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 |
|---|---|---|---|
| May 25, 2018 | 1.0 | Aftab Engaria | Initial Draft |
| | | | |

# Table of Contents

# Purpose of the Technical Safety Concept

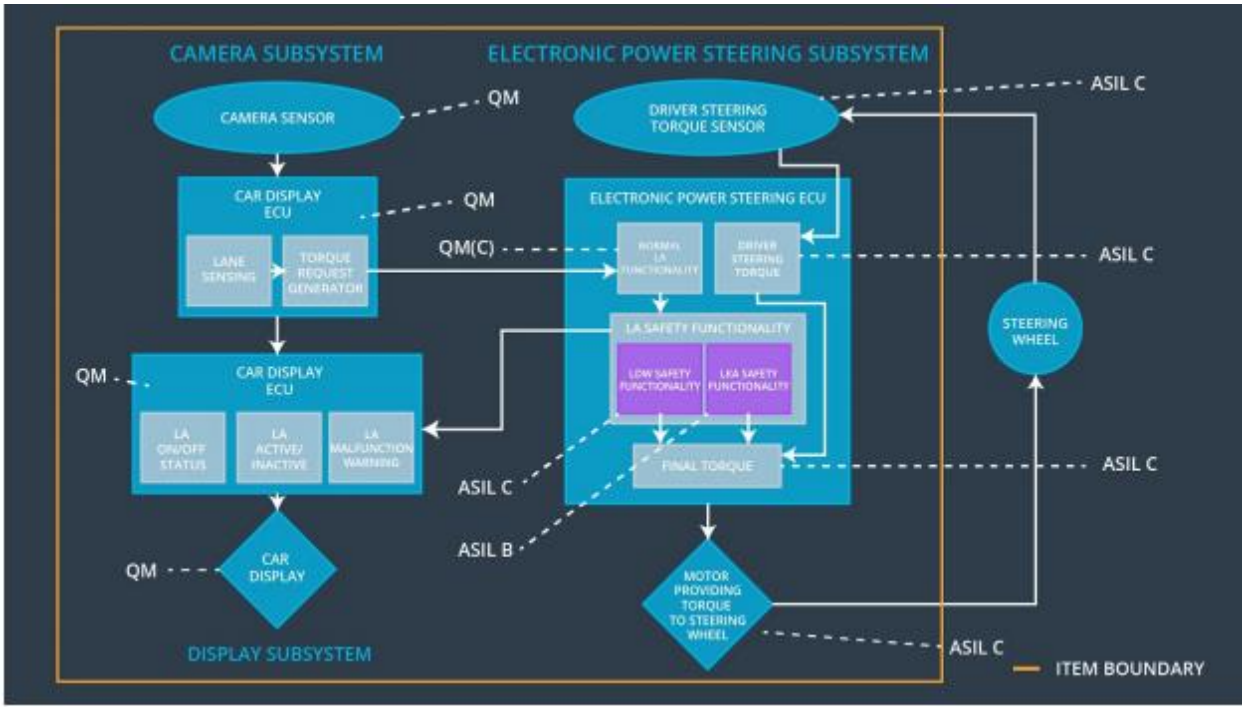
In this document, new requirements are defined and allocate these high level hardware and software requirements to system diagrams for the lane assistance functional safety project as pertain to the potential malfunctions of the electrical and electronic systems. These new requirements are more concrete and gets into details of the item's technology as specified by ISO 26262.

# 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 Departure Warning item shall ensure that the lane departure oscillating torque amplitude is below Max_Torque_Amplitude. | C | 50ms | Vibration torque amplitude below Max_Torque_Amplitude. |
| Functional Safety Requirement 01-02 | The Lane Departure Warning item shall ensure that the lane departure oscillating torque frequency is below Max_Torque_Frequency. | C | 50ms | Vibration frequency is below Max_Torque_Frequency. |
| Functional Safety Requirement 02-01 | The electronic power steering ECU shall ensure that the Lane Keeping Assistance torque is applied only Max_Duration. | B | 500ms | Lane Keeping Assistance torque is zero. |

