

Technical Safety Concept Lane Assistance

**Document Version: [Version]**

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



# Document history

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Editor | Description |
| 8/25/2018 | Ver 1.0 | Jun Imamura | 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

Technical safety concept is a documentation activity to define requirements in more detail. This will define the requirement for each sensor/controller/actuator level.

# 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 | System turned off |
| Functional  Safety  Requirement  01-02 | The lane keeping item shall ensure that the lane departure oscillating torque frequency is blow Max\_Torque\_Frequency | C | 50ms | System turned off |
| 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 | 500ms | System turned off |

## Refined System Architecture from Functional Safety Concept



### Functional overview of architecture elements

|  |  |
| --- | --- |
| **Element** | **Description** |
| Camera Sensor | Capture the images ahead of the vehicle and provide them to the Camera Sensor ECU |
| Camera Sensor ECU - Lane Sensing | Process the provided sensor raw values and detect / calculate the position of the car on the road. |
| Camera Sensor ECU - Torque request generator | Request a desirable torque to the electronic power steering ECU. |
| Car Display | Provide both activation status and operating status of the lane assistance functionality. |
| Car Display ECU - Lane Assistance On/Off Status | Indicate the ON/OFF status of the lane assistance functionality. |
| Car Display ECU - Lane Assistant Active/Inactive | Indicate the activation status of the lane assistance functionality. |
| Car Display ECU - Lane Assistance malfunction warning | Indicate a malfunction status of 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 | Receive steering torque value from driver steering torque sensor. |
| EPS ECU - Normal Lane Assistance Functionality | Receive torque request from camera sensor ECU torque request. |
| EPS ECU - Lane Departure Warning Safety Functionality | Ensure the torque amplitude and frequency are below Max\_Torque\_Amplitude / Max\_Torque\_Frequency respectively. |
| EPS ECU - Lane Keeping Assistant Safety Functionality | Ensure the lane keeping assistance functionality won’t be activated longer than Max\_duration. |
| EPS ECU - Final Torque | Integrate the information from lane safety functionality and driver steering torque sensor. Then send and steering torque request to the motor. |
| Motor | Apply required 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 01-01-01 | 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 | 50ms | EPS ECU - Lane Departure Warning Safety Functionality | LDW Torque Request Amplitude 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 | 50ms | EPS ECU - Lane Departure Warning Safety Functionality | LDW Torque Request Amplitude set to zero. |
| Technical  Safety  Requirement 01-01-03 | As soon as a failure is detected by the LDW function, the ‘LDW\_Torque\_Request’ shall be set to zero | C | 50ms | EPS ECU - Lane Departure Warning Safety Functionality | LDW Torque Request Amplitude 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 | 50ms | EPS ECU - Lane Departure Warning Safety Functionality |  |
| 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. | A | Ignition cycle | Data Transmission Integrity Check |  |

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 amplitude of the ‘LDW\_Torque\_Request’ sent to the ‘Final electronic power steering Torque’ component is below ‘Max\_Torque\_Frequency | C | 50ms | EPS ECU - Lane Departure Warning Safety Functionality | LDW Torque Request Amplitude set to zero. |
| 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. | C | 50ms | EPS ECU - Lane Departure Warning Safety Functionality |  |
| Technical  Safety  Requirement  01-02-03 | As soon as a failure is detected by the LDW function, the ‘LDW\_Torque\_Request’ shall be set to zero | C | 50ms | EPS ECU - Lane Departure Warning Safety Functionality |  |
| Technical  Safety  Requirement  01-02-04 | The validity and integrity of the data transmission for ‘LDW\_Torque\_Request’ signal shall be ensured. | C | 50ms | EPS ECU - Lane Departure Warning Safety Functionality |  |
| 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. | A | Ignition cycle | Data Transmission Integrity Check |  |

**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 LKA safety component shall ensure that the duration of the lane keeping assistance torque is applied for less than ‘Max\_Duration’. | B | 50ms | EPS ECU - Lane Keeping Assistance Safety Functionality | Lane Keeing Assistance torque set to zero. |
| 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. | B | 50ms | EPS ECU - Lane Keeping Assistance Safety Functionality |  |
| Technical  Safety  Requirement 02-01-03 | As soon as a failure is detected by the LKA function, the ‘LKA\_Torque\_Request’ shall be set to zero | B | 50ms | EPS ECU - Lane Keeping Assistance Safety Functionality |  |
| Technical  Safety  Requirement 02-01-04 | The validity and integrity of the data transmission for ‘LKA\_Torque\_Request’ signal shall be ensured. | B | 50ms | EPS ECU - Lane Keeping Assistance Safety Functionality |  |
| 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. | A | Ignition cycle | Data Transmission Integrity Check |  |

## 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, 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, 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 that the duration of the lane keeping assistance torque is applied for 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 LKA function, 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 | System turned off | Malfunction\_01  Malfunction\_02 | Yes | Warning indication on the car display |
| WDC-02 | System turned off | Malfunction\_03 | Yes | Warning indication of the car display |