Elektrobit

UDACITY

# Technical Safety Concept Lane Assistance

**Document Version: 1.0**

# Document history

| Date | Version | Editor | Description |
|---|---|---|---|
| 2018-01-28 | 1.0 | Josef Steinbaeck | First attempt |
| | | | |
| | | | |
| | | | |
| | | | |

# Table of Contents

# Purpose of the Technical Safety Concept

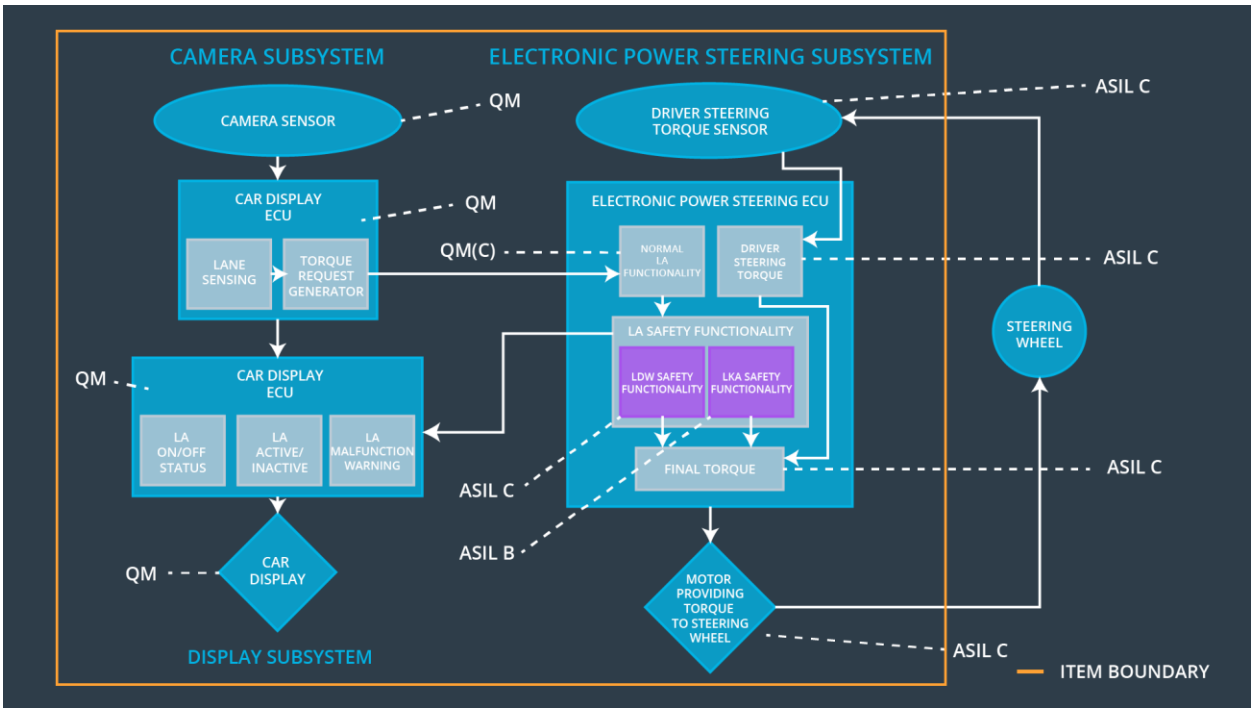
The technical Safety Concept describes how the subsystems interact at the message level and describe how the ECUs communicate with each other. A technical safety requirement indicates the signal flow and describes which components are in charge of the functionality.

# 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 will set the oscillating torque amplitude 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 | The torque request from the lane keeping assistance will be 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 | 50 ms | The torque request from the lane keeping assistance will be set to zero |

# Refined System Architecture from Functional Safety Concept



## Functional overview of architecture elements

| Element | Description |
|---|---|
| Camera Sensor | The camera sensor reads in images from the road |
| Camera Sensor ECU - Lane Sensing | Locates the lane on the sequentially obtained camera images |
| Camera Sensor ECU - Torque request generator | Generates a torque request to the Electronic Power Steering ECU using the result of the lane sensing |
| Car Display | The display contains lights indicating the current state of the lane assistance system |
| Car Display ECU - Lane Assistance On/Off Status | Tells the driver weather the lane keeping item is on or off |
| Car Display ECU - Lane Assistant Active/Inactive | Tells the driver weather the lane departure warning is activated |
| Car Display ECU - Lane Assistance malfunction warning | A light indicating a malfunction within the lane assistance system |
| Driver Steering Torque Sensor | Senses the steering torque applied by the driver and sends it to the Electronic Power Steering ECU |
| Electronic Power Steering (EPS) ECU - Driver Steering Torque | Senses how much the driver is turning the steering wheel. |
| EPS ECU - Normal Lane Assistance Functionality | Receive and interpret the torque request from the camera subsystem (Non-safety relevant) |
| EPS ECU - Lane Departure Warning Safety Functionality | Make sure the torque request does not exceed certain limits (amplitude, frequency) |
| EPS ECU - Lane Keeping Assistant Safety Functionality | Make sure the torque request does not exceed certain limits (time) |
| EPS ECU - Final Torque | Adds the torque request by the driver and the lane assistance block together to output a final torque to the motor. |
| Motor | Moves 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 | LA Safety Functionality | LDW torque output is 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 | LA Safety Functionality | LDW torque output is 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 | LA Safety Functionality | LDW torque output is 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 output is set to zero |
| Technical Safety Requirement 05 | Memory test shall be conducted at start-up of the EPS ECU to check for any faults in memory. | A | Ignition Cycle | Safety startup | LDW torque output is 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 | LA Safety Functionality | LDW torque output is 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 | LA Safety Functionality | LDW torque output is set to zero |
| Technical Safety Requirement | As soon as a failure is detected by the LDW function, it shall deactivate | C | 50 ms | LA Safety Functionality | LDW torque output is |

| | | | | | |
|---|---|---|---|---|---|
| 03 | the LDW feature and the 'LDW_Torque_Request' shall be set to zero. | | | | 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 output is set to zero |
| Technical Safety Requirement 05 | Memory test shall be conducted at start-up of the EPS ECU to check for any faults in memory. | A | Ignition Cycle | Safety startup | LDW torque output is set to zero |

