

Technical Safety Concept Lane Assistance

**Document Version: 1.0**

**Released on 2018-05-25**



# Document history

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Editor | Description |
| 25-05-2018 | 1.0 | Srigandhan | First Submission |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# 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 refine the functional safety requirements established in the functional safety concept into technical safety requirement.​ ​These new​ ​requirements​ ​are​ ​more​ ​concrete​ ​and​ ​gets​ ​into​ ​details​ ​of​ ​the​ ​item’s​ ​technology​ ​as​ ​specified by​ ​ISO​ ​26262.

# 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 | Turn Off System |
| 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 | Turn Off System |
| Functional  Safety  Requirement  02-01 | The electronic power steering ECU shall ensure that the lane keeping assistance torque is applied for only Max\_Duration | B | 500 ms | Turn Off System |
| Functional  Safety  Requirement  02-02 | The electronic power steering ECU shall be deactivated​ ​when​ ​the​ ​electronic​ ​power steering​ ​ECU​ ​detects​ ​the​ ​camera sensor​ ​is​ ​not​ ​working. | B | 50 ms | Turn Off System |

## Refined System Architecture from Functional Safety Concept



### Functional overview of architecture elements

|  |  |
| --- | --- |
| **Element** | **Description** |
| Camera Sensor | Provides camera images to the Camera Sensor ECU. |
| Camera Sensor ECU - Lane Sensing | Detects lane line positions from camera images. |
| Camera Sensor ECU - Torque request generator | Generates a torque request to the Electronic Power Steering ECU. |
| Car Display | Car Display is responsible for providing feedback to the driver about the status of lane assistant system |
| Car Display ECU - Lane Assistance On/Off Status | Software module responsible for displaying **On/Off** status of LDW & LKA functions. |
| Car Display ECU - Lane Assistant Active/Inactive | Software module responsible for displaying **Active/Inactive** status of LDW & LKA function. |
| Car Display ECU - Lane Assistance malfunction warning | Indicates malfunctions on the Lane Assistance functionality. |
| Driver Steering Torque Sensor | Measure the torque applied to the steering wheel by the driver. |
| Electronic Power Steering (EPS) ECU - Driver Steering Torque | Software module receiving the driver’s torque request from the steering wheel. |
| EPS ECU - Normal Lane Assistance Functionality | Receives torque request from Camera Sensor ECU and transfers it to Safety Lane Assistance Functionality. |
| EPS ECU - Lane Departure Warning Safety Functionality | Checks for malfunction of Lane Departure Warning and translates torque request into final torque output. |
| EPS ECU - Lane Keeping Assistant Safety Functionality | Checks for malfunction of Lane Keeping Assistant and transfers torque request to final torque output. |
| EPS ECU - Final Torque | Combine​ ​the​ ​torque​ ​request​ ​from​ ​the​ ​LKA safety​ ​and​ ​LDW safety functionalities​ ​and​ ​sends​ ​them​ ​to​ ​the​ ​Motor. |
| Motor | An electric motor that applies the torque indicated by the Electronic Power Steering ECU 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  01-01-01 | 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. | C | 50 ms | LDW safety block | LDW\_Torque\_Output is set to zero |
| 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 | C | 50 ms | LDW safety block | LDW\_Torque\_Output is set to zero |
| 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. | C | 50 ms | LDW safety block | LDW\_Torque\_Output is set to zero |
| Technical  Safety  Requirement  01-01-04 | The validity and integrity of the data transmission for 'LDW\_Torque\_Request' signal shall be ensured. | C | 50 ms | Data Transmission Integrity Check | LDW\_Torque\_Output is set to zero |
| Technical  Safety  Requirement  01-01-05 | Memory test shall be conducted at startup of the EPS ECU to check for any faults in memory. | A | Ignition cycle | Memory Test | LDW\_Torque\_Output 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  01-02-01 | 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 | 50 ms | LDW safety block | LDW\_Torque\_Output is 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’ shall e set to zero. | C | 50 ms | LDW Safety | LDW\_Torque\_Output is set to zero |
| Technical  Safety  Requirement  03 | 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\_Output is 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 | Data Transmission Integrity Check | LDW\_Torque\_Output is 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 | Memory Test | LDW\_Torque\_Output is set to zero |

