Elektrobit

UDACITY

# Technical Safety Concept Lane Assistance

**Document Version: 1.2**
**Released on 2017-11-13**

# Document history

| Date | Version | Editor | Description |
|---|---|---|---|
| 2017-10-22 | 1.0 | Martin Hintz | Initial Version |
| 2017-10-30 | 1.1 | Martin Hintz | Layout and spelling corrections |
| 2017-11-13 | 1.2 | Martin Hintz | Updated ASILs in Technical Safety Requirement |
| | | | |
| | | | |

# Table of Contents

# Purpose of the Technical Safety Concept

This document provides a detailed overview of the technologies present in the Lane Assistance item as of the product development phase of its life cycle, presented at the system level.

# 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 | 50 ms | Turn Off System |
| Functional Safety Requirement 01-02 | The Electronic Power Steering ECU shall ensure that the lane departure warning oscillating torque amplitude is below Max_Torque_Frequency | C | 50 ms | Turn Off System |
| Functional Safety Requirement 02-01 | The electronic power steering ECU shall ensure that the lane keeping assistance torque is applied for only Max_Duration. | C | 500 ms | Turn Off System |

# Refined System Architecture from Functional Safety Concept

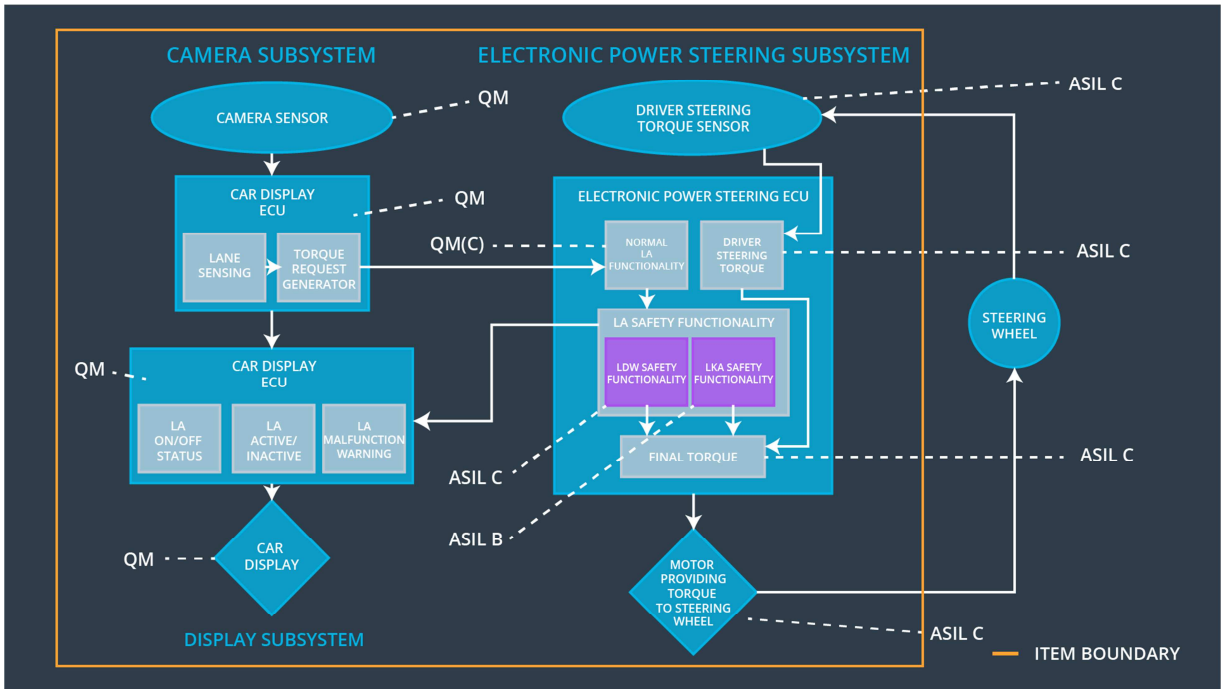


*Figure 1: Refined Architecture of the Lane Assistance System*

## Functional overview of architecture elements

| Element | Description |
|---|---|
| Camera Sensor | One or more sensor(s) located at the front of the vehicle that collect(s) visual data (image, video). |
| Camera Sensor ECU - Lane Sensing | A computer (electronic control unit) that interprets data collected by the camera sensor(s) and that detects lane lines and triggers audio-visual warnings on the car display ECU. |
| Camera Sensor ECU - Torque request generator | A computer that interprets detected lane lines to identify and calculate steering corrections that trigger the power steering ECU. |
| Car Display | A physical display in front of the vehicle's driver to provide audio-visual feedback. |

