

Technical Safety Concept Lane Assistance

**Document Version: [Version]**

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



# Document history

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Editor | Description |
| 2018.10.29 |  | Wanlin Yang | gandue |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# 

# 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 defines how the subsystems interact at the message level and describes how the ECUs communicate with each other.

# 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 Electric Power Steering ECU shall ensure that the oscillation torque amplitude requested by the LDW function is below MAX\_Torque\_Amplitude | C | 50 ms | LDW will set the oscillating torque amplitude to 0. |
| Functional  Safety  Requirement  01-02 | The Electric Power Steering ECU shall ensure that the oscillation torque frequency requested by the LDW function is below MAX\_Torque\_Frequency | C | 50 ms | LDW will set the oscillating torque frequency to 0. |
| 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 | 50 ms | LKA will turn off the assistance system. |

## Refined System Architecture from Functional Safety Concept



### Functional overview of architecture elements

|  |  |
| --- | --- |
| **Element** | **Description** |
| Camera Sensor | Capture road images and provide them to the Camera Sensor ECU. |
| Camera Sensor ECU - Lane Sensing | Software module detecting the lane line positions from the Camera Sensor images. |
| Camera Sensor ECU - Torque request generator | Software module calculating the necessary torque to be requested to the Electronic Power Steering ECU. |
| Car Display | Display warning for the driver. |
| Car Display ECU - Lane Assistance On/Off Status | Indicate the status of the Lane Assistance functionality (On/Off). |
| Car Display ECU - Lane Assistant Active/Inactive | Indicate if the Lane Assistance functionality is properly functioning (Active/Inactive). |
| Car Display ECU - Lane Assistance malfunction warning | Indicate a malfunction 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 | Software module receiving the Camera Sensor ECU torque request. |
| EPS ECU - Lane Departure Warning Safety Functionality | Software module ensuring the torque amplitude is below Max\_Torque\_Amplitude and torque frequency is below Max\_Torque\_Frequency. |
| EPS ECU - Lane Keeping Assistant Safety Functionality | Software module ensuring the Lane Keeping Assistance functionality application is not activate more than Max\_Duration time. |
| EPS ECU - Final Torque | Combine the torque request from the Lane Keeping and Lane Departure Warning functionalities and sends them to the driver. |
| Motor | Applies the required torque to the steering wheels. |

# 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 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 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 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 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 | LDW Safety | LDW torque 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 | 50 ms | LDW Safety | LDW torque 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 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 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 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 | LDW Safety | LDW torque 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 the duration of the lane keeping assistance torque is applied for less than Max\_Duration | C | 50 ms | LKA Safety | LKA torque to zero |
| Technical  Safety  Requirement  02 | When the LKA function deactivates, the “LKA Safety” shall send a signal to the Car Display ECU to turn on a warning light. | C | 50 ms | LKA Safety | LKA torque to zero |
| Technical  Safety  Requirement  03 | When a failure is detected, the LKA function shall deactivate and the “LKA\_Torque\_Request” shall be zero. | C | 50 ms | LKA Safety | LKA torque to zero |
| Technical  Safety  Requirement  04 | The validity and integrity of the data transmission for “LKA\_Torque\_Request” signal shall be ensured. | C | 50 ms | LKA Safety | LKA torque to zero |
| Technical  Safety  Requirement  05 | Memory test shall be conducted at stat up of the EPS ECU to check for any memory problems. | A | Ignition cycle | Data Transmission Integrity Check | LKA torque to zero |

## Refinement of the System Architecture



## Allocation of Technical Safety Requirements to Architecture Elements

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Functional 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  Requirement  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” sent to the “Final Electronic Power Steering Torque” component is below Max\_Torque\_Frequency. | X |  |  |
| Technical Safety  Requirement  01-02-02 | 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  01-02-03 | 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  01-02-04 | The validity and integrity of the data transmission for “LDW\_Torque\_Request” signal shall be ensured. | 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 lane keeping assistance torque is applied for less than Max\_Duration | X |  |  |
| Technical Safety  Requirement  02-01-02 | When the LKA function deactivates, the “LKA Safety” shall send a signal to the Car Display ECU to turn on a warning light. | X |  |  |
| Technical Safety  Requirement  02-01-03 | When a failure is detected, the LKA function shall deactivate and the “LKA\_Torque\_Request” shall be zero. | X |  |  |
| Technical Safety  Requirement  02-01-04 | The validity and integrity of the data transmission for “LKA\_Torque\_Request” signal shall be ensured. | X |  |  |
| Technical Safety  Requirement  02-01-05 | Memory test shall be conducted at stat up of the EPS ECU to check for any memory problems. | X |  |  |

## 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,Malfunction\_04 | Yes | The warning is shown on the Car Display system. |
| WDC-02 | Turn off the functionality. | Malfunction\_03,Malfunction\_05 | Yes | The warning is shown on the Car Display system. |