Elektrobit

UDACITY

# Technical Safety Concept Lane Assistance

**Document Version:** [1.0]

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

# Document history

| Date | Version | Editor | Description |
|---|---|---|---|
| 1/6/2018 | 1.0 | Pratul Singh | First attempt |
| | | | |
| | | | |
| | | | |
| | | | |

# Table of Contents



# Purpose of the Technical Safety Concept

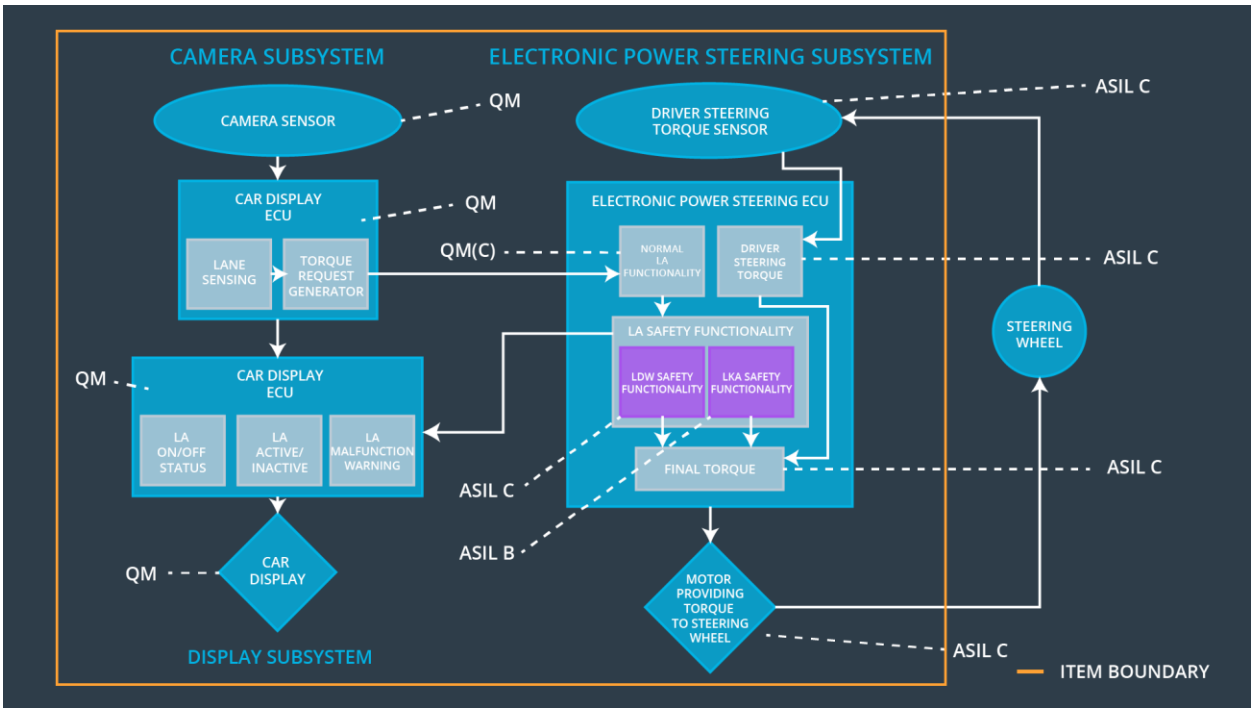
A technical safety concept is similar to a functional safety concept in the sense that it defines requirements and allocates them to subsystems. While a functional safety concept provides a bird’s eye view of the system, a technical safety concept goes deeper into the technical details of the system. Technical safety requirements are derived from functional safety requirements.

# 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 | 50ms | Lane Departure warning function is not activated |
| Functional Safety Requirement 01-02 | The electronic power steering ECU shall ensure that the lane departure warning oscillating torque frequency is below Max_Torque_Frequency | C | 50ms | Lane Departure warning function is not activated |
| 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 | 50ms | Lane Keeping assistance system is not activated |

