

Technical Safety Concept Lane Assistance

**Document Version: 1.0**

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



# Document history

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Editor | Description |
| 26.03.2018 | 0.1 | Stefan Cyliax | Initial version for functional safety project |
| 01.04.2018 | 1.0 | Stefan Cyliax | First RC |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# Table of Contents

Contents

[Document history 2](#_Toc510360241)

[Table of Contents 2](#_Toc510360242)

[Purpose of the Technical Safety Concept 2](#_Toc510360243)

[Inputs to the Technical Safety Concept 3](#_Toc510360244)

[Functional Safety Requirements 3](#_Toc510360245)

[Refined System Architecture from Functional Safety Concept 3](#_Toc510360246)

[Functional overview of architecture elements 4](#_Toc510360247)

[Technical Safety Concept 5](#_Toc510360248)

[Technical Safety Requirements 5](#_Toc510360249)

[Refinement of the System Architecture 10](#_Toc510360250)

[Allocation of Technical Safety Requirements to Architecture Elements 10](#_Toc510360251)

[Warning and Degradation Concept 11](#_Toc510360252)

# Purpose of the Technical Safety Concept

The Purpose of the Technical Safety Concept is to derive technical requirements from the Functional Safety requirements by getting into more detail about the items technology. In contrast to the Functional Safety Concept, it is part of the product development phase.

# 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 lane departure oscillation torque amplitude is below Max\_Torque\_Amplitude. | C | 50 ms | Gradually reduce steering torque to zero |
| Functional  Safety  Requirement  01-02 | The Electronic Power Steering ECU shall ensure that the lane departure oscillation torque frequency is below Max\_Torque\_Frequency. | C | 50 ms | Gradually reduce steering torque to 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 | 500 ms | Gradually reduce steering torque to zero |

## Refined System Architecture from Functional Safety Concept



### 

### Functional overview of architecture elements

|  |  |
| --- | --- |
| **Element** | **Description** |
| Camera Sensor | Provides the Camera Display ECU with images of the street in front of the vehicle. |
| Camera Sensor ECU - Lane Sensing | Detects lane line markers on the camera image and calculates the relative vehicle position to it. |
| Camera Sensor ECU - Torque request generator | Takes position of the lane line markers and the relative position of the vehicle and creates a correction torque. |
| Car Display | Displays various information to the driver. |
| Car Display ECU - Lane Assistance On/Off Status | Provides the Car Display with information of the On/Off state of the Lane Assistance system. |
| Car Display ECU - Lane Assistant Active/Inactive | Provides the Car Display with information of the Active/Inactive state of the Lane Assistance system. |
| Car Display ECU - Lane Assistance malfunction warning | Provides the Car Display with information of a possible malfunction of the Lane Assistance system. |
| Driver Steering Torque Sensor | Senses the current steering torque of the driver. |
| Electronic Power Steering (EPS) ECU - Driver Steering Torque | Reads the current steering torque of the driver from the Driver Steering Torque Sensor. |
| EPS ECU - Normal Lane Assistance Functionality | Implements both Lane Assistance functions. Receives torque requests from Camera Sensor ECU and generates steering torque. |
| EPS ECU - Lane Departure Warning Safety Functionality | Safety module to ensure that torque amplitude and frequency are below maximum. |
| EPS ECU - Lane Keeping Assistant Safety Functionality | Safety module to ensure that LKA is not activated longer than maximum duration time. |
| EPS ECU - Final Torque | Combine torque requests from LKA, LDW and Driver Steering Torque to the final torque to be send to the motor. |
| Motor | Applies the correct torque to the steering wheel of the vehicle. |

# 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 | 50 ms | LDW\_Safety | 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 | 50 ms | LDW\_Safety | 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 | 50 ms | 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 | 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 oscillating torque frequency of the 'LDW\_Torque\_Request' sent to the 'Final electronic power steering Torque' component is below 'Max\_Torque\_Frequency. | 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 | 50 ms | LDW\_Safety | 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 | 50 ms | LDW\_Safety | 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 | 50 ms | 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 | Safety Startup | LDW\_Torque\_Request = 0 |

**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 duration of the 'LKA\_Torque\_Request' sent to the 'Final electronic power steering Torque' is applied for only ‘Max\_Duration’. | B | 500 ms | LKA\_Safety | 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 | 500 ms | LKA\_Safety | 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 | 500 ms | LKA\_Safety | 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 | 500 ms | 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 | Safety Startup | LKA\_Torque\_Request = 0 |

## 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 | LDW\_Torque\_Request = 0 | 'LDW\_Torque\_Request' >= 'Max\_Torque\_Amplitude.  OR  'LDW\_Torque\_Request' >= 'Max\_Torque\_Frequency | Yes | Warning on car display |
| WDC-02 | LKA\_Torque\_Request = 0 | ‘Max\_Duration’ time limit is exceeded. | Yes | Warning on car display |