Elektrobit

UDACITY

# Technical Safety Concept
# Lane Assistance

**Document Version:** [Version]

Template Version 1.0, Released on 2017-06-21

# Document history

| Date | Version | Editor | Description |
|---|---|---|---|
| 2017-09-06 | 0.01 | Olli Vertanen | Initial version |
| | | | |
| | | | |
| | | | |
| | | | |

# Table of Contents

Purpose of the Technical Safety Concept 3
Inputs to the Technical Safety Concept 3
Functional Safety Requirements 3
System Architecture from Functional Safety Concept 4
Functional overview of architecture elements 4
Technical Safety Concept 6
Technical Safety Requirements 6
Lane Departure Warning (LDW) Requirements 6
Lane Departure Warning (LDW) Verification and Validation Acceptance Criteria 8
Lane Keeping Assistance (LKA) Requirements 10
Lane Keeping Assistance (LKA) Verification and Validation Acceptance Criteria 12
Refinement of the System Architecture 13
Allocation of Technical Safety Requirements to Architecture Elements 13
Warning and Degradation Concept 14

# Purpose of the Technical Safety Concept

The purpose of technical safety concept is to refine the functional safety concept and the preliminary architectural assumptions.

Technical safety concept derives the technical safety requirements from the functional safety concept and functional safety requirement. Technical safety concept also presents a refined item architecture and allocates the technical safety requirements to the architecture.

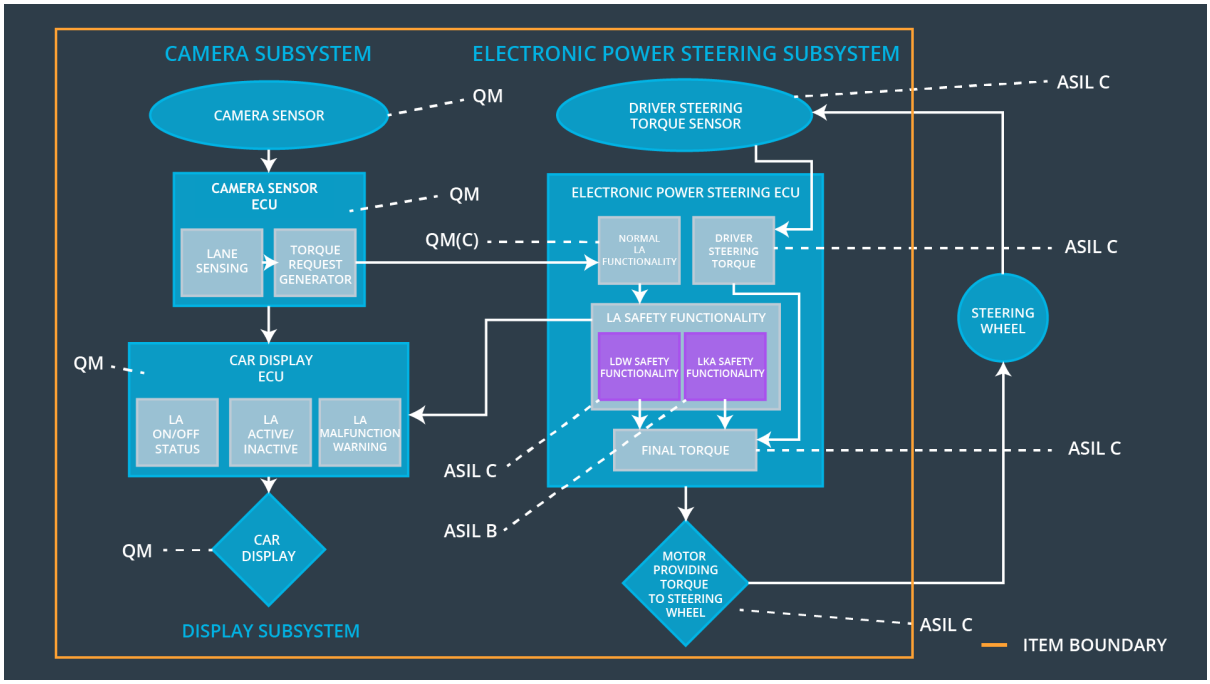
Technical safety requirements indicates the signal flow and describes which components are in charge of the functionality.

