

Technical Safety Concept Lane Assistance

**Document Version: 1.0**

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



# Document history

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Editor | Description |
| 24.05.2018 | 1.0 | Arindam Baidya | First attempt |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# 

# 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

ISO 26262 places the technical safety concept is part of the product development phase which also includes designing of hardware and software. This is because the technical safety concept is more concrete and gets into the details of the item's technology. The purpose of Technical Safety Concept is to refine the functional safety requirements established in the functional safety concept, into technical safety requirements. The technical safety concept involves:

* Turning functional safety requirements into technical safety requirements
* Allocating technical safety requirements to the system architecture

# 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 | 50ms | Lane Assistant  functionality off |
| Functional  Safety  Requirement  01-02 | The lane keeping item shall ensure that the lane departure oscillating torque frequency is below Max\_Torque\_Frequency | C | 50ms | Lane Assistant  functionality off |
| Functional  Safety  Requirement  02-01 | The LKA function shall be deactivated when the camera sensor or any other sensor starts malfunctioning. | C | 10ms | LKA Function is deactivated |

## Refined System Architecture from Functional Safety Concept

### 

### Functional overview of architecture elements

|  |  |
| --- | --- |
| **Element** | **Description** |
| Camera Sensor | Captures images from the road and provide them to Camera Sensor ECU |
| Camera Sensor ECU - Lane Sensing | Detects lane lines from camera sensor images |
| Camera Sensor ECU - Torque request generator | Calculates the necessary torque to be requested to the Power Steering ECU |
| Car Display | Displays warning, feedback status to the driver |
| Car Display ECU - Lane Assistance On/Off Status | Indicates the status of Lane Assistance functionality |
| Car Display ECU - Lane Assistant Active/Inactive | Indicates if Lane Assistance functionality is properly functioning and is active at the moment |
| Car Display ECU - Lane Assistance malfunction warning | Indicates malfunction of Lane assistance functionality |
| Driver Steering Torque Sensor | Measures the driving torque intensity of the driver and send it to Electronic Power Steering ECU |
| Electronic Power Steering (EPS) ECU - Driver Steering Torque | Processes input from Driver’s Steering torque sensor |
| EPS ECU - Normal Lane Assistance Functionality | Receives torque request from Camera sensor ECU and transfers it to Lane Assistance Safety functionality. |
| EPS ECU - Lane Departure Warning Safety Functionality | Checks for malfunctions in Lane Departure Warning and translates torque request into final torque output |
| EPS ECU - Lane Keeping Assistant Safety Functionality | Checks for malfunctions in Lane Keep Assistance and translates torque request into final torque output |
| EPS ECU - Final Torque | Combines the torque requests from Lane Keep Assistance and Lane Departure Warning functionalities and sends them to the motor. |
| Motor | Applies the required 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 ‘LDW\_Torque\_Request’ sent to the ‘Final electronic power steering Torque’ component is below Max\_Torque\_Amplitude’. | C | 50ms | LDW Safety | LDW\_Activati on\_Status is zero |
| Technical  Safety  Requirement  02 | 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 | LDW Safety | LDW\_Activati on\_Status is zero |
| Technical  Safety  Requirement  03 | 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 | LDW Safety | LDW\_Activati on\_Status is zero |
| Technical  Safety  Requirement  04 | The validity and integrity of the data transmission for  ‘LDW\_Torque\_Request’ signal shall be ensured. | C | 50ms | Data Transmission Integrity check | NA |
| 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 | Memory Test | LDW\_Activati on\_Status is 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  ‘LDW\_Torque\_Request’ sent to the  ‘Final electronic power steering  Torque’ component is below  ‘Max\_Torque\_Frequency’. | C | 50ms | LDW Safety | LDW\_Activation\_Status is zero |
| Technical  Safety  Requirement  02 | 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 | LDW Safety | LDW\_Activation\_Status is zero |
| Technical  Safety  Requirement  03 | 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 | LDW Safety | LDW\_Activation\_Status is zero |
| Technical  Safety  Requirement  04 | The validity and integrity of the data transmission for LDW\_Torque\_Request’ signal shall be ensured. | C | 50ms | Data Transmission Integrity Check | LDW\_Activation\_Status is 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 | Memory Test | LDW\_Activation\_Status is zero |

