Elektrobit

UDACITY

# Technical Safety Concept Lane Assistance

**Document Version: 1.0**

# Document history

| Date | Version | Editor | Description |
|---|---|---|---|
| 5/24/18 | 1.0 | Ganesh Prabakaran | Initial |
| | | | |
| | | | |
| | | | |
| | | | |

# Table of Contents

## Contents

# Purpose of the Technical Safety Concept

The Technical Safety Concept defines how the subsystems interact at message level and describes how the ECU's communicate with each other. Technical safety concept is part of the product development phase. The product development phase also includes designing hardware and software.

# 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 system shall ensure the lane departure oscillating torque amplitude is not exceeding Max_Torque_Amplitude. | C | 50 | Set Oscillating Torque amplitude to zero when fault is detected |
| Functional Safety Requirement 01-02 | The lane departure warning system shall ensure the lane departure oscillating torque frequency is not exceeding Max_Torque_Frequency. | C | 50 | Set Oscillating Torque frequency to zero when fault is detected |
| Functional Safety Requirement 02-01 | Lane keeping assistance function shall be time limited and the additional steering torque shall end after a given timer interval so that the driver cannot misuse the system for autonomous driving | B | 50 | Lane keeping assistance function should stop applying extra torque after the fault tolerant time interval |

# Refined System Architecture from Functional Safety Concept

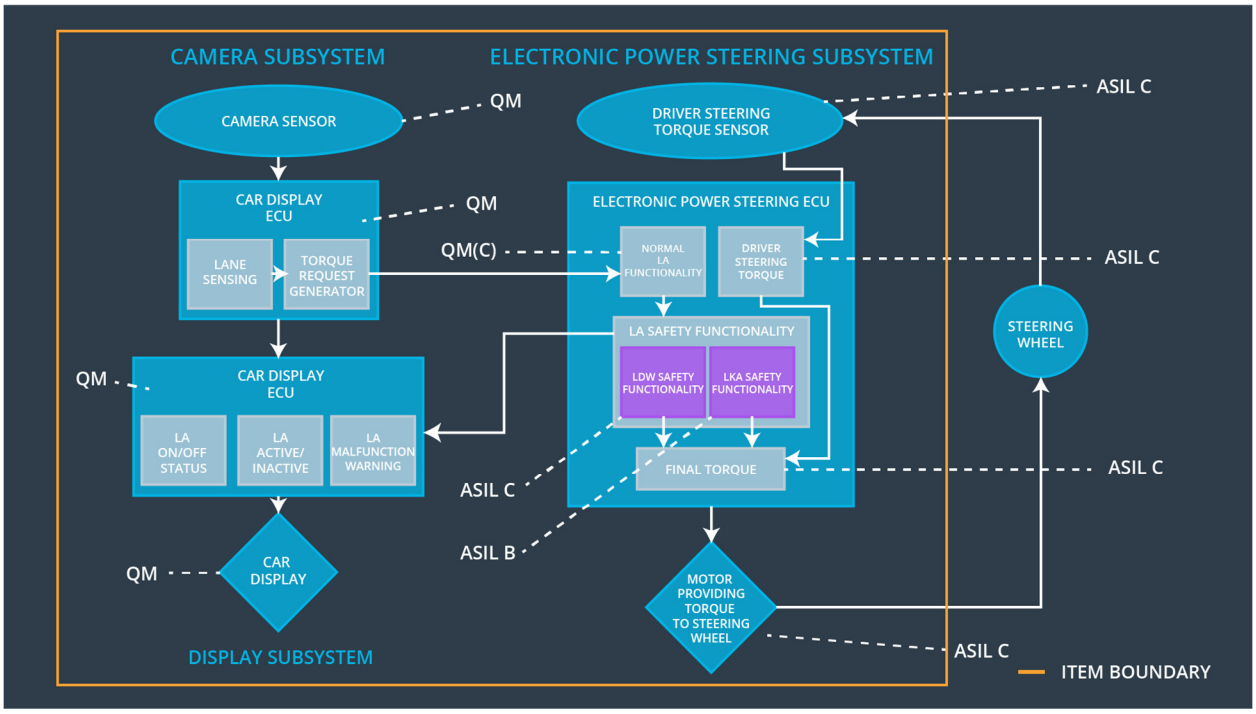



*Fig.1 Lane Assistance System Architecture*
*[Image source: Udacity course content]*