# 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 turned 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 | 50 ms | LDW turned off |
| Functional Safety Requirement 02-01 | The lane keeping item shall ensure that the lane keeping assistance torque is applied for only Max_Duration. | B | 500 ms | LKA turned off |

# System Architecture from Functional Safety Concept




# Functional overview of architecture elements

| Element | Description |
|---|---|
| Camera Sensor | Provides digital images of the road ahead of the vehicle. |
| Camera Sensor ECU - Lane Sensing | Detects lanes from camera sensor images. Calculates vehicle's position within ego lane. |
| Camera Sensor ECU - Torque request generator | Calculates required torque for LKA function, and sends the request to EPS ECU. |
| Car Display | Physical display of lane departure warning indicator (light) and other indicators. |
| Car Display ECU - Lane Assistance On/Off Status | Controls warning indicator based on lane assistance on/off status. |
| Car Display ECU - Lane Assistant Active/Inactive | Controls warning indicator based on lane assistance active/inactive status. |
| Car Display ECU - Lane Assistance malfunction warning | Controls warning indicator based on lane assistance malfunction status. |
| Driver Steering Torque Sensor | Senses the torque that driver is applying to the steering wheel. |

| | |
|---|---|
| Electronic Power Steering (EPS) ECU - Driver Steering Torque | Measures how much the driver is turning to the steering wheel |
| EPS ECU - Normal Lane Assistance Functionality | Receives torques requests from the camera ECU. |
| EPS ECU - Lane Departure Warning Safety Functionality | Limits the torque requests for LDW function within safety limits. |
| EPS ECU - Lane Keeping Assistant Safety Functionality | Limits the torque requests for LKA function to within safety limits. |
| EPS ECU - Final Torque | Calculates the final torque needed from torque request and driver’s steering action. |
| Motor | Provides actual torque to 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 01-01/01 | The LDW Safety component shall ensure that the amplitude of LDW_Torque_Request sent to the Final Torque component is below Max_Torque_Amplitude. | C | 50 ms | LDW Safety | LDW_Torque_Request == 0 |
| Technical Safety Requirement 01-01/02 | The validity and integrity of LDW_Torque_Request signal shall be ensured. | C | 50 ms | Data Transmission Integrity Check | N/A |
| Technical Safety Requirement 01-01/03 | As soon as a failure is detected by the LDW function, it shall deactivate the LDW feature and LDW_Torque_Request shall be set to zero. | C | 50 ms | LDW Safety | LDW_Torque_Request == 0 |

| | | | | | |
|---|---|---|---|---|---|
| Technical Safety Requirement 01-01/04 | 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 | LDW Safety | LDW_Torque_Request == 0 |
| Technical Safety Requirement 01-01/05 | Memory test shall be conducted at startup of the EPS ECU to check for any faults in memory. | A | ignition cycle | Memory Test | N/A |

Functional Safety Requirement 01-02 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 01-02/01 | The LDW Safety component shall ensure that the frequency of LDW_Torque_Request sent to the Final Torque component is below Max_Torque_Frequency. | C | 50 ms | LDW Safety | LDW_Torque_Request == 0 |
| Technical Safety Requirement 01-02/02 | The validity and integrity of LDW_Torque_Request signal shall be ensured. | C | 50 ms | Data Transmission Integrity Check | N/A |

| | | | | | |
|---|---|---|---|---|---|
| Technical Safety Requirement 01-02/03 | As soon as a failure is detected by the LDW function, it shall deactivate the LDW feature and LDW_Torque_Request shall be set to zero. | C | 50 ms | LDW Safety | LDW_Torque_Request == 0 |
| Technical Safety Requirement 01-02/04 | 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 | LDW Safety | LDW_Torque_Request == 0 |
| Technical Safety Requirement 01-02/05 | Memory test shall be conducted at startup of the EPS ECU to check for any faults in memory. | A | ignition cycle | Memory Test | LDW_Torque_Request == 0 |