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

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

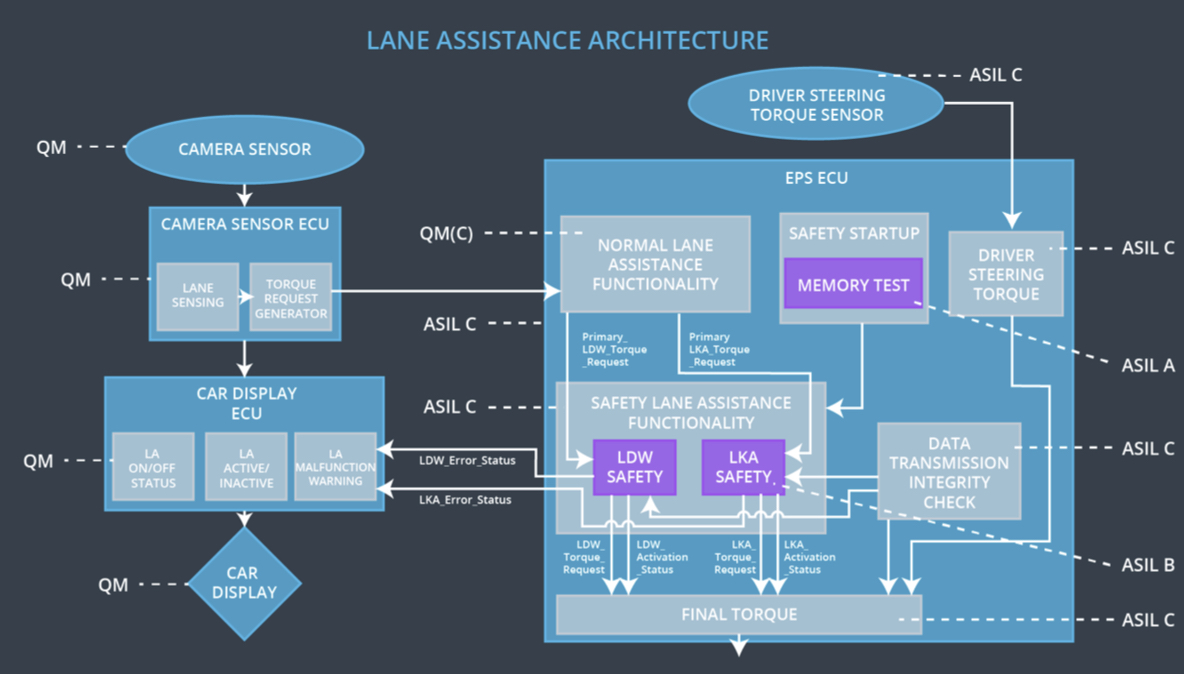
Functional Safety Requirement 02-1 with its associated system elements (derived in the functional safety concept)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **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 ‘LKA\_Torque\_Request’ is sent to the ‘Final electronic power steering Torque’ component for only ‘Max\_Duration’. | B | 500ms | LKA Safety | LKA\_Activation\_Status is zero |
| Technical  Safety  Requirement 02 | 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 | LKA Safety | LKA\_Activation\_Status is zero |
| Technical  Safety  Requirement 03 | 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 | LKA Safety | LKA\_Activation\_Status is zero |
| Technical  Safety  Requirement 04 | The validity and integrity of the  data transmission for  ‘LKA\_Torque\_Request’ signal shall be ensured. | B | 500ms | Data Transmission Integrity Check | LKA\_Activation\_Status is 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 | Memory Test | LKA\_Activation\_Status is zero |

## Refinement of the System Architecture

****

## Allocation of Technical Safety Requirements to Architecture Elements

All technical safety requirements were allocated to the Electronic Power Steering ECU. For the exact allocation within EPS ECU compare the technical requirement tables above.

## Warning and Degradation Concept

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Degradation Mode** | **Trigger for Degradation Mode** | **Safe State invoked?** | **Driver Warning** |
| WDC-01 | Turn off Lane Assistant functionality | Malfunction\_01 | Yes | Lane Departure Warning Malfunction Warning on Car Display |
| WDC-02 | Turn off Lane Assistant functionality | Malfunction\_02 | Yes | Lane Departure Warning Malfunction Warning on Car Display |
| WDC-03 | Turn off Lane Assistant functionality | Malfunction\_03 | Yes | Lane Keeping Assistance Malfunction Warning on Car Display |
| WDC-04 | Turn off Lane Assistant functionality | Malfunction\_04 | Yes | Lane Departure Warning Malfunction Warning on Car Display |
| WDC-05 | Turn off Lane Assistant functionality | Malfunction\_05 | Yes | Lane Keeping Assistance Malfunction Warning on Car Display |