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

|  |  |  |
| --- | --- | --- |
| **ID** | **Validation Acceptance Criteria and Method** | **Verification Acceptance Criteria and Method** |
| Technical  Safety  Requirement  01-01-01 | Validate the Max\_Torque\_Amplitude is the chosen from the Lane Departure Warning Validation | Verify the Lane Departure Warning functionality is turned off. |
| Technical  Safety  Requirement  01-01-02 | Validate the ‘TORQUE\_LIMITER’ sends the error\_status\_torque\_limiter signal to the LDW\_SAFETY\_ACTIVATION. | Verify the Car Display ECU displays the Lane Departure Warning malfunction warning signal. |
| Technical Safety Requirement  01-01-03 | Validate the ‘TORQUE\_LIMITER’ sends ‘LDW\_Torque\_Request’ with zero. | Verify the Final EPS Torque generator receives LDW\_Torque\_Request of zero. |
| Technical Safety Requirement 01-01-04 | Validate the ‘TORQUE\_LIMITER’ calculate and sends the correct cyclic redundancy check (CRC) and Alive counter for data transmission validity and integrity. | Verify the functionality is turn off if there is a CRC or Alive counter discrepancy. |
| Technical Safety Requirement  01-01-05 | Validate the Safety Startup Memory test to check memory faults catch memory faults. | Verify the Lane Departure Warning is turned off when the Safety Startup Memory fails. |
| Technical Safety Requirement 01-02-01 | Validate the Max\_Torque\_Frequency set is the chosen from the Lane Departure Warning Acceptance Criteria. | Verify the functionality is turned off if the ‘LDW\_Torque\_Request’ frequency exceeds Max\_Torque\_Request. |

**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  02-01-01 | The Lane Keeping Assistance safety component shall ensure the duration of the lane keeping assistance torque is applied for less than Max\_Duration | B | 500 ms | LKA Safety | Lane Keeping Assistance torque to zero. |
| Technical  Safety  Requirement  02-01-02 | When the Lane Keeping Assistance function deactivates, the ‘LKA Safety’ shall send a signal to the Car Display ECU to turn on a warning light. | B | 500 ms | LKA Safety | Lane Keeping Assistance torque to zero. |
| Technical  Safety  Requirement  02-01-03 | When a failure is detected, the Lane Keeping Assistance function shall deactivate and the ‘LKA\_Torque\_Request’ shall be zero. | B | 500 ms | LKA Safety | Lane Keeping Assistance torque to zero. |
| Technical  Safety  Requirement  02-01-04 | The validity and integrity of the data transmission for ‘LKA\_Torque\_Request’ signal shall be ensured. | B | 500 ms | LKA Safety | Lane Keeping Assistance torque to zero. |
| Technical  Safety  Requirement  02-01-05 | Memory test shall be conducted at startup of the EPS ECU to check for any memory problems | A | Ignition cycle | Data Transmission Integrity Check | Lane Departure Warning torque to zero. |

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

|  |  |  |
| --- | --- | --- |
| **ID** | **Validation Acceptance Criteria and Method** | **Verification Acceptance Criteria and Method** |
| Technical  Safety  Requirement  02-01-01 | Validate the Max\_Duration is set to the chosen value from LKA Validation Assistance Criteria | Verify the functionality is turned off after it is applied for Max\_Duration. |
| Technical  Safety  Requirement  02-01-02 | Validate the ‘TORQUE\_LIMITER’ sends the error\_status\_torque\_limiter signal to the LKA\_SAFETY\_ACTIVATION. | Verify the Car Display ECU displays the Lane Keeping Assistance malfunction warning signal. |
| Technical Safety Requirement  02-01-03 | Validate the ‘TORQUE\_LIMITER’ sends ‘LKA\_Torque\_Request’ with zero. | Verify the Final EPS Torque generator receives LKA\_Torque\_Request of zero. |
| Technical Safety Requirement 02-01-04 | Validate the ‘TORQUE\_LIMITER’ calculate and sends the correct cyclic redundancy check (CRC) and Alive counter for data transmission validity and integrity. | Verify the functionality is turn off if there is a CRC or Alive counter discrepancy. |
| Technical Safety Requirement  02-01-05 | Validate the Safety Startup Memory test to check memory faults catch memory faults. | Verify the Lane Keeping Assistance is turned off when the Safety Startup Memory fails. |

## Refinement of the System Architecture

****

## Allocation of Technical Safety Requirements to Architecture Elements

For the Lane Assistance item, all technical safety requirements are allocated to the Electronic Power Steering ECU. For the exact allocation within EPS ECU, please refer to the technical safety requirements tables above.

## Warning and Degradation Concept

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Degradation Mode** | **Trigger for Degradation Mode** | **Safe State invoked?** | **Driver Warning** |
| WDC-01 | Turn off LDW functionality | Malfunction\_01,  Malfunction\_02 | Yes | Turn on warning light of the LDW functionality |
| WDC-02 | Turn off LKA functionality | Malfunction\_03,  Malfunction\_04 | Yes | Turn on warning light of the LKA functionality |