## Lane Departure Warning (LDW) Verification and Validation Acceptance Criteria

**Validation**: checking that requirement's inputs, performed activities or generated outputs fulfil defined quality criteria.
**Verification**: means for checking that the final product (of the phase) fulfils the requirement.

| ID | Validation Acceptance Criteria and Method | Verification Acceptance Criteria and Method |
|---|---|---|
| Technical Safety Requirement 01-01/01 | Test at the functional level. Validation of the corresponding functional safety requirement 01-01 gives confidence of the correct threshold value. | Send to LDW safety function LDW_Torque_Requests with wide range of torque amplitude (below and above Max_Torque_Amplitude). Check that in all cases Final_LDW_Torque_Request has amplitude less than Max_Torque_Amplitude. |
| Technical Safety Requirement 01-01/02 | Requirements review. | Inject faults to LDW_Torque_Request (bit flips, burst errors etc.) Check that corruption during transfer is detected correctly. |

| | | |
|---|---|---|
| Technical Safety Requirement 01-01/03 | Requirements review. | Send to LDW safety function LDW_Torque_Requests with torque amplitude above Max_Torque_Amplitude. Check that LDW function deactivates and torque request is set to zero. |
| Technical Safety Requirement 01-01/04 | Requirements review. | Deactivate the LDW Safety function, and check that signal is sent to Car Display ECU. |
| Technical Safety Requirement 01-01/05 | Requirements review. | Check that LDW Safety function only activates when memory test is conducted successfully after ignition cycle. |

| ID | Validation Acceptance Criteria and Method | Verification Acceptance Criteria and Method |
|---|---|---|
| Technical Safety Requirement 01-02/01 | Test at the functional level. Validation of the corresponding functional safety requirement 01-02 gives confidence of the correct threshold value. | Send to LDW safety function LDW_Torque_Requests with wide range of torque frequency (below and above Max_Torque_Frequency). Check that in all cases Final_LDW_Torque_Request has frequency less than Max_Torque_Frequency. |
| Technical Safety Requirement 01-02/02 | Requirements review. | Inject faults to LDW_Torque_Request (bit flips, burst errors etc.) Check that corruption during transfer is detected correctly. |
| Technical Safety Requirement 01-02/03 | Requirements review. | Send to LDW safety function LDW_Torque_Requests with torque frequency above Max_Torque_Frequency. Check that LDW function deactivates and torque request is set to zero. |
| Technical Safety Requirement 01-02/04 | Requirements review. | Deactivate the LDW Safety function, and check that signal is sent to Car Display ECU. |
| Technical Safety Requirement 01-02/05 | Requirements review. | Check that LDW Safety function only activates when memory test is conducted successfully after ignition cycle. |

## Lane Keeping Assistance (LKA) Requirements

Functional Safety Requirement 02-01 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 02-01 | The lane keeping item shall ensure that the lane keeping assistance torque is applied only for Max_Duration of time. | 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 02-01 /01 | The LKA Safety component shall ensure that the duration of LKA_Torque_Request sent to the Final Torque component is less than Max_Duration. | B | 500 ms | LKA Safety | LKA_Torque_Request == 0 |
| Technical Safety Requirement 02-01/02 | The validity and integrity of LKA_Torque_Request signal shall be ensured. | B | 500 ms | Data Transmission Integrity Check | N/A |
| Technical Safety Requirement 02-01/03 | As soon as a failure is detected by the LKA function, it shall deactivate the LKA feature and LKA_Torque_Request shall be set to zero. | B | 500 ms | LKA Safety | LKA_Torque_Request == 0 |
| Technical Safety Requirement 02-01/04 | 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 | LKA Safety | LKA_Torque_Request == 0 |
| Technical Safety Requirement 02-01/05 | Memory test shall be conducted at startup of the EPS ECU to check for any faults in memory. | A | Ignition cycle | Memory Test | LKA_Torque_Request == 0 |

