

Technical Safety Concept Lane Assistance

**Document Version: 1.2**

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



# Document history

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Editor | Description |
| 06/23/19 | 1.0 | Adam Gotlib | First draft |
| 06/23/19 | 1.1 | Adam Gotlib |  |
| 06/23/19 | 1.2 | Adam Gotlib | Removed template-specific parts of the document |
|  |  |  |  |
|  |  |  |  |

# 

# 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 Technical Safety Concept serves the purpose of deriving more detailed Technical Safety Requirements from the Functional Safety Requirements defined in the Functional Safety Concept.

# 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 | 50 ms | The LDW function shall deactivate and display a visual warning to the driver. |
| Functional  Safety  Requirement  01-02 | The lane keeping item shall ensure that the lane departure oscillating torque frequency is below Max\_Torque\_Frequency. | C | 50 ms | The LDW function shall deactivate and display a visual warning to the driver. |
| Functional  Safety  Requirement  02-01 | The lane keeping item shall ensure that the lane keeping assistance torque is applied only for Max\_Duratoin. | B | 500 ms | The LKA function shall deactivate and display a visual warning to the driver. |

## Refined System Architecture from Functional Safety Concept

### 

### Functional overview of architecture elements

|  |  |
| --- | --- |
| **Element** | **Description** |
| Camera Sensor | Captures images in front of the vehicle. |
| Camera Sensor ECU - Lane Sensing | Analyses captured images and determines when the vehicle leaves the lane by mistake. |
| Camera Sensor ECU - Torque request generator | Generates lane keeping torque and lane departure oscillating torque request when the vehicle leaves the lane by mistake. |
| Car Display | Displays visual cues for the driver, informing them of functioning of the system. |
| Car Display ECU - Lane Assistance On/Off Status | Displays on/off status of the Lane Assistance item. |
| Car Display ECU - Lane Assistant Active/Inactive | Displays active/inactive status of LDW and LKA functions. |
| Car Display ECU - Lane Assistance malfunction warning | Informs the driver when LDW or LKA malfunction. |
| Driver Steering Torque Sensor | Measures the torque provided by the driver. |
| Electronic Power Steering (EPS) ECU - Driver Steering Torque | Reads the measured torque from the Driver Steering Torque Sensor. |
| EPS ECU - Normal Lane Assistance Functionality | Estimates the required amount of additional torque to be applied based on a lane assistance system torque request and the torque provided by the driver. |
| EPS ECU - Lane Departure Warning Safety Functionality | Ensures that the lane departure oscillating torque amplitude is below Max\_Torque\_Amplitude and the lane departure oscillating torque frequency is below Max\_Torque\_Frequency. |
| EPS ECU - Lane Keeping Assistant Safety Functionality | Ensures that the lane keeping assistance torque is applied only for Max\_Duratoin. |
| EPS ECU - Final Torque | Passes torque request to the Motor. |
| Motor | Applies additional 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 | The LDW safety compontent shall ensure that the amplitude of the LDW\_Torque\_Request sent to the Final EPS Torque component is below Max\_Torque\_Amplitude. | C | 50 ms | LDW Safety Functionality | The LDW function shall deactivate and display a visual warning to the driver. |
| Technical  Safety  Requirement  02 | The validity and integrity of the data transmission for LDW\_Torque\_Request signal shall be ensured. | C | 50 ms | LDW Safety Functionality | The LDW function shall deactivate and display a visual warning to the driver. |
| Technical  Safety  Requirement  03 | As soon as a failure is detected by the LDW function, it shall deactiveate the LDW feature and the LDW\_Torque\_Request shall be set to zero. | C | 50 ms | LDW Safety Functionality | The LDW function shall deactivate and display a visual warning to the driver. |
| 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 | 50 ms | LDW Safety Functionality | The LDW function shall deactivate and display a visual warning to the driver. |
| 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 | LDW Safety Functionality | The LDW function shall deactivate and display a visual warning to the driver. |

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 compontent shall ensure that the frequency of the LDW\_Torque\_Request sent to the Final EPS Torque component is below Max\_Torque\_Frequency | C | 50 ms | LDW Safety Functionality | The LDW function shall deactivate and display a visual warning to the driver. |
| Technical  Safety  Requirement  02 | The validity and integrity of the data transmission for LDW\_Torque\_Request signal shall be ensured. | C | 50 ms | LDW Safety Functionality | The LDW function shall deactivate and display a visual warning to the driver. |
| Technical  Safety  Requirement  03 | As soon as a failure is detected by the LDW function, it shall deactiveate the LDW feature and the LDW\_Torque\_Request shall be set to zero. | C | 50 ms | LDW Safety Functionality | The LDW function shall deactivate and display a visual warning to the driver. |
| 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 | 50 ms | LDW Safety Functionality | The LDW function shall deactivate and display a visual warning to the driver. |
| 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 | LDW Safety Functionality | The LDW function shall deactivate and display a visual warning to the driver. |

**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 compontent shall ensure that the LKA\_Torque\_Request sent to the Final EPS Torque component has non-zero value for only Max\_Duration. | B | 500 ms | LKA Safety Functionality | The LKA function shall deactivate and display a visual warning to the driver. |
| Technical  Safety  Requirement  02 | The validity and integrity of the data transmission for LKA\_Torque\_Request signal shall be ensured. | B | 500 ms | LKA Safety Functionality | The LKA function shall deactivate and display a visual warning to the driver. |
| Technical  Safety  Requirement  03 | As soon as a failure is detected by the LKA function, it shall deactiveate the LKA feature and the LKA\_Torque\_Request shall be set to zero. | B | 500 ms | LKA Safety Functionality | The LKA function shall deactivate and display a visual warning to the driver. |
| 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 | 500 ms | LKA Safety Functionality | The LKA function shall deactivate and display a visual warning to the driver. |
| 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 | LKA Safety Functionality | The LKA function shall deactivate and display a visual warning to the driver. |

## Refinement of the System Architecture

****

## Allocation of Technical Safety Requirements to Architecture Elements

For this particular item, all technical safety requirements are allocated to the EPS ECU component.

## Warning and Degradation Concept

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Degradation Mode** | **Trigger for Degradation Mode** | **Safe State invoked?** | **Driver Warning** |
| WDC-01 | Deactivate LDW function. | Malfunction\_01  Malfunction\_02 | YES | Visual display |
| WDC-02 | Deactivate LKA function. | Malfunction\_03 | YES | Visual display |