Safety  Requirement  03 | As soon as a failure is detected by the LDW function it shall deactivate the LDW feature and LDW\_Torque\_Request shall be set to zero | C | 50ms | LDW safety | LDW\_Torque\_Request amplitude shall be set to zero. |
| Technical  Safety  Requirement  04 | 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 | Data Transmission Integrity Check | LDW\_Torque\_Request amplitude shall be set to zero. |
| Technical  Safety  Requirement  05 | 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 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 | 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 | LDW\_Torque\_Request frequency shall be set to zero. |
| Technical  Safety  Requirement  02 | The validity and integrity of the data transmission for LDW\_Torque\_Request signal shall be ensured | C | 50ms | LDW safety | LDW\_Torque\_Request frequency shall be set to zero. |
| Technical  Safety  Requirement  03 | As soon as a failure is detected by the LDW function it shall deactivate the LDW feature and LDW\_Torque\_Request shall be set to zero | C | 50ms | LDW safety | LDW\_Torque\_Request frequency shall be set to zero. |
| Technical  Safety  Requirement  04 | 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 | Data Transmission Integrity Check | LDW\_Torque\_Request frequency shall be set to zero. |
| Technical  Safety  Requirement  05 | Memory test shall be conducted at startup of the EPS ECU to check for any faults in memory | C | Ignition cycle | Safety Startup | LDW\_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 | 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 | 500ms | LKW safety | LKA\_Torque\_Request shall be set to zero. |
| Technical  Safety  Requirement  02 | The validity and integrity of the data transmission for LKA\_Torque\_Request signal shall be ensured | B | 500ms | LKW safety | LKA\_Torque\_Request shall be set to zero. |
| Technical  Safety  Requirement  03 | As soon as a failure is detected by the LKA function it shall deactivate the LKA feature and LKA\_Torque\_Request shall be set to zero | B | 500ms | LKW safety | LKA\_Torque\_Request shall be 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 | 500ms | Data Transmission Integrity Check | LKA\_Torque\_Request shall be set to zero. |
| Technical  Safety  Requirement  05 | 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 shall be set to zero. |

## Refinement of the System Architecture



Figure - Refined system architecture

## Allocation of Technical Safety Requirements to Architecture Elements

These allocations are already included as part of the technical requirement tables. For this particular item, 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 | Car display will show fault |
| WDC-02 | turn off the functionality | Malfunction\_03 | Yes | Car display will show fault |