

Technical Safety Concept Lane Assistance

**Document Version: 1.0**

**Version 1.0, Released on 2018-05-22**



# Document history

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Editor | Description |
| 2018-05-22 | 1.0 | Navin Rawther | Initial Draft |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# 

# 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

A technical Safety Concept defines requirements and allocates them to the system architecture. The new requirements are more concrete and gets into the item’s technology.

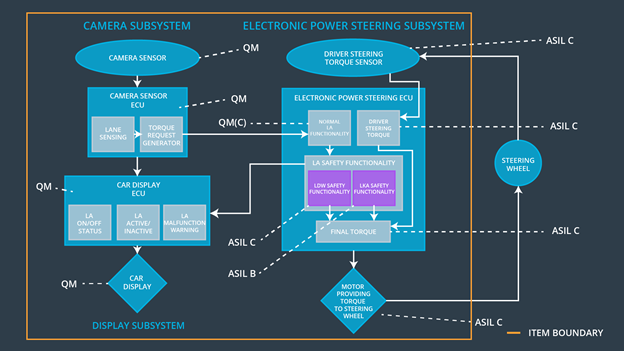
# Inputs to the Technical Safety Concept

## 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 warning oscillating torque amplitude is below Max\_Torque\_Amplitude | C | 50ms | Lane departure warning oscillating amplitude is below Max\_Torque\_Amplitude |
| Functional  Safety  Requirement  01-02 | The electronic power steering ECU shall ensure that the lane departure warning oscillating torque frequeny is below Max\_Torque\_Frequency | C | 50ms | Lane departure warning 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 for only Max\_Duration | B | 500ms | Lane keeping assistance torque is 0 after Max\_Duration |

## Refined System Architecture from Functional Safety Concept

The figure below shows the refined system architecture with the ASIL values:



### Functional overview of architecture elements

|  |  |
| --- | --- |
| **Element** | **Description** |
| Camera Sensor | Reads images of the road |
| Camera Sensor ECU - Lane Sensing | Computes and senses where the lane markings are on the road |
| Camera Sensor ECU - Torque request generator | Generates the torque request in case of vehicle reaching edge of a lane and sends it to the Electronic Power Steering Subsystem |
| Car Display | The display that contains the signals of the lane assistance item for the driver |
| Car Display ECU - Lane Assistance On/Off Status | Switches the signal corresponding to Lane Assistance to On/Off |
| Car Display ECU - Lane Assistant Active/Inactive | Decides whether the Lane Assistance system is active or not |
| Car Display ECU - Lane Assistance malfunction warning | Provides warning if the Lane Assistance system is malfunctioning by obtaining input from Electronic Power Steering Subsystem |
| Driver Steering Torque Sensor | Detects how much the steering wheel is already turned |
| Electronic Power Steering (EPS) ECU - Driver Steering Torque | Senses how much the driver is turning the steering wheel |
| EPS ECU - Normal Lane Assistance Functionality | Receives vibrational torque request from camera subsystem and computes the torque required to get back to the lane center |
| EPS ECU - Lane Departure Warning Safety Functionality | Limits the amplitude and frequency torque provided by the Normal Lane Assistance Functionality |
| EPS ECU - Lane Keeping Assistant Safety Functionality | Switches the Lane Keeping Assistance output torque to 0 when exceeds the Max\_Duration |
| EPS ECU - Final Torque | Computes the final torque from the Driver Steering Torque subsystem and the Lane Assistance Safety Functionality |
| Motor | Provides torque to the steering wheel to obtain the required 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 component is below Max\_Torque\_Amplitude | C | 50ms | LDW safety block | LDW\_Torque\_Request Amplitude shall be set to zero |
| Technical  Safety  Requirement  02 | The validity and integrity of the data transmission for LDW\_Torque\_Request signal shall be ensured | C | 50ms | Data Transmission Integrity Check | LDW\_Torque\_Request Amplitude shall be set to zero |
| Technical  Safety  Requirement  03 | As soon as a failure is detected by the LDW function, it shall deactivate the feature and the LDW\_Torque\_Request shall be set to zero | C | 50ms | LDW safety block | LDW\_Torque\_Request Amplitude shall be set to zero |
| Technical  Safety  Requirement  04 | As soon as the LDW function deactivates the LDW feature, the LDW safety feature block shall send a signal to the car display ECU to turn on a warning light | C | 50ms | LDW safety block | LDW\_Torque\_Request Amplitude shall be set to zero |
| Technical  Safety  Requirement  05 | Memory test shall be conducted at the startup of the EPS ECU to check for any faults in memory | A | ignition cycle | Safety Startup | LDW\_Torque\_Request Amplitude shall be 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 safety component shall ensure that the frequency of the LDW\_Torque\_Request sent to the Final electronic power steering component is below Max\_Torque\_Frequency | C | 50ms | LDW safety block | LDW\_Torque\_Request Frequency shall be set to zero |
| Technical  Safety  Requirement  02 | The validity and integrity of the data transmission for LDW\_Torque\_Request signal shall be ensured | C | 50ms | Data Transmission Integrity Check | LDW\_Torque\_Request Frequency shall be set to zero |
| Technical  Safety  Requirement  03 | As soon as a failure is detected by the LDW function, it shall deactivate the feature and the LDW\_Torque\_Request shall be set to zero | C | 50ms | LDW safety block | LDW\_Torque\_Request Frequency shall be set to zero |
| Technical  Safety  Requirement  04 | As soon as the LDW function deactivates the LDW feature, the LDW safety feature block shall send a signal to the car display ECU to turn on a warning light | C | 50ms | LDW safety block | LDW\_Torque\_Request Frequency shall be set to zero |
| Technical  Safety  Requirement  05 | Memory test shall be conducted at the startup of the EPS ECU to check for any faults in memory | A | ignition cycle | Safety Startup | LDW\_Torque\_Request Frequency shall be set to zero |

