

Technical Safety Concept Lane Assistance

**Document Version: [Version]**

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



# Document history

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Editor | Description |
| 9/23/2017 | 1.0 | Martin Pfeifle | First draft of technical safety concept |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# 

# Table of Contents

Contents

[Document history 2](#_Toc494215127)

[Table of Contents 2](#_Toc494215128)

[Purpose of the Technical Safety Concept 3](#_Toc494215129)

[Inputs to the Technical Safety Concept 3](#_Toc494215130)

[Functional Safety Requirements 3](#_Toc494215131)

[Refined System Architecture from Functional Safety Concept 3](#_Toc494215132)

[Functional overview of architecture elements 4](#_Toc494215133)

[Technical Safety Concept 5](#_Toc494215134)

[Technical Safety Requirements 5](#_Toc494215135)

[Refinement of the System Architecture 10](#_Toc494215136)

[Allocation of Technical Safety Requirements to Architecture Elements 10](#_Toc494215137)

[Warning and Degradation Concept 10](#_Toc494215138)

# Purpose of the Technical Safety Concept

The technical safety concept defines how the subsystems interact at a message level and describes how the ECUs communicate with each other.

# 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 | LDW will set the oscillating torque to 0 |
| Functional  Safety  Requirement  01-02 | The lane keeping item shall ensure that the lane departure oscillating torque amplitude is below Max\_Torque\_Frequency | C | 50 ms | Lane keeping item output torque = 0 |
| 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 | Lane keeping item output torque = 0 |

## Refined System Architecture from Functional Safety Concept



### 

### Functional overview of architecture elements

|  |  |
| --- | --- |
| **Element** | **Description** |
| Camera Sensor | A sensor that outputs a front-facing image |
| Camera Sensor ECU - Lane Sensing | A control module software feature that processes an image and identifies the lane markings for the current lane in the car coordinate system |
| Camera Sensor ECU - Torque request generator | A control module software feature that processes the vehicles position and trajectory with respect to the position and trajectory of the ego lane, and issues a torque request to alert the driver or correct the vehicle trajectory in case the car’s trajectory deviates from the center line of the ego lane. |
| Car Display | An actuator that displays information and messages to the driver via warning lamps and LCD display |
| Car Display ECU - Lane Assistance On/Off Status | A control module that displays whether the lane assistance feature is currently on or off |
| Car Display ECU - Lane Assistant Active/Inactive | A control module feature that displays whether the lane assistance feature is currently active or inactive |
| Car Display ECU - Lane Assistance malfunction warning | A control module feature that displays a warning message if the lane assistance feature has experienced a malfunction |
| Driver Steering Torque Sensor | A sensor that outputs the torque that the driver is applying to the steering wheel |
| Electronic Power Steering (EPS) ECU - Driver Steering Torque | A control module that calculates the amount of steering torque being applied by the driver via the steering wheel |
| EPS ECU - Normal Lane Assistance Functionality | A control module that calculates the nominal amount of torque to apply, based on the driver steering torque and torque request from the camera sensor ECU |
| EPS ECU - Lane Departure Warning Safety Functionality | A control module that monitors the frequency and amplitude of the torque request for the LDW feature and limits both to a maximum; moreover, the feature will indicate a malfunction if the limits are exceeded |
| EPS ECU - Lane Keeping Assistant Safety Functionality | A control module that monitors the duration of the torque request for the LKA feature and limits it to a maximum; moreover, the feature will indicate a malfunction if the limit is exceeded |
| EPS ECU - Final Torque | A control module that applies the final torque |
| Motor | An actuator that adds torque to the steering |

# 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 | LDW\_Torque\_Request = 0 |
| 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 | 50ms | Electronic Power Steering ECU - LDW Safety Functionality | LDW\_Torque\_Request = 0 |
| 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 | Electronic Power Steering ECU - LDW Safety Functionality | LDW\_Torque\_Request = 0 |
| Technical  Safety  Requirement  04 | The validity and integrity of the data transmission for 'LDW\_Torque\_Request' signal shall be ensured. | C | 50ms | Electronic Power Steering ECU – Data transmission integrity check | LDW\_Torque\_Request = 0 |
| 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 | Electronic Power Steering ECU – Safety Startup | LDW\_Torque\_Request = 0 |

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 frequency of the 'LDW\_Torque\_Request' sent to the 'Final electronic power steering Torque' component is below 'Max\_Torque\_Frequency. | C | 50ms | Electronic Power Steering ECU - LDW Safety Functionality | LDW\_Torque\_Request = 0 |
| 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 | 50ms | Electronic Power Steering ECU - LDW Safety Functionality | LDW\_Torque\_Request = 0 |
| 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 | Electronic Power Steering ECU - LDW Safety Functionality | LDW\_Torque\_Request = 0 |
| Technical  Safety  Requirement  04 | The validity and integrity of the data transmission for 'LDW\_Torque\_Request' signal shall be ensured. | C | 50ms | Electronic Power Steering ECU – Data transmission integrity check | LDW\_Torque\_Request = 0 |
| 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 | Electronic Power Steering ECU – Safety Startup | LDW\_Torque\_Request = 0 |

**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 greater than 0 for no more than 'Max\_Duration. | B | 500ms | Electronic Power Steering ECU - LKA Safety Functionality | LKA\_Torque\_Request = 0 |
| 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 | 500ms | Electronic Power Steering ECU - LKA Safety Functionality | LKA\_Torque\_Request = 0 |
| 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 | 500ms | Electronic Power Steering ECU - LKA Safety Functionality | LKA\_Torque\_Request = 0 |
| Technical  Safety  Requirement  04 | The validity and integrity of the data transmission for 'LKA\_Torque\_Request' signal shall be ensured. | B | 500ms | Electronic Power Steering ECU – Data transmission integrity check | LKA\_Torque\_Request = 0 |
| 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 | Electronic Power Steering ECU – Safety Startup | LKA\_Torque\_Request = 0 |

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

**[OPTIONAL: For each technical safety requirement, identify both the verification and validation acceptance criteria. “Validation” asks whether or not you chose the appropriate parameters. “Verification” involves testing to make sure the vehicle behaves as expected when the parameter value is crossed. There is not necessarily one right answer. Look at your verification and validation acceptance criteria from the functional safety concept for inspiration.]**

## 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 | Functionality is turned off | Malfunction\_01 | Yes,  immediately | audible warning signal combined with a pop-up message on instrument cluster |
| WDC-02 | Functionality is turned off | Malfunction\_02 | Yes,  immediately | audible warning signal combined with a pop-up message on instrument cluster |