

Technical Safety Concept Lane Assistance

**Document Version: [Version]**

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



|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Editor | Description |
| 23.06.2018 | 1.0 | Malgorzata Plonka | Initial version |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# 

# 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 the technical safety concept is to refine the functional safety requirements established in the functional safety concept into technical safety requirements.

These requirements are assigned to the system architecture. They are more concrete and go into details of the item’s technology as specified by ISO 26262.

# 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 | 50 ms | Turn off Lane Departure Warning |
| Functional  Safety  Requirement  01-02 | The lane keeping item shall ensure that the  lane departure oscillating torque frequency  is below *Max\_Torque\_Frequency* | C | 50 ms | Turn off Lane Departure Warning |
| 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 | 500 ms | Turn off Lane Keeping Assistant |

## Refined System Architecture from Functional Safety Concept



### Functional overview of architecture elements

|  |  |
| --- | --- |
| **Element** | **Description** |
| Camera Sensor | Captures road images and provide them to the  Camera Sensor ECU. |
| Camera Sensor ECU - Lane Sensing | Detects lane line positions from camera images. |
| Camera Sensor ECU - Torque request generator | Generates a torque request to the Electronic Power  Steering ECU. |
| Car Display | Shows warning to driver. |
| Car Display ECU - Lane Assistance On/Off Status | Indicates the status of the Lane Assistance functionality (On/Off.) |
| Car Display ECU - Lane Assistant Active/Inactive | Indicates if the Lane Assistance functionality is properly functioning (Active/Inactive.) |
| Car Display ECU - Lane Assistance malfunction warning | Indicates fault malfunction of Lane Assistance functionality. |
| Driver Steering Torque Sensor | Measures the torque applied to the steering wheel by the driver. |
| Electronic Power Steering (EPS) ECU - Driver Steering Torque | Processes input from Driver Steering Torque  Sensor. |
| EPS ECU - Normal Lane Assistance Functionality | Receives torque request from Camera Sensor ECU  and transfers it to Safety Lane Assistance  Functionality. |
| EPS ECU - Lane Departure Warning Safety Functionality | Ensures the torque amplitude is below *Max\_Torque\_Amplitude*  and torque frequency is below  *Max\_Torque\_Frequency*. |
| EPS ECU - Lane Keeping Assistant Safety Functionality | Ensures the Lane Keeping  Assistance functionality application is not activate more than *Max\_duration* time. |
| EPS ECU - Final Torque | Generates final torque from torque requests received from LDW and LKA safety. |
| 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 ‘LDW\_Torque\_Request’ sent  to the ‘Final electronic power  steering Torque’ component is  below *Max\_Torque\_Amplitude*. | C | 50 ms | LDW Safety | LDW torque set to zero. |
| Technical  Safety  Requirement  02 | When the LDW is deactivated, the ‘LDW Safety’ software module shall send a signal to the  Car Display ECU to turn on a warning signal. | C | 50 ms | LDW Safety | LDW torque set to zero. |
| Technical  Safety  Requirement  03 | When the 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 set 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 | Data Transmission Integrity Check | N/A |
| 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 torque set 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 component shall  ensure that the frequencyof  ‘LDW\_Torque\_Request’ sent to the  ‘Final electronic power steering  Torque’ component is below  *Max\_Torque\_Frequency*. | C | 50 ms | LDW Safety | LDW torque set to zero. |
| Technical  Safety  Requirement  02 | When 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 set to zero. |
| Technical  Safety  Requirement  03 | When 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 set 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 | Data  Transmission  Integrity  Check | N/A |
| 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 torque set to zero. |

**Lane Departure Warning (LDW) Verification and Validation Acceptance Criteria:**

**[OPTIONAL]**

**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 the active duration  time is below *Max\_Duration*. | B | 500 ms | LKA safety | LAK torque set to zero. |
| Technical  Safety  Requirement  02 | When failure is detected  by the LKA function, it shall  deactivate the LKA feature and  the “LKA\_Torque\_Request” shall  be set to zero. | B | 500 ms | LKA safety | LAK torque set to zero. |
| Technical  Safety  Requirement  03 | When 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 | LAK torque set to zero. |
| 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 | N/A |
| Technical  Safety  Requirement  05 | Memory test shall be conducted  at start up of the EPS ECU to  check for any faults in memory | A | 500 ms | Memory Test | LAK torque set to zero. |

**Lane Keeping Assistance (LKA) Verification and Validation Acceptance Criteria:**

**[OPTIONAL]**

Refinement of the System Architecture

****

## Allocation of Technical Safety Requirements to Architecture Elements

As shown in the tables above, all technical safety requirements are allocated to the Electronic Power Steering ECU.

## Power Steering ECU.Warning and Degradation Concept

The technical safety requirements have not changed how functionality will be degraded or what

the warning will be. Thus, the warning and degradation concept is the same for the technical

safety requirements as for the functional safety requirements

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Degradation Mode** | **Trigger for Degradation Mode** | **Safe State invoked ?** | **Driver Warning** |
| WDC-01 | Turn off LDW  functionality | Malfunction\_01,  Malfunction\_02 | YES | LDW  Malfunction  Warning on  Car Display |
| WDC-02 | Turn off LKA  functionality | Malfunction\_03 | YES | LKA  Malfunction  Warning on  Car Display |