## Refined System Architecture from Functional Safety Concept

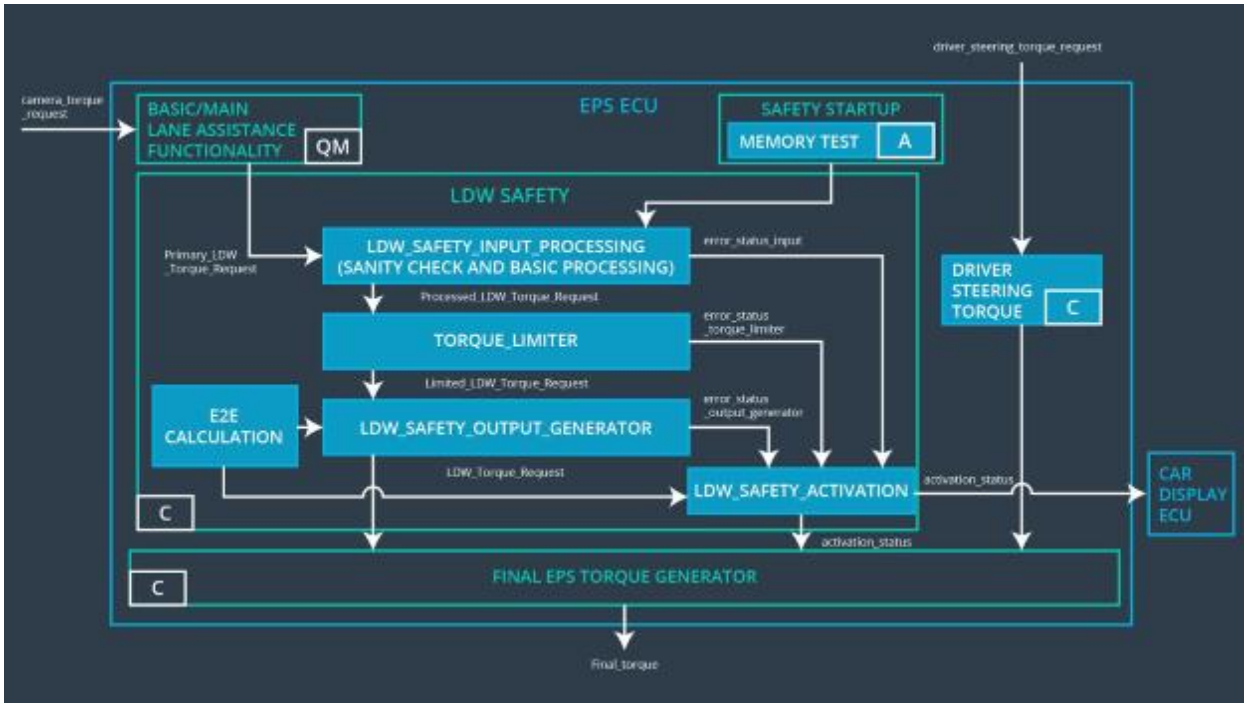



## Functional overview of architecture elements

| Element | Description |
|---|---|
| Camera Sensor | Capture road images and provide them to the Camera Sensor ECU. |
| Camera Sensor ECU - Lane Sensing | Software module detecting the lane line positions from the Camera Sensor images. |
| Camera Sensor ECU - Torque request generator | Software module calculating the necessary torque to be requested to the Electronic Power Steering ECU. |
| Car Display | Display warning for the driver. |
| Car Display ECU - Lane Assistance On/Off Status | Indicate the status of the Lane Assistance functionality (On/Off.) |
| Car Display ECU - Lane Assistant Active/Inactive | Indicate if the Lane Assistance functionality is properly functioning (Active/Inactive.) |
| Car Display ECU - Lane Assistance malfunction warning | Indicate a malfunction on the Lane Assistance functionality. |

| | |
|---|---|
| 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 Lane Departure Warning 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 | Lane Departure Warning torque to zero. |
| Technical Safety Requirement 02 | When the Lane Departure Warning is deactivated, the 'LDW Safety' software module shall send a signal to the Car Display ECU to turn on a warning signal. | C | 50 ms | LDW Safety | Lane Departure Warning torque to zero. |
| Technical Safety Requirement 03 | When a failure is detected by the Lane Departure Warning functionality, it shall deactivate the Lane Departure Warning feature and set 'LDW_Torque_Request' to zero. | C | 50 ms | LDW Safety | Lane Departure Warning torque 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 | LDW Safety | Lane Departure Warning torque to zero |
| Technical Safety Requirement 05 | Memory test shall be conducted at startup of the EPS ECU to check for any memory problems | A | Ignition cycle | Data Transmission Integrity Check | Lane Departure Warning torque 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 Lane Departure Warning safety component shall ensure 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 | Lane Departure Warning torque to zero |

