

Technical Safety Concept Lane Assistance

**Document Version: [Version]**

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



# Document history

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Editor | Description |
| 27.02.2020 | 1.0 | Uwe Ehmann | Initial Document |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# 

# 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 similar to the functional safety concept. New requirements are defined and allocated to the system architecture. The technical safety requirements are more concrete and get more into details of the item technology.

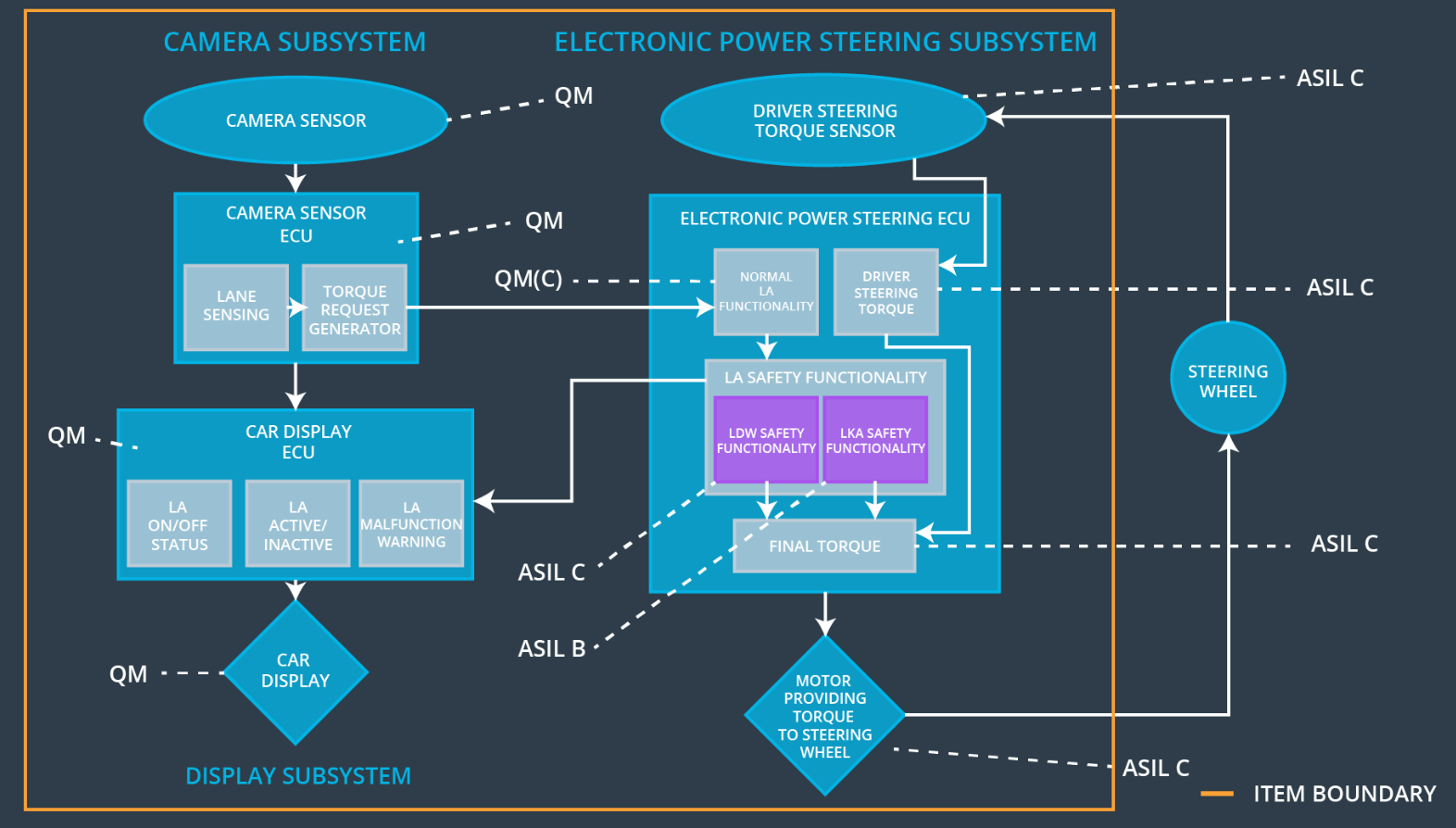
# Inputs to the Technical Safety Concept