## Functional overview of architecture elements

| Element | Description |
|---|---|
| Camera Sensor | Captures images from the front view of the car to assist in lane detection. |
| Camera Sensor ECU - Lane Sensing | Performs computation on the captured images to detect lanes and find the position of the car with respect to the lane |
| Camera Sensor ECU - Torque request generator | Performs computation on the position of the car with respect to the lane and generate torque request for the steering wheel in order to keep the car stay in lane. |
| Car Display | Display warning for the driver |
| Car Display ECU - Lane Assistance On/Off Status | Indicate if the Lane Assistance system is ON or OFF |

| | |
|---|---|
| Car Display ECU - Lane Assistant Active/Inactive | Indicate the active/inactive status Lane Assistance system |
| Car Display ECU - Lane Assistance malfunction warning | Display warning if the Lane Assistance system is malfunctioning |
| Driver Steering Torque Sensor | This sensor captures the steering wheel angular displacement initiated by the driver and sends it to the Electronic Power Steering ECU |
| Electronic Power Steering (EPS) ECU - Driver Steering Torque | This module receives input from driver steering torque sensor |
| EPS ECU - Normal Lane Assistance Functionality | This module receives input from camera ECU torque request |
| EPS ECU - Lane Departure Warning Safety Functionality | This module performs lane departure warning functionality and ensure steering torque request is well below Max torque amplitude and Max torque frequency |
| EPS ECU - Lane Keeping Assistant Safety Functionality | This module performs lane keeping assistant functionality and ensure steering torque request is not exceeding more than Max duration time |
| EPS ECU - Final Torque | Combine the driver steering torque request and LKA/LDW torque request to send it to the motor controlling steering |
| Motor | Motor provides steering torque to the steering wheel based on the amplitude received from the Electronic Power steering ECU |

# 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 | 50ms | LDW Safety | LDW torque amplitude request 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 | 50ms | LDW Safety | LDW torque amplitude request 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 | LDW torque amplitude request set to zero |
| Technical Safety Requirement 04 | The validity and integrity of the data transmission for 'LDW_Torque_Request' signal shall be ensured. | C | 50ms | LDW Safety | LDW torque amplitude request 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 | Data Transmission Integrity Check | LDW torque amplitude request 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 amplitude of the 'LDW_Torque_Request' sent to the 'Final electronic power steering Torque' component is below 'Max_Torque_Frequency. | C | 50ms | LDW Safety | LDW torque frequency request 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 | 50ms | LDW Safety | LDW torque frequency request 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 | LDW torque frequency request set to zero |
| Technical Safety Requirement 04 | The validity and integrity of the data transmission for 'LDW_Torque_Request' signal shall be ensured. | C | 50ms | LDW Safety | LDW torque frequency request |

| | | | | | |
|---|---|---|---|---|---|
| | | | | | set to zero |
| Technical Safety Requirement 05 | Memory test shall be conducted at startup of the EPS ECU to check for any faults in memory. | A | Ignition cycle | Data Transmission Integrity Check | LDW torque frequency request 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 | | |