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

| ID | Technical Safety Requirement | Verification Acceptance Criteria and Method |
|---|---|---|
| Technical Safety Requirement 01-01 | Validate the Max_Torque_Amplitude is the chosen from the Lane Departure Warning Validation' | Verify the Lane Departure Warning functionality is turned off. |
| Technical Safety Requirement 01-02 | Validate the 'TORQUE_LIMITER' sends the error_status_torque_limiter signal to the LDW_SAFETY_ACTIVATION | Verify the Car Display ECU displays the Lane Departure Warning malfunction warning signal. |
| Technical Safety Requirement 01-03 | Validate the 'TORQUE_LIMITER' sends 'LDW_Torque_Request' with zero | Verify the Final EPS Torque generator receives a LDW_Torque_Request of zero |

| | | |
|---|---|---|
| Technical Safety Requirement 01-04 | Validate the 'TORQUE_LIMITER' calculate and sends the correct cyclic redundancy check (CRC) and Alive counter for data transmission validity and integrity. | Verify the functionality is turn off if there is a CRC or Alive counter discrepancy. |
| Technical Safety Requirement 01-05 | Validate the Safety Startup Memory test to check memory faults catch memory faults. | Verify the Lane Departure Warning is turned off when the Safety Startup Memory fails. |
| Technical Safety Requirement 02-01 | Validate the Max_Torque_Frequency set is the chosen from the Lane Departure Warning Acceptance Criteria. | Verify the functionality is turned off if the 'LDW_Torque_Request' frequency exceeds Max_Torque_Request. |

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

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

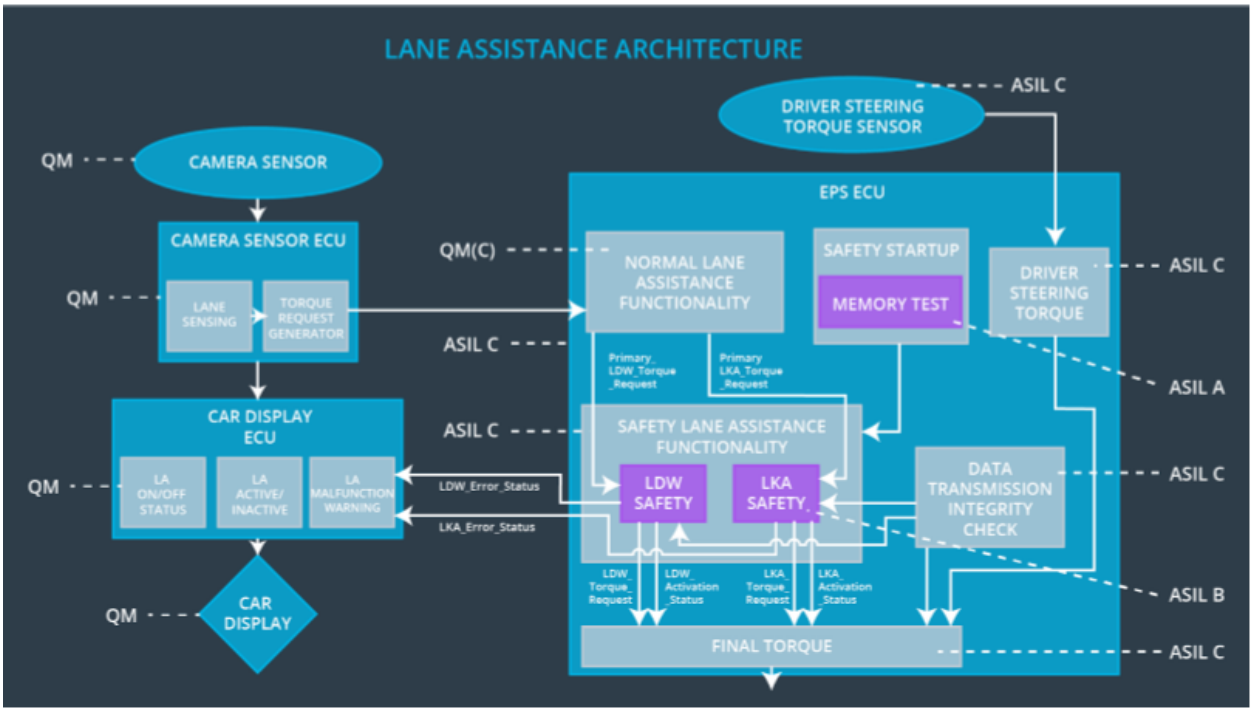
| ID | Functional Safety Requirement | Electronic Power Steering ECU | Camera ECU | Car Display ECU |
|---|---|---|---|---|
| Functional Safety Requirement 02-01 | The lane keeping item shall ensure that the lane keeping assistance torque is applied for only Max_Duration | X | | |