## Functional Safety Requirements

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Functional Safety Requirement** | **ASIL** | **Fault Tolerant Time Interval** | **Safe State** |
| Functional  Safety  Requirement  01-01 | The lane keeping item shall ensure that the lane departure oscillating torque amplitude is below MAX\_TORQUE\_AMPLITUDE. | C | 50 ms | LDW torque request amplitude is set to zero. |
| Functional  Safety  Requirement  01-02 | The lane keeping item shall ensure that the lane departure oscillating torque frequency is below MAX\_TORQUE\_FREQUENCY. | C | 50 ms | LDW torque request frequency is set 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 | LKA torque is set to zero |

## 

## Refined System Architecture from Functional Safety Concept



### 

### Functional overview of architecture elements

|  |  |
| --- | --- |
| **Element** | **Description** |
| Camera Sensor | Provides environment images to the camera ECU. |
| Camera Sensor ECU - Lane Sensing | Detects lane lines from camera images |
| Camera Sensor ECU - Torque request generator | Generates a torque request to the Electronic Power Steering ECU |
| Car Display | Displays a lane departure warning. |
| Car Display ECU - Lane Assistance On/Off Status | Shows the status of the lane assistance functionality. |
| Car Display ECU - Lane Assistant Active/Inactive | Shows whether the function is turned on or off. |
| Car Display ECU - Lane Assistance malfunction warning | Show whether the system has detected a malfunction of the function. |
| Driver Steering Torque Sensor | Measures the steering torque of the driver and provides it to the Electronic Power Steering ECU. |
| Electronic Power Steering (EPS) ECU - Driver Steering Torque | Takes signals from the sensor ECUs and derives a steering torque to be applied. |
| EPS ECU - Normal Lane Assistance Functionality | Receives signals from sensor ECU and derives a steering torque to be applied. |
| EPS ECU - Lane Departure Warning Safety Functionality | Limits the torque request from the normal lane assistance functionality to a defined value. Signals the car display ECU in case of malfunctioning. |
| EPS ECU - Lane Keeping Assistant Safety Functionality | Limits the time the LKA is available to the driver. Signals the car display ECU in case of malfunctioning. |
| EPS ECU - Final Torque | Computes the final torque that needs to be applied to the steering wheel |
| Motor | Physically applies the requested 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 | EPS ECU – LDW Safety | LDW Torque Request Frequen cy shall be set to 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 | EPS ECU – LDW Safety | LDW Torque Request Frequen cy shall be set to 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 | EPS ECU – LDW Safety | LDW Torque Request Frequen cy shall be set to 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 | LDW Torque Request Frequen cy shall be set to zero |
| Technical  Safety  Requirement  05 | Memory test shall be conducted at startup of the EPS ECU to check for any faults in memory. | C | Ignition cycle | Safety startup - Memory test | LDW Torque Request Frequen cy 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 Torque' component is below MAX\_TORQUE\_FREQUENCY. | C | 50 ms | EPS ECU – LKA Safety | LDW Torque Request Frequen cy 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 | 50 ms | EPS ECU – LKA Safety | LDW Torque Request Frequen cy shall be set to 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 | EPS ECU – LKA Safety | LDW Torque Request Frequen cy shall be set to zero |
| Technical  Safety  Requirement  04 | 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 | Data transmission integrity check | LDW Torque Request Frequen cy shall be set to zero |
| Technical  Safety  Requirement  05 | Memory test shall be conducted at startup of the EPS ECU to check for any faults in memory. | A | Ignition cycle | EPS ECU – LKA Safety | LDW Torque Request Frequen cy shall be set to zero |