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

Functional Safety Requirement 02-1 with its associated system elements

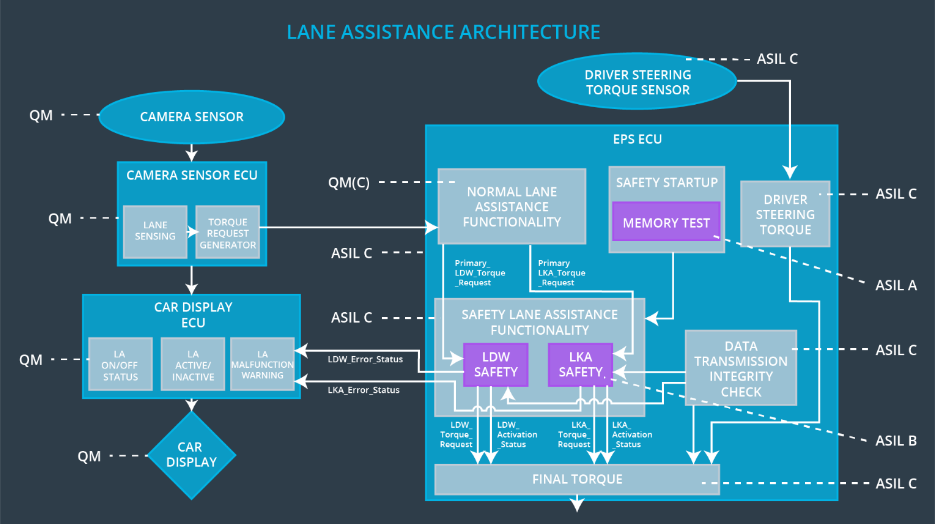
(derived in the functional safety concept)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **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 is sent to the Final electronic power steering component for only Max\_Duration | B | 500ms | LKA safety block | LKA\_Torque\_Request is 0 after Max\_Duration |
| Technical  Safety  Requirement  02 | The validity and integrity of the data transmission for LKA\_Torque\_Request signal shall be ensured | B | 500ms | Data Transmission Integrity Check | LKA\_Torque\_Request is 0 after Max\_Duration |
| Technical  Safety  Requirement  03 | As soon as a failure is detected by the LKA function, it shall deactivate the feature and the LKA \_Torque\_Request shall be set to zero | B | 500ms | LKA safety block | LKA\_Torque\_Request is 0 after Max\_Duration |
| Technical  Safety  Requirement  04 | As soon as the LKA function deactivates the LKA feature, the LKA safety feature block shall send a signal to the car display ECU to turn on a warning light | B | 500ms | LKA safety block | LKA\_Torque\_Request is 0 after Max\_Duration |
| Technical  Safety  Requirement  05 | Memory test shall be conducted at the startup of the EPS ECU to check for any faults in memory | A | ignition cycle | Safety Startup | LKA\_Torque\_Request is 0 after Max\_Duration |

## 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 | Lane Departure Warning functionality is turned off | Malfunction\_01, Malfunction\_02 | Yes | Lane Assistance Warning light in driver dashboard turned on |
| WDC-02 | Lane Assistance function turned off | Malfunction\_03 | Yes | Lane Assistance Warning light in driver dashboard turned on |