| | |
|---|---|
| Car Display ECU - Lane Assistance On/Off Status | A section in the car display to visualize the engagement status of the lane assistance item. |
| Car Display ECU - Lane Assistant Active/Inactive | A section in the car display to visualize the activation status of the lane assistance item. |
| Car Display ECU - Lane Assistance malfunction warning | A section in the car display to visualize the malfunction status of the Lane Assistance item. |
| Driver Steering Torque Sensor | A sensor that measures the torque applied to the steering wheel by the driver. |
| Electronic Power Steering (EPS) ECU - Driver Steering Torque | A computer attached to the power steering that converts torque applied by the driver to appropriate steering actions for the vehicle |
| EPS ECU - Normal Lane Assistance Functionality | A computer attached to the power steering that controls the torque applied to the steering wheel when the Lane Assistance is operating normally. |
| EPS ECU - Lane Departure Warning Safety Functionality | A computer attached to the power steering that triggers warnings on the car display ECU if the vehicle is leaving its ego lane. |
| EPS ECU - Lane Keeping Assistant Safety Functionality | A computer attached to the power steering that triggers warnings on the car display ECU if the LKA is exceeding limits. |
| EPS ECU - Final Torque | A computer attached to the power steering that ensures torque frequency and amplitude applied to the steering wheel are within limits. |
| Motor | An actuator responsible for applying 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 Functionality | Turn off system |
| 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 Functionality | Turn off system |

| | | | | | |
|---|---|---|---|---|---|
| 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 Functionality | Turn off system |
| Technical Safety Requirement 04 | The validity and integrity of the data transmission for 'LDW_Torque_Request' signal shall be ensured. | C | 50 ms | EPS ECU LDW Data Integrity Check | Turn off system |
| Technical Safety Requirement 05 | Memory test shall be conducted at startup of the EPS ECU to check for any faults in memory. | A | Time of ignition Cycle | EPS ECU Memory Test | Turn off system |

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 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 Functionality | Turn off system |
| 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 Functionality | Turn off system |
| 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 Functionality | Turn off system |
| Technical Safety Requirement 04 | The validity and integrity of the data transmission for 'LDW_Torque_Request' signal shall be ensured. | C | 50 ms | EPS ECU LDW Data Integrity Check | Turn off system |
| Technical Safety Requirement 05 | Memory test shall be conducted at startup of the EPS ECU to check for any faults in memory. | A | Time of ignition Cycle | EPS ECU Memory Test | Turn off system |

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

| ID | Validation Acceptance Criteria and Method | Verification Acceptance Criteria and Method |
|---|---|---|
| Technical Safety Requirement 01 | Measure various LDW_Torque_Request values sent to the EPS Final Torque component to ensure all values are within limits. | All measured LDW_Torque_Request values sent to the Final EPS Torque component are within limits. |
| Technical Safety Requirement 02 | Test audio-visual warning display by artificially inducing a deactivation of the LDW | An audio-visual warning is displayed when the LDW function deactivates the LDW feature. |
| Technical Safety Requirement 03 | Test zero torque is applied by artificially inducing a deactivation of the LDW | The applied torque is set to zero as soon as the LDW function deactivates the LDW feature. |
| Technical Safety Requirement 04 | Test reliability and throughput of data connection. | Data is transmitted to the ECU within a specified data rate |
| Technical Safety Requirement 05 | Test for memory faults. | No memory faults are present during operation. |

**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 lane keeping assistance torque is applied only for Max_Duration | B | 500 ms | EPS ECU LDW Safety Functionality | Turn off system |
| Technical Safety Requirement 02 | As soon as a failure is detected by the LKA function, it shall deactivate the LKA feature and the LKA_Error_Status shall update the car display to display a malfunction warning light. | B | 500 ms | EPS ECU LDW Safety Functionality | Turn off system |
| Technical Safety Requirement 03 | As soon as the LKA function deactivates the LKA feature, the LKA Safety software block shall send an LKA_Activation_Status to the car display ECU to set the item to inactive status. | B | 500 ms | EPS ECU LDW Safety Functionality | Turn off system |

| | | | | | |
|---|---|---|---|---|---|
| Technical Safety Requirement 04 | The validity and integrity of the data transmission for the LKA Safety software block shall be ensured. | B | 500 ms | EPS ECU LDW Data Integrity Check | Turn off system |
| Technical Safety Requirement 05 | Memory test shall be conducted at startup of the EPS ECU to check for any faults in memory. | A | Time of ignition cycle | EPS ECU Memory Test | Turn off system |

