

Technical Safety Concept Lane Assistance

**Document Version: 1.0**

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



# Document history

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Editor | Description |
| 5/28/2018 | 1.0 | Rahul Bhartari | First Revision |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# 

# 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 technical safety concept is to transform functional safety requirements established in functional safety concept into the technical safety requirements. These requirements get into the details of the item’s technology.

The technical safety concept involves:

* Turning functional safety requirements into technical safety requirements
* Allocating technical safety requirements to the system architecture

# 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 | Oscillation torque amplitude is less than Max\_Torque\_Amplitude |
| 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 | Oscillation torque frequency is less than Max\_Torque\_Frequency |
| Functional  Safety  Requirement  02-01 | The lane keeping item shall ensure that the lane keeping assistance torque is applied for only Max\_Duration | B | 200ms | The Lane Keeping Assistance Torque is zero |

## Refined System Architecture from Functional Safety Concept

### 

### Functional overview of architecture elements

|  |  |
| --- | --- |
| **Element** | **Description** |
| Camera Sensor | Capture and provide road images to Camera ECU |
| Camera Sensor ECU - Lane Sensing | Detect lane positions in camera images |
| Camera Sensor ECU - Torque request generator | Generate torque request to Electronic Power Steering ECU |
| Car Display | Show warnings and system status to driver |
| Car Display ECU - Lane Assistance On/Off Status | Indicates if Lane Assistance function is turned on/off |
| Car Display ECU - Lane Assistant Active/Inactive | Indicates if LA function is active and detecting lanes |
| Car Display ECU - Lane Assistance malfunction warning | Indicates the malfunction in Lane Assistance function |
| Driver Steering Torque Sensor | Measures torque provided by the driver on the steering wheels and delivers to Electronic Power Steering ECU |
| Electronic Power Steering (EPS) ECU - Driver Steering Torque | Process input from Driver Steering Torque Sensor |
| EPS ECU - Normal Lane Assistance Functionality | Receives torque request from Camera Sensor ECU and sends it to Lane Assistance function |
| EPS ECU - Lane Departure Warning Safety Functionality | Checks for malfunctions in Lane Departure Warning function and transforms torque request into final torque output |
| EPS ECU - Lane Keeping Assistant Safety Functionality | Checks for malfunctions in Lane Keeping Assistance function and transfers the output torque |
| EPS ECU - Final Torque | Generates final torque from torque requests from LDW and LKA functions |
| Motor | Applies received 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 ‘LDW\_Torque\_Request’ sent to ‘Final electronic power steering torque’ component is below ‘Max\_Torque\_Amplitude’ | C | 50ms | LDW Safety | LDW\_Activation\_Status is zero |
| Technical  Safety  Requirement  02 | If failure is detected by LDW function, it LDW safety component shall deactivate LDW function and set ‘LDW\_Torque\_Request’ to zero | C | 50ms | LDW Safety | LDW\_Activation\_Status is zero |
| Technical  Safety  Requirement  03 | When LDW function is deactivated, ‘LDW Safety’ component shall send a signal to the Car display ECU to turn on a warning light | C | 50ms | LDW Safety | LDW\_Error\_Status is zero |
| Technical  Safety  Requirement  04 | The validity and integrity of the data transmission for ‘LDW\_Torque\_Request’ shall be ensured | C | 50ms | Data Transmission Integrity Check | NA |
| Technical  Safety  Requirement  05 | At the startup of EPS ECU, a memory test shall be conducted to check for any faults in memory | A | Ignition cycle | Memory Test | LDW\_Activation\_Status is zero |

Functional Safety Requirement 01-02 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 ‘LDW\_Torque\_Request’ sent to ‘Final electronic power steering torque’ component is below ‘Max\_Torque\_Frequency | C | 50ms | LDW Safety | LDW function torque is 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 chosen from the Lane Departure Warning Validation | Verify the Lane Departure function is turned off if torque amplitude exceeds Max\_Torque\_Amplitude |
| 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 zero as ‘LDW\_Torque\_Request’ | Verify the Final EPS Torque generator receives a LDW\_Torque\_Request of zero |
| Technical  Safety  Requirement  01-01-04 | Validate the ‘TORQUE\_LIMITER’ calculates and sends the correct cyclic redundancy check(CRC) and ‘Alive’ counter for data transmission validity and integrity | Verify the function is turned off if CRC mismatch or Alive counter discrepancy happens |
| Technical  Safety  Requirement  01-01-05 | Validate the Safety Startup Memory test to check and catch memory faults | Very the Lane Departure Warning function is turned off if Safety Startup Memory test fails |
| Technical  Safety  Requirement  01-02-01 | Validate the ‘Max\_Torque\_Frequency’ is set as chosen from Lane Departure Warning Acceptance Criteria | Very the Lane Departure Warning function is turned off if the ‘LDW\_Torque\_Request’ frequency exceeds Max\_Torque\_Frequency |

**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 ‘LKA\_Torque\_Request’ is sent to the ‘Final electronic power steering Torque’ component for only ‘Max\_Duration’. | B | 500ms | LKA Safety |  |
| 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 e set to zero. | B | 500ms | LKA Safety |  |
| Technical  Safety  Requirement  03 | As soons 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 | LKA Safety |  |
| Technical  Safety  Requirement  04 | The validity and integrity of the data transmission for ‘LKA\_Torque\_Request’ signal shall be ensured. | B | 500 ms | Data Transmission Integrity Check |  |
| Technical  Safety  Requirement  05 | Memory test shall be conducted at start up of the EPS ECU to check for any faults in mermory. | A | ignition cycle | Memory Test |  |

**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 a 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 turned 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

All technical safety requirements were allocated to the Electronic Power Steering ECU. For the exact allocation within EPS ECU compare the technical requirement tables above.

## Warning and Degradation Concept

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Degradation Mode** | **Trigger for Degradation Mode** | **Safe State invoked?** | **Driver Warning** |
| WDC-01 | Turn off Lane Departure Warning Function | Malfunction\_01  Malfunction\_02  Malfunction\_05  Malfunction\_06 | Yes | Lane Departure Warning Malfunction warning on car display |
| WDC-02 | Turn off Lane Keeping Assistance Function | Malfunction\_03  Malfunction\_04 | Yes | Lane Keeping Assistance Malfunction warning on car display |