

Technical Safety Concept Lane Assistance

**Document Version: [Version]**

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



# Document history

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Editor | Description |
| 2018/9/26 | 1.0 | Jiang Yue | First attempt |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# 

# 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

**[Instructions: Answer what is the purpose of a 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 Electronic Power Steering ECU shall ensure that the oscillating 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 electronic power steering ECU shall eusure that the lane departure warning oscillating torque frequency 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 within Max\_Duration | B | 500 ms | Turn off the system and warning. |

## Refined System Architecture from Functional Safety Concept



### Functional overview of architecture elements

|  |  |
| --- | --- |
| **Element** | **Description** |
| Camera Sensor | Capture road image data and send to Camera sensor ECU. |
| Camera Sensor ECU - Lane Sensing | Identifying accidental departure from the road and sending information to the Car Display ECU |
| Camera Sensor ECU - Torque request generator | Generator torque and send to Electronic Power Steering ECU |
| Car Display | Display the messages and warnings send from Car Display ECU to the driver |
| Car Display ECU - Lane Assistance On/Off Status | Indicate the status of the Lane Assistance Functionality |
| Car Display ECU - Lane Assistant Active/Inactive | Indicate if the Lane Assistance Functionality is active |
| Car Display ECU - Lane Assistance malfunction warning | Indicate if the Lane Assistance Functionality is malfunction |
| Driver Steering Torque Sensor | Measure the steering wheel torque applied by the driver |
| Electronic Power Steering (EPS) ECU - Driver Steering Torque | Measure the steering wheel torque applied by the EPS |
| EPS ECU - Normal Lane Assistance Functionality | Receive torque request from Camera Sensor ECU |
| EPS ECU - Lane Departure Warning Safety Functionality | Send malfunction warning to Car Display ECU. send LDW Torque Request and LDW Action Status to Final Torque ensure the torque amplitude and frequency is below limit. |
| EPS ECU - Lane Keeping Assistant Safety Functionality | Receive Primary\_LDW\_Torque\_Request and ensure Assistance function is not exceed Max\_Duration |
| EPS ECU - Final Torque | Combine torque request and send to motor |
| Motor | Apply torque to 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 amplitude shall set to 0. |
| 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 amplitude shall set to 0. |
| 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 amplitude shall set to 0. |
| 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 amplitude shall set to 0. |
| 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 | Memery Test | LDW torque amplitude shall set to 0. |

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 amplitude 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 frequency shall set to 0. |
| 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 frequency shall set to 0. |
| 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 frequency shall set to 0. |
| 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 frequency shall set to 0. |
| 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 | Memery Test | LDW torque frequency shall set to 0. |

**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 lane keeping item shall ensure that the lane keeping assistance torque is applied less than Max\_Duration | B | 500 ms | LKA Safety | LKA torque request shall set to 0 |
| Technical  Safety  Requirement  02 | 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 request shall set to 0 |
| Technical  Safety  Requirement  03 | As soon as a failure is detected by the LDW function, it shall deactivate the LDW feature and the 'LKA\_Torque\_Request' shall be set to zero. | B | 500 ms | LKA Safety | LKA torque request shall set to 0 |
| 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 | LKA torque request shall set to 0 |
| Technical  Safety  Requirement  05 | Memory test shall be conducted at start up of the EPS ECU to check for any faults in memory. | B | ignition cycle | Memery Test | LKA torque request shall set to 0 |

## 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 amplitude 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 lane keeping item shall ensure that the lane keeping assistance torque is applied less than Max\_Duration | **X** |  |  |
| Technical  Safety  Requirement  02-01-02 | 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  02-01-03 | As soon as a failure is detected by the LDW function, it shall deactivate the LDW feature and the 'LKA\_Torque\_Request' shall be set to 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 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 off the torque and warning. | Malfunction\_01  Malfunction\_02 | YES | Warning light on dashboard with warning noise. |
| WDC-02 | Turn system off and warning. | Malfunction\_03 | YES | Warning light on dashboard with warning noise. |