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 Departure Warning safety component shall ensure the frequency of the 'LDW_Torque_Reques' sent to the 'Final electronic power steering Torque' component is | C | 50 ms | LDW Safety | Lane Depart ure Warnin g torque to zero. |

| | | | | | |
|---|---|---|---|---|---|
| | below ‘Max_Torque_Frequency.’ | | | | |

## Architecture




## Allocation of Technical Safety Requirements to Architecture Elements

| ID | Technical Safety Requirement | Electronic Power Steering ECU | Camera ECU | Car Display ECU |
|---|---|---|---|---|
| Technical Safety Requirement 01-01 | The Lane Departure Warning 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.’ | X | 50 ms | LDW Safety |
| Technical Safety Requirement | When the Lane Departure Warning is deactivated, the | X | | |

| | | | | |
|---|---|---|---|---|
| 01-02 | ‘LDW Safety’ software module shall send a signal to the Car Display ECU to turn on a warning signal. | | | |
| Technical Safety Requirement 01-03 | When a failure is detected by the Lane Departure Warning functionality, it shall deactivate the Lane Departure Warning feature and set ‘LDW_Torque_Request’ to zero. | X | | |
| Technical Safety Requirement 01-04 | The validity and integrity of the data transmission for ‘LDW_Torque_Request’ signal shall be ensured. | X | | |
| Technical Safety Requirement 01-05 | Memory test shall be conducted at startup of the EPS ECU to check for any memory problems. | X | | |
| Technical Safety Requirement 01-02-01 | The Lane Departure Warning safety component shall ensure the frequency of the ‘LDW_Torque_Reques’ sent to the ‘Final electronic power steering Torque’ component is below ‘Max_Torque_Frequency.’ | X | | |
| Technical Safety Requirement 02-01-01 | The Lane Keeping Assistance safety component shall ensure the duration of the lane keeping assistance torque is applied for less than Max_Duration | X | | |
| Technical Safety Requirement 02-01-02 | When the Lane Keeping Assistance function deactivates, the ‘LKA Safety’ shall send a signal to the Car Display ECU to turn on a warning light. | X | | |

| | | | | |
|---|---|---|---|---|
| Technical Safety Requirement 02-01-03 | When a failure is detected, the Lane Keeping Assistance function shall deactivate and the ‘LKA_Torque_Request’ shall be zero. | X | | |
| Technical Safety Requirement 02-01-04 | The validity and integrity of the data transmission for ‘LKA_Torque_Request’ signal shall be ensured. | X | | |
| Technical Safety Requirement 02-01-05 | Memory test shall be conducted at startup of the EPS ECU to check for any memory problems | X | | |

## Warning and Degradation Concept

| ID | Degradation Mode | Trigger for Degradation Mode | Safe State invoked? | Driver Warning |
|---|---|---|---|---|
| WDC-01 | Turn off Lane Departure Warning functionality | Malfunction_01, Malfunction_02, Malfunction_04 | Yes | Lane Departure Warning Malfunction Warning on Car Display |
| WDC-02 | Turn off Lane Keeping Assistance functionality | Malfunction_03, Malfunction_05 | Yes | Lane Keeping Assistance Malfunction Warning on Car Display |