Functional Safety Requirement 02-02 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 02-02 | The lane keeping item shall ensure that the lane keeping assistance torque has same direction than Lane_Centre_Distance. The ego lane centre is on the left (driving direction), if the distance is negative. | X | | |

Technical Safety Requirements related to Functional Safety Requirement 02-02 are:

| ID | Technical Safety Requirement | ASIL | Fault Tolerant Time Interval | Allocation to Architecture | Safe State |
|---|---|---|---|---|---|
| Technical Safety Requirement 02-02 /01 | The LKA Safety component shall ensure that the direction of LKA_Torque_Request sent to the Final Torque component is same as the assumed ego lane center. | B | 50 ms | LKA Safety | LKA_Torque_Request == 0 |
| Technical Safety Requirement 02-02/02 | The validity and integrity of LKA_Torque_Request signal shall be ensured. | B | 50 ms | Data Transmission Integrity Check | N/A |
| Technical Safety Requirement 02-02/03 | As soon as a failure is detected by the LKA function, it shall deactivate the LKA feature and LKA_Torque_Request shall be set to zero. | B | 50 ms | LKA Safety | LKA_Torque_Request == 0 |
| Technical Safety Requirement 02-02/04 | 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 | 50 ms | LKA Safety | LKA_Torque_Request == 0 |
| Technical Safety Requirement 02-02/05 | Memory test shall be conducted at startup of the EPS ECU to check for any faults in memory. | A | Ignition cycle | Memory Test | LKA_Torque_Request == 0 |

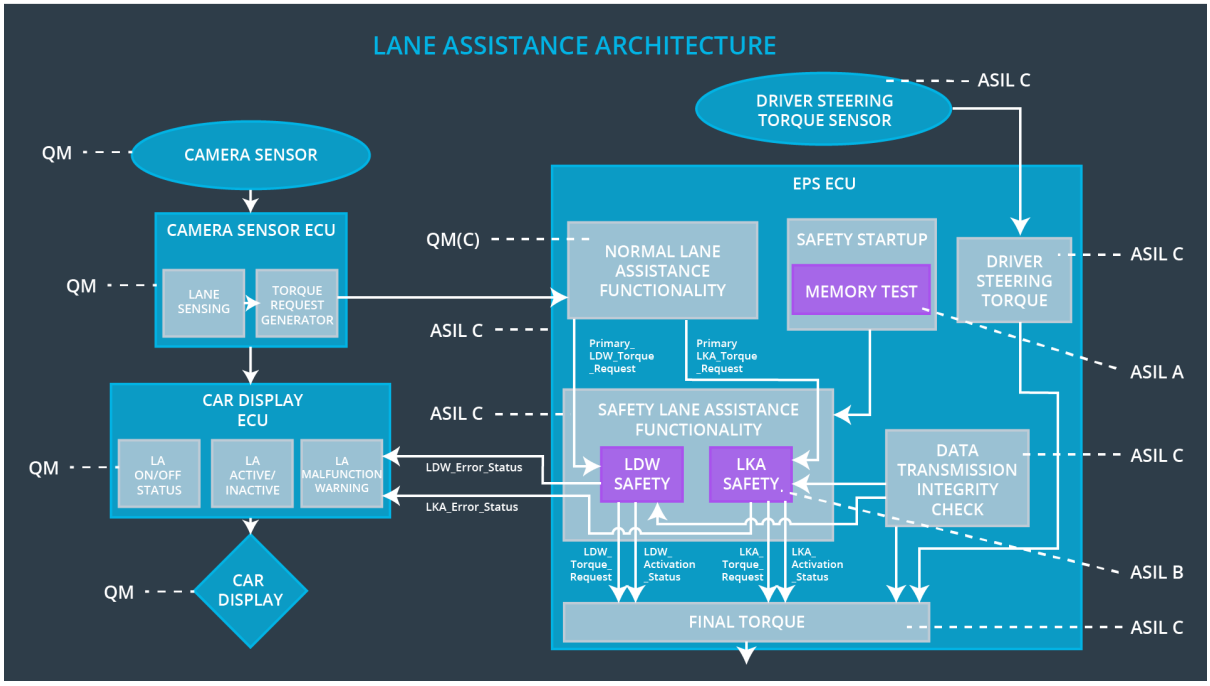
## Lane Keeping Assistance (LKA) Verification and Validation Acceptance Criteria

