

Technical Safety Concept Lane Assistance

**Document Version: 1.0**

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



# Document history

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Editor | Description |
| 19.02.2018 | 1.0 | VIvanov | Draft 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 technical safety concept is more concrete than the functional safety concept and gets into the details of the item's technology.

The technical safety requirements need to be determined for each of item’s systems.

The technical safety concept involves:

* Turning functional safety requirements into technical safety requirements
* Allocating technical safety requirements to the system architecture

# 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 | Lane departure oscillating torque amplitude is below Max\_Torque\_Amplitude |
| 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 | Lane departure oscillating torque frequency is below Max\_Torque\_Frequency |
| 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 | Lane Keeping Assistance is deactivated |

## Refined System Architecture from Functional Safety Concept



### 

### Functional overview of architecture elements

|  |  |
| --- | --- |
| **Element** | **Description** |
| Camera Sensor | Image Processing and providing images to Camera Sensor ECU |
| Camera Sensor ECU - Lane Sensing | Object perception and recognition, detection of lane boundaries |
| Camera Sensor ECU - Torque request generator | Generation of torque request to the Electronic Power Steering ECU |
| Car Display | Displaying of Lane Assistant item state, activity and warning messaged to the driver |
| Car Display ECU - Lane Assistance On/Off Status | Indicating Lane Assistance On/Off Status |
| Car Display ECU - Lane Assistant Active/Inactive | Indicating Lane Assistance Active/Inactive Status |
| Car Display ECU - Lane Assistance malfunction warning | Indicating Lane Assistance malfunction warnings |
| Driver Steering Torque Sensor | Measuring of torque applied to the steering wheel by the driver to Electronic Power Steering ECU |
| Electronic Power Steering (EPS) ECU - Driver Steering Torque | Processing of input from Driver Steering Torque Sensor |
| EPS ECU - Normal Lane Assistance Functionality | Receiving the torque request from Camera Sensor ECU and sending to Safety Lane Assistance Functionality |
| EPS ECU - Lane Departure Warning Safety Functionality | Checking for malfunction of Lane Departure Warning Functionality and sending torque request to final torque output or malfunction warning to Car Display ECU - Lane Assistance malfunction warning |
| EPS ECU - Lane Keeping Assistant Safety Functionality | Checking for malfunction of Lane Keeping Assistant Functionality and sending torque request to final torque output or malfunction warning to Car Display ECU - Lane Assistance malfunction warning |
| EPS ECU - Final Torque | Evaluating of final torque from Lane Departure Warning Safety Functionality and Lane Keeping Assistant Safety Functionality requests |
| Motor | Receiving torque request from Electronic Power Steering ECU and applying 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 | 50ms | LDW Safety | LDW torque output is set to zero |
| Technical  Safety  Requirement  02 | 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 torque output is set to zero |
| Technical  Safety  Requirement  03 | 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 torque output is set to zero |
| Technical  Safety  Requirement  04 | The validity and integrity of the data transmission for ‘LDW\_Torque\_Request’ signal shall be ensured | C | 50ms | 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 errors in memory | A | Ignition cycle | Safety Startup Memory Test | LDW torque output is set to zero |

Functional Safety Requirement 01-02 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 | 50ms | LDW Safety | LDW torque output is set to zero |
| Technical  Safety  Requirement  02 | 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 torque output is set to zero |
| Technical  Safety  Requirement  03 | 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 torque output is set to zero |
| Technical  Safety  Requirement  04 | The validity and integrity of the data transmission for ‘LDW\_Torque\_Request’ signal shall be ensured | C | 50ms | 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 errors in memory | A | Ignition cycle | Safety Startup Memory Test | LDW torque output is set to zero |

**Lane Keeping Assistance (LKA) Requirements:**

Functional Safety Requirement 02-01 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  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 ‘LKA\_Torque\_Request’ is sent to ‘Final electronic power steering Torque’ for less than Max\_Duration | C | 500ms | LKA Safety | LKA torque output is set to zero |
| Technical  Safety  Requirement  02 | As soon as a failure is detected by the LKA function, it shall deactivate the LKA feature and the LKA\_Torque\_Request shall be set to zero | C | 500ms | LKA Safety | LKA torque output is set to zero |
| Technical  Safety  Requirement  03 | 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 | C | 500ms | LKA Safety | LKA torque output is set to zero |
| Technical  Safety  Requirement  04 | The validity and integrity of the data transmission for ‘LKA\_Torque\_Request’ signal shall be ensured | C | 500ms | 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 errors in memory | A | Ignition cycle | Safety Startup Memory Test | LKA torque output is set 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 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  01-01-03 | 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  01-01-04 | 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 startup of the EPS ECU to check for any errors 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 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  01-02-03 | 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  01-02-04 | 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 startup of the EPS ECU to check for any errors in memory | **X** |  |  |
| Technical  Safety  Requirement  02-01-01 | The LKA safety component shall ensure the ‘LKA\_Torque\_Request’ is sent to ‘Final electronic power steering Torque’ for less than Max\_Duration | **X** |  |  |
| Technical  Safety  Requirement  02-01-02 | As soon as a failure is detected by the LKA function, it shall deactivate the LKA feature and the LKA\_Torque\_Request shall be set to zero | **X** |  |  |
| Technical  Safety  Requirement  02-01-03 | 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  02-01-04 | 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 startup of the EPS ECU to check for any errors in memory | **X** |  |  |

## 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 | Yes | Lane Assistance malfunction Warning |
| WDC-02 | Turn off Lane Departure Warning functionality | Malfunction\_02 | Yes | Lane Assistance malfunction Warning |
| WDC-03 | Turn off Lane Keeping Assistance functionality | Malfunction\_03 | Yes | Lane Assistance malfunction Warning |
| WDC-04 | Turn off Lane Keeping Assistance functionality | Malfunction\_04 | Yes | Lane Assistance malfunction Warning |
| WDC-05 | Turn off Lane Departure Warning functionality | Malfunction\_05 | Yes | Lane Assistance malfunction Warning |