

Technical Safety Concept Lane Assistance

**Document Version: [Version]**

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



# Document history

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Editor | Description |
| 05.03.2018 | 1.0 | Qingqing Xia | First version of this document |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# 

# 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 part of the product development phase. It is derived from functional safety concept and give more concrete and details of the item's technology.

# 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 |  |
| 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 |  |
| Functional  Safety  Requirement  02-01 | The electronic power steering ECU  shall ensure that the Lane Keeping  Assistance torque is applied only  Max\_Duration. | B | 500ms |  |

## Refined System Architecture from Functional Safety Concept

### 

### Functional overview of architecture elements

|  |  |
| --- | --- |
| **Element** | **Description** |
| Camera Sensor | Deliver camera(road) images to the Camera Sensor ECU. |
| Camera Sensor ECU - Lane Sensing | Sense where the car position in the lane |
| Camera Sensor ECU - Torque request generator | Calculate the torque in order to keep the car in the lane |
| Car Display | Show warning to the driver |
| Car Display ECU - Lane Assistance On/Off Status | Show the driver is the Lane Assistance is on or off |
| Car Display ECU - Lane Assistant Active/Inactive | Show the driver is the Lane Assistance is active or inactive |
| Car Display ECU - Lane Assistance malfunction warning | Show the driver is the Lane Assistance is malfunction |
| Driver Steering Torque Sensor | Measure the steering torque by the driver and provides it to Electronic Power Steering ECU |
| Electronic Power Steering (EPS) ECU - Driver Steering Torque | Module receive the torque introduced by the driver |
| EPS ECU - Normal Lane Assistance Functionality | Module receive the camera senor torque request |
| EPS ECU - Lane Departure Warning Safety Functionality | Module to make sure the oscillating torque amplitude is below Max\_Torque\_Amplitude and frequency below the Max\_Torque\_Frequency |
| EPS ECU - Lane Keeping Assistant Safety Functionality | Module to make sure the lane keeping torque applied only for a max duration defined in the |
| EPS ECU - Final Torque | Based on the torque request from the Lane  Keeping and Lane Departure Warning  Items, to calculate the final torque and deliver them to the Motor. |
| Motor | Applied the received final torque from EPS ECU to the 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 validity and integrity of the  data transmission for  ‘LDW\_Torque\_Request’ signal  shall be ensured. | C | 50ms | Data transmission integrity check | LDW\_Activation\_Status  is zero |
| Technical  Safety  Requirement  02 | The LDW safety component  shall ensure that the amplitude  of ‘LDW\_Torque\_Request’ sent  to the ‘Final electronic power  steering Torque’ component is  below ‘Max\_Torque\_Amplitude’. | C | 50ms | LDW Safety | LDW\_Activation\_Status  is 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 | 50ms | LDW Safety | LDW\_Activation\_Status  is zero |
| Technical  Safety  Requirement  04 | As soons 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 | LDW Safety | LDW\_Er  ror\_Stat  us is 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 | Memory test | LDW\_A  ctivation  \_Status  is 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 validity and integrity of the  data transmission for  ‘LDW\_Torque\_Request’ signal  shall be ensured. | C | 50ms | Data transmission integrity check | LDW\_A  ctivation  \_Status  is zero |
| Technical  Safety  Requirement  02 | The LDW safety component  shall ensure that the frequency  of ‘LDW\_Torque\_Request’ sent  to the ‘Final electronic power  steering Torque’ component is  below ‘Max\_Torque\_Amplitude’. | C | 50ms | LDW Safety | LDW\_A  ctivation  \_Status  is 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 | 50ms | LDW Safety | LDW\_A  ctivation  \_Status  is zero |
| Technical  Safety  Requirement  04 | 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 | LDW Safety | LDW\_Er  ror\_Stat  us is 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\_A  ctivation  \_Status  is 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 validity and integrity of the  data transmission for  ‘LKA\_Torque\_Request’ signal  shall be ensured. | B | 500ms | Data transmission integrity check | LKA\_Acion\_Status  is zero |
| Technical  Safety  Requirement  02 | The LKA safety component  shall ensure that the duration  of ‘LKA\_Torque\_Request’ sent  to the ‘Final electronic power  steering Torque’ component is  below ‘Max\_Duration’. | B | 500ms | LKA Safety | LKA\_Activat  ion\_Status  is zero |
| Technical  Safety  Requirement  03 | As soon as a failure is detected  by the LKW function, it shall  deactivate the LKW feature and  the ‘LKW\_Torque\_Request’  shall be set to zero. | B | 500ms | LKA Safety | LKA\_Activat  ion\_Status  is zero |
| Technical  Safety  Requirement  04 | As soon as the LKW function  deactivates the LKW feature,  the ‘LKW Safety’ software block  shall send a signal to the car  display ECU to turn on a  warning light. | B | 500ms | LKA Safety | LKA\_Error\_Status  is zero |
| Technical  Safety  Requirement  05 | Memory test shall be conducted  at startup of the EPS ECU to  check for any faults in memory | A | cycle | Memory test | LKA\_Error\_Status  is zero |

## Refinement of the System Architecture



## Allocation of Technical Safety Requirements to Architecture Elements

All technical safety requirements are allocated to the Electronic Power Steering ECU.

## Warning and Degradation Concept

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Degradation Mode** | **Trigger for Degradation Mode** | **Safe State invoked?** | **Driver Warning** |
| WDC-01 | Turn off Lane Departure Warning functionality | Malfunction\_01,  Malfunction\_02, | Yes | Lane Departure Warning Malfunction Warning on Car Display |
| WDC-02 | Turn off Lane Keeping Assistance  functionality | Malfunction\_03 | Yes | Lane Keeping Assistance Malfunction Warning on Car Display |