# Refined System Architecture from Functional Safety Concept




## Functional overview of architecture elements

| Element | Description |
|---|---|
| Camera Sensor | Sensor responsible for capturing vehicle driving condition including detectable lane lines. |
| Camera Sensor ECU - Lane Sensing | Software Module in the Camera Sensor ECU responsible for detecting lane lines and determining when the vehicle leaves the lane by mistake. |
| Camera Sensor ECU - Torque request generator | Software Module in the Camera Sensor ECU responsible for calculating and sending the additional torque for the LDW and LKA functions. |
| Car Display | Visual display responsible to displaying warning of lane departures and LKA and LDW activation and deactivations. |
| Car Display ECU - Lane Assistance On/Off Status | Visual display responsible to displaying LKA and LDW ON/OFF status. |

| | |
|---|---|
| Car Display ECU - Lane Assistant Active/Inactive | Visual display responsible to displaying displaying warning of lane departures, LKA and LDW activation and deactivations. |
| Car Display ECU - Lane Assistance malfunction warning | Visual display responsible to displaying warning of LKA and LDW malfunctions. |
| Driver Steering Torque Sensor | Sensor responsible for measuring how much force (steering torque) the driver is applying to the steering wheel. |
| Electronic Power Steering (EPS) ECU - Driver Steering Torque | Software Module in the electronic power steering ECU responsible for receiving the Camera Sensor ECU torque requests. |
| EPS ECU - Normal Lane Assistance Functionality | Software Module in the electronic power steering ECU responsible for receiving the Driver Steering torque sensor input from the steering wheel. |
| EPS ECU - Lane Departure Warning Safety Functionality | Software Module in the electronic power steering ECU responsible for keeping the lane departure oscillating torque amplitude and frequence below MAX_Torque_Amplitude and MAX_Torque_Fequency respectively |
| EPS ECU - Lane Keeping Assistant Safety Functionality | Software Module in the electronic power steering ECU responsible for ensuring the application of the lane keeping assistance torque does not ever exceeded Max_Duration and if lane detection is lost, the LKA function is deactivated. |
| EPS ECU - Final Torque | Software Module in the electronic power steering ECU responsible for ensuring the LDW, LKA and the driver’s steering torque requests are combined and sent to the Motor. |
| Motor | Actuator responsible for applying requested torque to the steering column by the Electronic Power Steering ECU for either the LKA or the LDW functions. |

# 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 | LDW Safety Block | The lane departure warning torque request amplitude 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 | Data Transmission Integrity Check | The lane departure warning torque request amplitude shall be set to zero |
| Technical Safety Requirem | As soon as a failure is detected by the LDW function, it shall | C | 50 ms | LDW Safety Block | The lane departure warning |

| | | | | | |
|---|---|---|---|---|---|
| ent<br>03 | deactivate the LDW feature and the 'LDW_Torque_Request' shall be set to zero. | | | | torque request amplitude shall be set to zero |
| Technical Safety Requirement<br>04 | The validity and integrity of the data transmission for 'LDW_Torque_Request' signal shall be ensured. | C | 50 ms | LDW Safety Block | The lane departure warning torque request amplitude shall be set to zero |
| Technical Safety Requirement<br>05 | Memory test shall be conducted at start up of the EPS ECU to check for any faults in memory | A | Ignition cycle | Separate External block with Memory test code | The lane departure warning torque request amplitude 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 | 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 | 50ms | LDW Safety Component | The lane departure warning torque request amplitude shall be set to zero |
| Technical Safety Requirement 02 | Validity and Integrity of the data transmission for the LDW_Torque_Request signal shall be ensured | C | 50ms | Data Transmission Integrity Check | The lane departure warning torque request amplitude 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 | 50ms | LDW Safety Component | The lane departure warning torque request amplitude 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 | 50ms | LDW Safety Component | The lane departure warning torque request amplitude shall be set to zero |
| Technical Safety | Memory test shall be conducted at the startup of EPS ECU to check | A | Iginition Cycle | Separate External block | The lane |

| | | | | | |
|---|---|---|---|---|---|
| Requirement 05 | for any faults in memory. | | | with Memory test code | departur e warning torque request amplitud e 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)