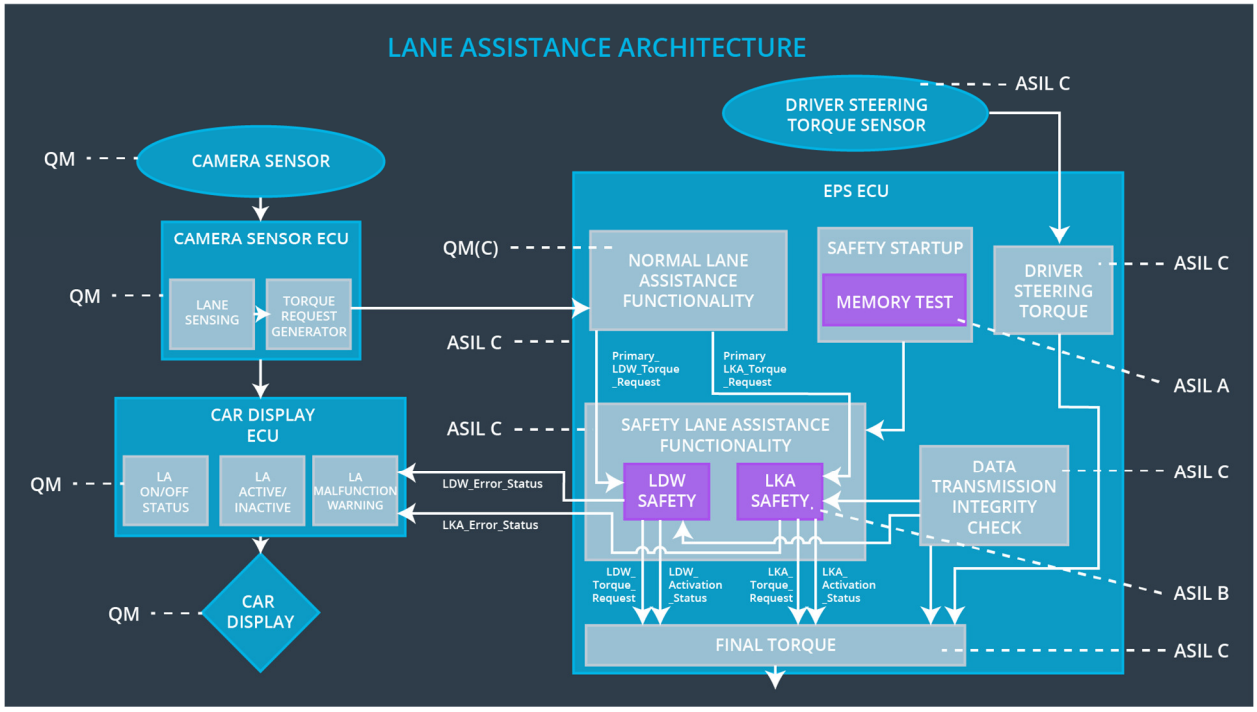
Technical Safety Requirements related to Functional Safety Requirement 02-01 are:

| ID | Technical Safety Requirement | ASIL | Fault Tolerant Time Interval | Allocation to Architecture | Safe State |
|---|---|---|---|---|---|
| Technical Safety Requirement 01 | The LKA safety component shall ensure that the amplitude of the 'LKA_Torque_Request' sent to the 'Final electronic power steering Torque' component is below 'Max_Torque_Amplitude. | B | 500ms | LKA Safety | LKA torque request set to zero |
| Technical Safety Requirement 02 | 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 | LKA torque request set to zero |
| Technical | As soon as a failure is detected | B | 500ms | LKA Safety | LKA torque |

| | | | | | |
|---|---|---|---|---|---|
| Safety Requirement 03 | by the LKA function, it shall deactivate the LKA feature and the 'LKA_Torque_Request' shall be set to zero. | | | | request set to zero |
| Technical Safety Requirement 04 | The validity and integrity of the data transmission for 'LKA_Torque_Request' signal shall be ensured. | B | 500ms | LKA Safety | LKA torque request 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 | Data Transmission Integrity Check | LKA torque request set to zero |

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

# Refinement of the System Architecture



## Allocation of Technical Safety Requirements to Architecture Elements

All The Technical Safety Requirements like LDW (Lane Departure Warning) Safety, LKA (Lane Keeping Assistance) Safety and memory are assigned to the EPS ECU (Fig. 2)

## Warning and Degradation Concept

| ID | Degradation Mode | Trigger for Degradation Mode | Safe State invoked? | Driver Warning |
|---|---|---|---|---|
| WDC-01 | Lane Departure Functionality set to zero | Malfunction_01, Malfunction_02 | Yes | Lane Departure Malfunction warning on display |
| WDC-02 | Lane Keeping Assistance Functionality set to zero | Malfunction_03 | Yes | Lane Keeping Assistance Malfunction warning on display |