**Validation**: checking that requirement's inputs, performed activities or generated outputs fulfil defined quality criteria.
**Verification**: means for checking that the final product (of the phase) fulfils the requirement.

| ID | Validation Acceptance Criteria and Method | Verification Acceptance Criteria and Method |
|---|---|---|
| Technical Safety Requirement 02-01/01 | Test at the functional level. Validation of the corresponding functional safety requirement 02-01 gives confidence of the correct threshold value. | Send to LDW safety function LDW_Torque_Requests with wide range of torque amplitude (below and above Max_Torque_Amplitude). Check that in all cases Final_LDW_Torque_Request has amplitude less than Max_Torque_Amplitude. |
| Technical Safety Requirement 02-01/02 | Requirements review. | Inject faults to LKA_Torque_Request (bit flips, burst errors etc.) Check that corruption during transfer is detected correctly. |
| Technical Safety Requirement 02-01/03 | Requirements review. | Send to LKA safety function LKA_Torque_Request with torque duration above Max_Torque_Duration. Check that LKA safety function deactivates and torque request is set to zero. |
| Technical Safety Requirement 02-01/04 | Requirements review. | Deactivate the LKA Safety function, and check that signal is sent to Car Display ECU. |
| Technical Safety Requirement 02-01/05 | Requirements review. | Check that LKA Safety function only activates when memory test is conducted successfully after ignition cycle. |
| Technical Safety Requirement 02-02/01 | Test at the functional level. Validation of the corresponding functional safety requirement 02-02 gives confidence of the correct threshold value. | Send to LDW safety function LDW_Torque_Requests with different ego lane centre distance (either left or right). Check that in all cases Final_LDW_Torque_Request has the same direction. |
| Technical Safety Requirement 02-02/02 | See Technical Safety Requirement 02-01/02 | See Technical Safety Requirement 02-01/02 |

| | | |
|---|---|---|
| Technical Safety Requirement 02-02/03 | See Technical Safety Requirement 02-01/03 | See Technical Safety Requirement 02-01/03 |
| Technical Safety Requirement 02-02/04 | See Technical Safety Requirement 02-01/04 | See Technical Safety Requirement 02-01/04 |
| Technical Safety Requirement 02-02/05 | See Technical Safety Requirement 02-01/05 | See Technical Safety Requirement 02-01/05 |

## Refinement of the System Architecture




## Allocation of Technical Safety Requirements to Architecture Elements

For this safety item, all technical safety requirements are allocated to the Electronic Power Steering ECU.

For allocation of each individual technical safety requirements, see separate technical requirement lists.

# Warning and Degradation Concept

For malfunction explanations, see the Functional Safety Concept

| ID | Degradation Mode | Trigger for Degradation Mode | Safe State invoked? | Driver Warning |
|---|---|---|---|---|
| WDC-01 | Turn off LDW | Malfunction_01<br>Malfunction_02 | Yes | Dashboard light |
| WDC-02 | Turn off LKA | Malfunction_03<br>Malfunction_04 | Yes | Dashboard light |