

Technical Safety Concept Lane Assistance

**Document Version: 1.0**

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



# Document history

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Editor | Description |
| 2018-03-04 | 1.0 | Maximilian Wenger | Initial version |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# Table of Contents

[Document history 2](#_Toc507934015)

[Table of Contents 2](#_Toc507934016)

[Purpose of the Technical Safety Concept 3](#_Toc507934017)

[Inputs to the Technical Safety Concept 3](#_Toc507934018)

[Functional Safety Requirements 3](#_Toc507934019)

[Refined System Architecture from Functional Safety Concept 4](#_Toc507934020)

[Functional overview of architecture elements 4](#_Toc507934021)

[Technical Safety Concept 5](#_Toc507934022)

[Technical Safety Requirements 5](#_Toc507934023)

[Refinement of the System Architecture 10](#_Toc507934024)

[Allocation of Technical Safety Requirements to Architecture Elements 10](#_Toc507934025)

[Warning and Degradation Concept 11](#_Toc507934026)

# Purpose of the Technical Safety Concept

The purpose of this technical safety concept is to translate the functional safety requirements into technical safety requirements that have to be implemented during the development of the item.

# 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 is below Max\_Torque\_Amplitude. | C | 50ms | LA off (torque zero) |
| Functional  Safety  Requirement  01-02 | The electronic power steering ECU shall ensure that the oscillating torque frequency is below Max\_Torque\_Frequency. | C | 50ms | LA off (torque zero) |
| 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 | LA off (torque zero) |

## Refined System Architecture from Functional Safety Concept



### Functional overview of architecture elements

|  |  |
| --- | --- |
| **Element** | **Description** |
| Camera Sensor | Provide images of the road to the ECU. |
| Camera Sensor ECU - Lane Sensing | Detect lane markings and position of vehicle in relation to them. |
| Camera Sensor ECU - Torque request generator | Calculate the torque required to steer the vehicle back into the middle of the ego lane. |
| Car Display | Show visual information to the driver (e.g. warning light). |
| Car Display ECU - Lane Assistance On/Off Status | Display the LA system on/off status. |
| Car Display ECU - Lane Assistant Active/Inactive | Display the LA activity system status received from the EPS ECU. |
| Car Display ECU - Lane Assistance malfunction warning | Display the LA system malfunction warning received from the EPS ECU or Camera ECU. |
| Driver Steering Torque Sensor | Measure the torque applied to the steering wheel by the driver. |
| Electronic Power Steering (EPS) ECU - Driver Steering Torque | Calculate the steering torque the motor should apply to the steering wheel from the camera and torque sensor inputs. |
| EPS ECU - Normal Lane Assistance Functionality | Translate and integrate torque requests from the camera. |
| EPS ECU - Lane Departure Warning Safety Functionality | Ensure that the torque amplitude and frequency stay within the lower and upper boundaries. |
| EPS ECU - Lane Keeping Assistant Safety Functionality | Ensure that the LKA torque amplitude stays within the boundary. |
| EPS ECU - Final Torque | Ensure that the torque amplitude and frequency stay within the lower and upper boundaries. |
| Motor | Apply 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 | 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 functionality | LA off (torque zero) |
| 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 functionality | LA off (torque 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 | 50 ms | LDW Safety functionality | LA off (torque 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 | LA off (torque 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 | LA off (torque 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 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 functionality | LA off (torque zero) |
| 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 functionality | LA off (torque 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 | 50 ms | LDW Safety functionality | LA off (torque 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 | LA off (torque 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 | LA off (torque zero) |

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

**--**

**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 'LKA\_Torque\_Request' sent to the 'Final electronic power steering Torque' component is different from zero for only Max\_Duration. | B | 500 ms | LKA Safety functionality | LA off (torque zero) |
| 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 functionality | LA off (torque zero) |
| Technical  Safety  Requirement  03 | 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. | B | 500 ms | LKA Safety functionality | LA off (torque 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 | LA off (torque 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 | LA off (torque zero) |

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

**--**

## Refinement of the System Architecture



## Allocation of Technical Safety Requirements to Architecture Elements

See the technical requirements tables. All technical safety requirements discussed in this document are within the EPS ECU.

## Warning and Degradation Concept

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Degradation Mode** | **Trigger for Degradation Mode** | **Safe State invoked?** | **Driver Warning** |
| WDC-01 | Turn LA off (additional torque set to zero) | Malfunction\_01  Malfunction\_02  Malfunction\_04  Malfunction\_05 | Yes | LA malfunction warning light |
| WDC-02 | Turn LA off (additional torque set to zero) | Malfunction\_03 | Yes | LA malfunction warning light |
| WDC-03 | Turn LA off (additional torque set to zero) | Malfunction\_06 | Yes | LA malfunction warning light |