

Technical Safety Concept Lane Assistance

**Document Version: [Version]**

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



# Document history

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Editor | Description |
| 07/02/2018 | 1.0 | A. Zheng | First Draft |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# 

# 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 turn functional safety requirements into technical safety requirements and allocating technical safety requirements to the system architecture. The technical safety concept 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 keeping item shall ensure that the lane departure oscillating torque amplitude stays below the max torque amplitude. | C | 50 ms | Lane departure oscillating torque amplitude is below the max torque amplitude. |
| Functional  Safety  Requirement  01-02 | The lane keeping item shall ensure that the oscillating torque amplitude stays above the minimum torque amplitude | C | 50 ms | Lane departure oscillating torque amplitude is above the min torque amplitude. |
| Functional  Safety  Requirement  02-01 | The electronic power steering control unit shall ensure that the lane keeping assistance torque is applied only until a max duration. | B | 500 ms | LKA torque is set to 0 |

## Refined System Architecture from Functional Safety Concept



### 

### Functional overview of architecture elements

|  |  |
| --- | --- |
| **Element** | **Description** |
| Camera Sensor | Sensor used to capture the road images and provide them to the Camera Sensor ECU |
| Camera Sensor ECU - Lane Sensing | Software module used to detect the lane line positions from the Camera Sensor’s images |
| Camera Sensor ECU - Torque request generator | Software module used to calculate the required torque requested by the Electronic Power Steering ECU |
| Car Display | Displays warning to the driver |
| Car Display ECU - Lane Assistance On/Off Status | Indicates the status of the Lane Assistance function |
| Car Display ECU - Lane Assistant Active/Inactive | Indicates a malfunction on the Lane Assistance function |
| Car Display ECU - Lane Assistance malfunction warning | Indicates if the Lane assistance function is properly functioning |
| Driver Steering Torque Sensor | Measures the torque applied to the steering wheel by the driver |
| Electronic Power Steering (EPS) ECU - Driver Steering Torque | Software module used to receive the driver’s torque request on the steering wheel |
| EPS ECU - Normal Lane Assistance Functionality | Software module used to receive the Camera Sensor ECU torque request |
| EPS ECU - Lane Departure Warning Safety Functionality | Software module used to ensure the torque amplitude stays below the maximum torque amplitude and above the minimum torque amplitude |
| EPS ECU - Lane Keeping Assistant Safety Functionality | Software module used to ensure the Lane Keeping Assistance functionality application is not activate more than the maximum duration time |
| EPS ECU - Final Torque | Combine the torque request from the Lane Keeping and Lane Departure Warning functionalities and send the final torque to the motor |
| Motor | Applies to the requested 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 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 Amplitude shall be set 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 | 50 ms | 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 the 'LDW\_Torque\_Request' shall be set to zero. | C | 50 ms | LDW Safety | LDW Torque Request Amplitude shall be set to zero |
| Technical  Safety  Requirement  04 | The validity and integrity of the data transmission for 'LDW\_Torque\_Request' signal shall be ensured. | C | 50 ms | LDW Safety | LDW Torque Request Amplitude shall be set 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 and Integrity Check | 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\_Frequency’ sent to the to the 'Final electronic power steering Torque' component is below ‘Max\_Torque\_Frequency’ | C | 50 ms | LDW Safety | LDW Torque Request Frequency shall be set to zero |
| Technical  Safety  Requirement  02 | As soon as a failure is detected by the LDW function, it shall deactivate the LDW feature and the 'LDW\_Torque\_Request\_Frequency' shall be set to zero. | C | 50 ms | LDW Safety | LDW Torque Request Frequency shall be set to zero |
| Technical  Safety  Requirement  03 | The validity and integrity of the data transmission for 'LDW\_Torque\_Request\_Frequency' signal shall be ensured. | C | 50 ms | 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 | 50 ms | LDW Safety | LDW Torque Request Frequency shall be set 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 and Integrity Check | LDW Torque Request Frequency shall be set to zero |

**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 the duration of the 'LKA\_Torque\_Request’ is applied for less than the max duration. | B | 500 ms | LKA Safety | LKA torque set to zero |
| Technical  Safety  Requirement  02 | As soon as a failure is detected by the LKA function, it shall deactivate the LKA feature and the ''LKA\_Torque\_Request’’ shall be set to zero. | B | 500 ms | LKA Safety | LKA torque set to zero |
| Technical  Safety  Requirement  03 | The validity and integrity of the data transmission for 'LKA\_Torque\_Request’ signal shall be ensured. | B | 500 ms | LKA Safety | LKA torque 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 | 500 ms | LKA Safety | LKA torque set 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 and Integrity Check | LKA torque set to zero |

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

**[**

## 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 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. | X |  |  |
| Technical  Safety  Requirement  01-01-02 | 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. | x |  |  |
| Technical  Safety  Requirement  01-01-03 | 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. | X |  |  |
| Technical  Safety  Requirement  01-01-04 | The validity and integrity of the data transmission for 'LDW\_Torque\_Request' signal shall be ensured. | X |  |  |
| Technical  Safety  Requirernent  01-01-05 | Memory test shall be conducted at start up of the EPS ECU to check for any faults in memory. | X |  |  |
| Technical  Safety  Requirement  01-02-01 | The LDW safety component shall ensure that the frequency of the ‘LDW\_Torque\_Request\_Frequency’ sent to the to the 'Final electronic power steering Torque' component is below ‘Max\_Torque\_Frequency’ | X |  |  |
| Technical  Safety  Requirement  01-02-02 | As soon as a failure is detected by the LDW function, it shall deactivate the LDW feature and the 'LDW\_Torque\_Request\_Frequency' shall be set to zero. | X |  |  |
| Technical  Safety  Requirement  01-02-03 | The validity and integrity of the data transmission for 'LDW\_Torque\_Request\_Frequency' signal shall be ensured. | X |  |  |
| Technical  Safety  Requirement  01-02-04 | 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. | X |  |  |
| Technical  Safety  Requirement  01-02-05 | Memory test shall be conducted at start up of the EPS ECU to check for any faults in memory. | X |  |  |
| Technical  Safety  Requirement  02-01-01 | The LKA safety component shall ensure the duration of the 'LKA\_Torque\_Request’ is applied for less than the max duration. | X |  |  |
| Technical  Safety  Requirement  02-01-02 | As soon as a failure is detected by the LKA function, it shall deactivate the LKA feature and the ''LKA\_Torque\_Request’’ shall be set to zero. | X |  |  |
| Technical  Safety  Requirement  02-01-03 | The validity and integrity of the data transmission for 'LKA\_Torque\_Request’ signal shall be ensured. | X |  |  |
| Technical  Safety  Requirement  02-01-04 | 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. | X |  |  |
| Technical  Safety  Requirement  02-01-05 | Memory test shall be conducted at start up of the EPS ECU to check for any faults in memory. | X |  |  |

## Warning and Degradation Concept

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Degradation Mode** | **Trigger for Degradation Mode** | **Safe State invoked?** | **Driver Warning** |
| WDC-01 | Turn System off | Malfunction 01  Malfunction 02 | Yes | Dashboard warning light |
| WDC-02 | Turn System off | Malfunction 03 | Yes | Dashboard warning light |