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

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

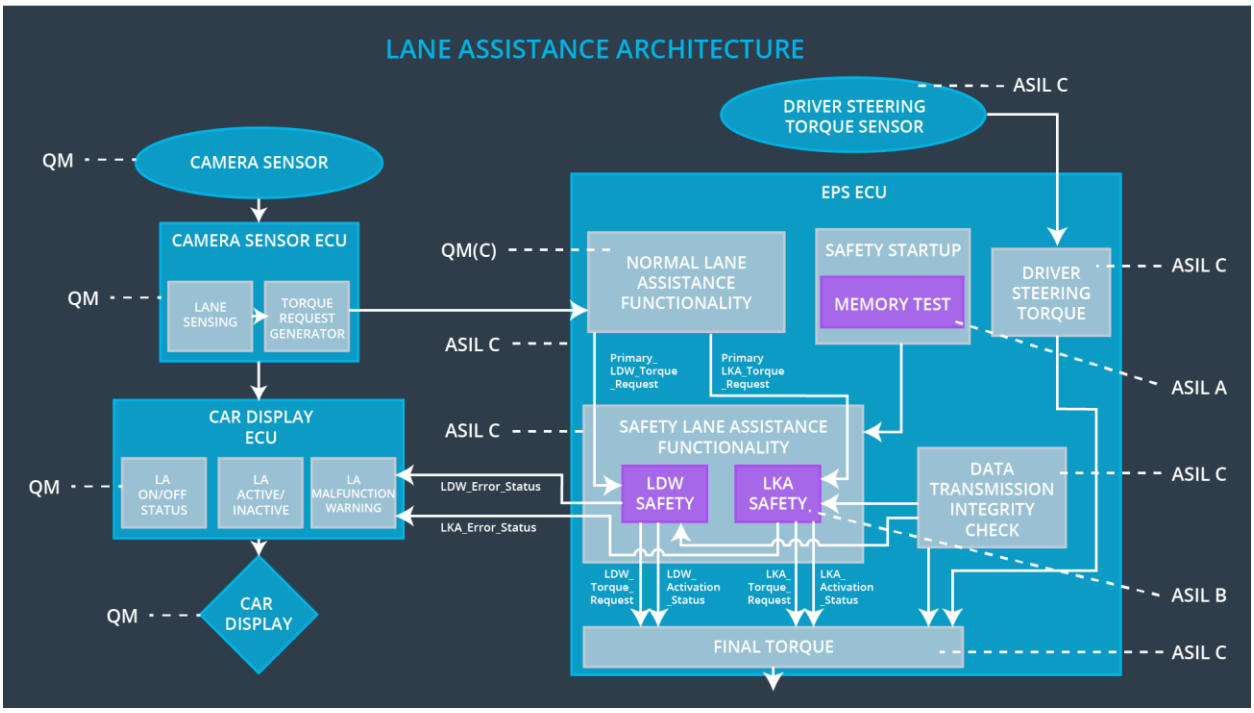
| ID | Functional Safety Requirement | Electronic Power Steering ECU | Camera ECU | Car Display ECU |
|---|---|---|---|---|
| Functional Safety Requirement 02-01 | The lane keeping item shall ensure that the lane keeping assistance torque is applied for only Max_Duration | X | | |

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 lane keeping safety component shall ensure that a steering torque is only applied for a maximum duration of Max_Duration | B | 500 ms | LA Safety Functionality | LKA torque output is set to zero |
| Technical Safety Requirement 02 | As soon as the lane keeping function deactivates the lane keeping feature, the 'LA Safety' software block shall send a signal | B | 500 ms | LA Safety Functionality | LKA torque output is set to zero |

| | | | | | |
|---|---|---|---|---|---|
| | to the car display ECU to turn on a warning light. | | | | |
| Technical Safety Requirement 03 | As soon as a failure is detected by the LA function, it shall deactivate the LKA feature and the 'LKA_Torque_Request' shall be set to zero. | B | 500 ms | LA Safety Functionality | LKA torque output is set to zero |
| Technical Safety Requirement 04 | The validity and integrity of the data transmission for 'LKA_Torque_Request' signal shall be ensured. | B | 500 ms | Data Transmission Integrity check | LKA torque output is set to zero |
| Technical Safety Requirement 05 | Memory test shall be conducted at start-up of the EPS ECU to check for any faults in memory. | A | Ignition Cycle | Safety startup | LKA torque output is set to zero |

## 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 | Turn off functionality | lane departure oscillating torque frequency or amplitude too high | Yes | Warning light on the dashboard |
| WDC-02 | Turn off functionality | lane keeping assistance torque is applied for Max_Time | Yes | Warning light on the dashboard |