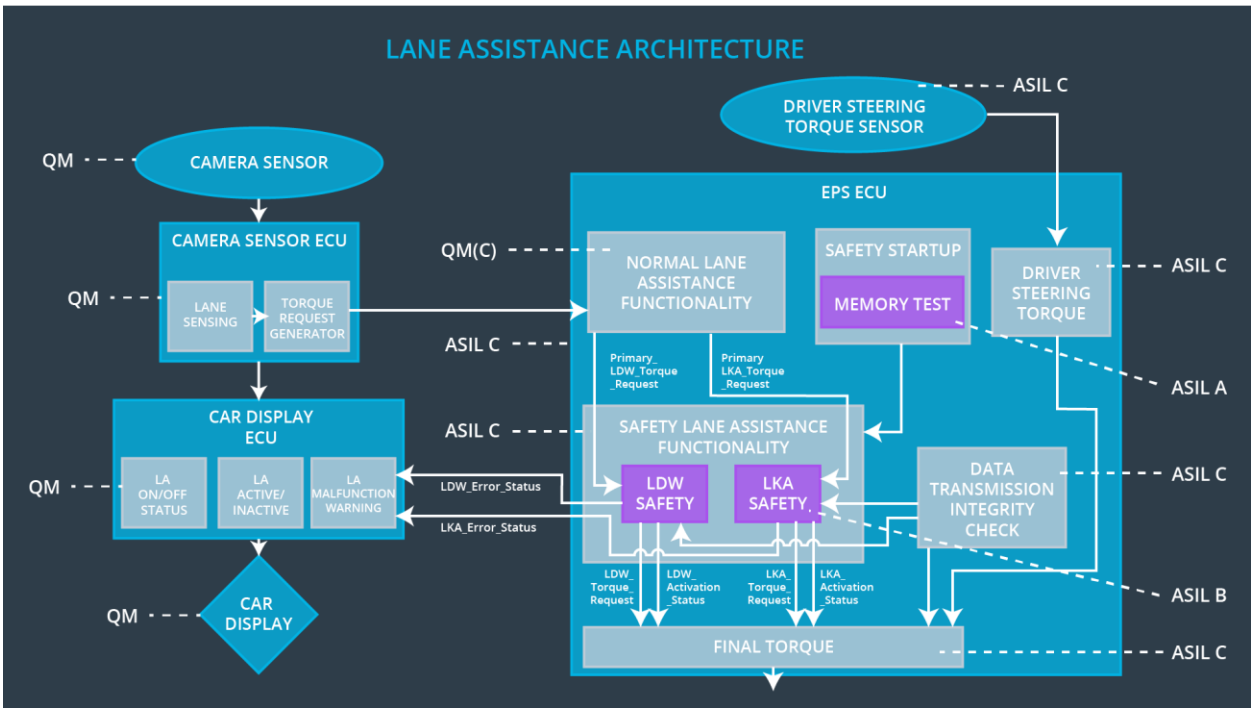
| ID | Functional Safety Requirement | Electronic Power Steering ECU | Camera ECU | Car Display ECU |
|---|---|---|---|---|
| Functional Safety Requirement 02-01 | The lane keeping item shall ensure that the lane keeping assistance torque is applied for only Max_Duration | X | | |

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 | LKA safety component shall ensure that the duration of the LKA_torque_request sent to the Final Electronic Power Steering Torque component is below Max_torque_duration | B | 500ms | LKA safety component | The lane departur e warning torque request amplitud e shall be set to zero |
| Technical Safety Requirement 02 | Validity and Integrity of the data transmission for the LKA_Torque_Request signal shall be ensured | B | 500ms | Data Transmission Integrity Check | The lane departur e warning torque request |

| | | | | | |
|---|---|---|---|---|---|
| | | | | | amplitud e 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 | 500ms | LKA safety component | The lane departur e warning torque request amplitud e 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 | 500ms | LKA safety component | The lane departur e warning torque request amplitud e shall be set to zero |
| Technical Safety Requirement 05 | Memory test shall be conducted at the startup of EPS ECU to check for any faults in memory | A | Ignition Cycle | Separate External block with Memory test code | The lane departur e warning torque request amplitud e shall be set to zero |

# Refinement of the System Architecture




# Allocation of Technical Safety Requirements to Architecture Elements

Ignore this item as all technical safety requirements are allocated to the Electronic Power Steering ECU

# Warning and Degradation Concept

The warning and degradation concept is the same for the technical safety requirements as for the functional safety requirements.

| | |
|---|---|
| Warning | Warning light displayed to the driver on the dashboard |
| Degradation | Turn off functionality |