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

| ID | Validation Acceptance Criteria and Method | Verification Acceptance Criteria and Method |
|---|---|---|
| Technical Safety Requirement 01 | Measure various LKA_Torque_Request values sent to the EPS Final Torque component to ensure all values are within limits. | All measured LKA_Torque_Request values sent to the Final EPS Torque component are within limits. |
| Technical Safety Requirement 02 | Test audio-visual warning display by artificially inducing a deactivation of the LKA | An audio-visual warning is displayed when the LKA function deactivates the LKA feature. |
| Technical Safety Requirement 03 | Test zero torque is applied by artificially inducing a deactivation of the LKA | The applied torque is set to zero as soon as the LKA function deactivates the LKA feature. |
| Technical Safety Requirement 04 | Test reliability and throughput of data connection. | Data is transmitted to the ECU within a specified data rate |
| Technical Safety Requirement 05 | Test for memory faults. | No memory faults are present during operation. |

## Refinement of the System Architecture

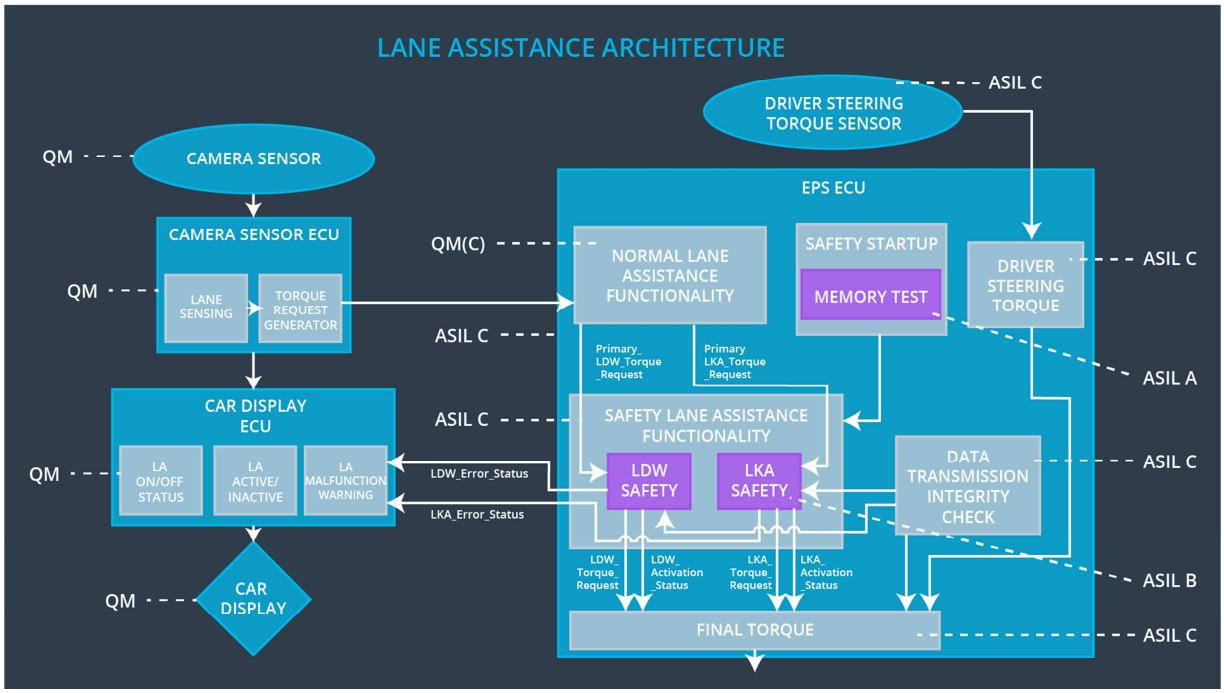


*Figure 2: Refinement of the System Architecture of the Lane Assistance Functionality*

## 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 | Turn off functionality | Malfunction_01<br>Malfunction_02 | Yes | Audio-visual warning in car display |
| WDC-02 | Turn off functionality | Malfunction_03 | Yes | Audio-visual warning in car display |