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

Functional Safety Requirement 02-1 with its associated system elements

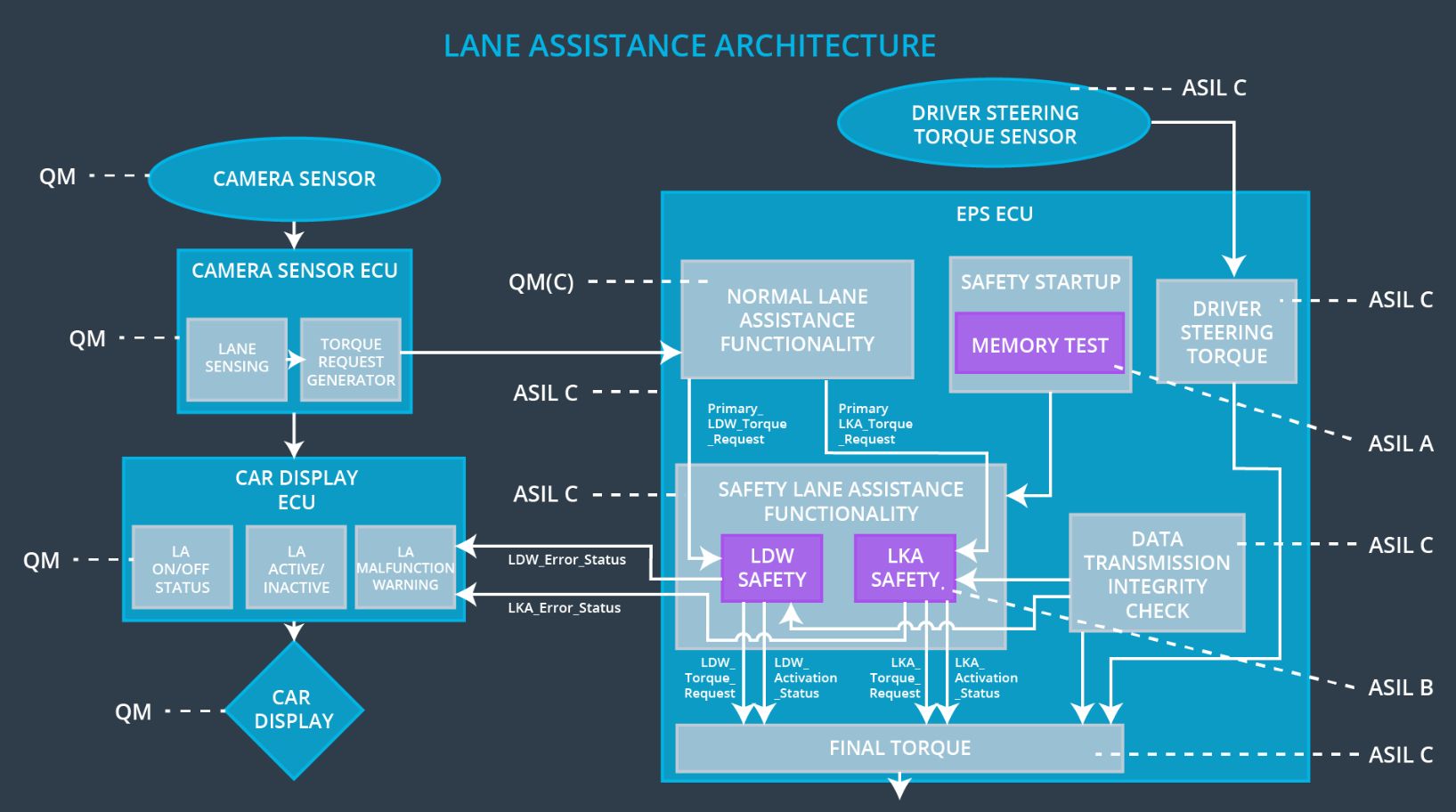
(derived in the functional safety concept)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **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 sent to the 'Final electronic power steering Torque' component is applied for only MAX\_DURATION. | B | 500 ms | EPS ECU – LKA Safety | LKA Torque Request shall be set to zero. |
| Technical  Safety  Requirement  02 | The validity and integrity of the data transmission for LKA\_TORQUE\_REQUEST signal shall be ensured. | B | 500 ms | EPS ECU – LKA Safety | LKA Torque Request shall be set to 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 | EPS ECU – LKA Safety | LKA Torque Request shall be set to zero. |
| Technical  Safety  Requirement  04 | 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 | Data transmission integrity check | LKA Torque Request shall be set to zero. |
| Technical  Safety  Requirement  05 | Memory test shall be conducted at startup of the EPS ECU to check for any faults in memory. | A | 500 ms | Safety startup - Memory test | LKA Torque Request shall be set to zero. |

## Refinement of the System Architecture



## Allocation of Technical Safety Requirements to Architecture Elements

All derived 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 | Turn off functionality | Malfunction\_01  Malfunction\_02 | Yes | The car display signals degraded functionality |
| WDC-02 | Turn off functionality | Malfunction\_03 | Yes | The car display signals degraded functionality |