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 |
|---|---|---|---|
| 3/15/2018 | 1.0 | David Simon | First Attempt |
| 3/22/2018 | 2.0 | David Simon | Remove instructions, format |
| 3/23/2018 | 3.0 | David Simon | Source content – Udacity lectures, revise functional safety requirements |
| | | | |
| | | | |

# Table of Contents

# Purpose of the Technical Safety Concept

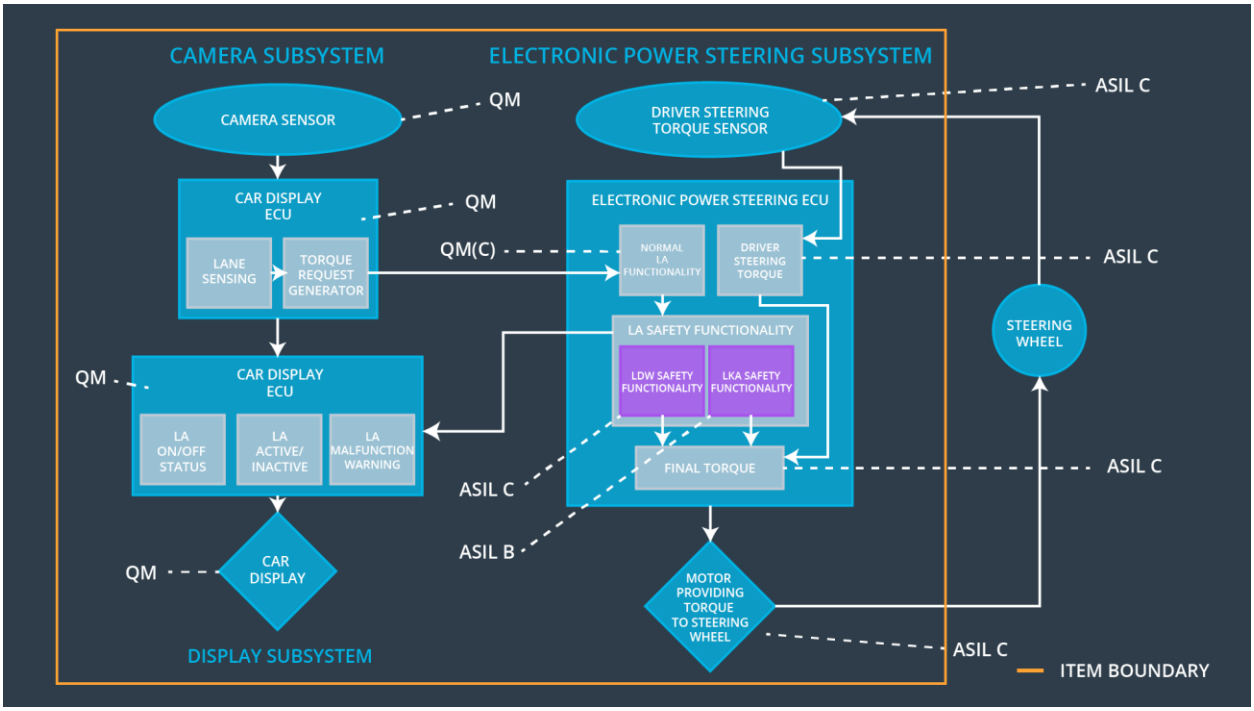
The Technical Safety Concept details the hardware and software elements needed to satisfy the functional safety requirements.

# 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 oscillating torque amplitude is below Max_Torque_Amplitude. | C | 50 msec | LDW off |
| Functional Safety Requirement 01-02 | The electronic power steering ECU shall ensure that the lane departure oscillating torque frequency is below Max_Torque_Frequency. | C | 50 msec | LDW off |
| 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 | 500 msec | LKA off |

# Refined System Architecture from Functional Safety Concept




## Functional overview of architecture elements

| Element | Description |
|---|---|
| Camera Sensor | Detects car location relative to lane lines |
| Camera Sensor ECU - Lane Sensing | Processes car location for input to torque request generator |
| Camera Sensor ECU - Torque request generator | Generates torque request to normal lane assistance block of electronic power steering ECU |
| Car Display | Notify driver of operation of lane departure warning |

| | |
|---|---|
| | and lane keeping assistance systems |
| Car Display ECU - Lane Assistance On/Off Status | Displays on/off status as set by driver |
| Car Display ECU - Lane Assistant Active/Inactive | Light displays when lane assistance is active |
| Car Display ECU - Lane Assistance malfunction warning | Displays malfunction warning light from error status generated by Lane Assistance safety block within electronic power steering ECU |
| Driver Steering Torque Sensor | Senses application of torque to steering wheel for lane departure warning and lane keeping assistance |
| Electronic Power Steering (EPS) ECU - Driver Steering Torque | Sends driver steering torque to final torque block |
| EPS ECU - Normal Lane Assistance Functionality | Sends primary torque request to lane assistance safety block |
| EPS ECU - Lane Departure Warning Safety Functionality | Checks primary torque from normal lane assistance for maximum torque and maximum frequency |
| EPS ECU - Lane Keeping Assistant Safety Functionality | Checks primary torque from normal lane assistance for maximum time duration |
| EPS ECU - Final Torque | Sends final torque to motor after clearance from lane assistance safety |
| Motor | Provides torque to steering wheel for lane departure warning and lane keeping assistance |

# 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 msec | LDW Safety | LDW Torque Request Amplitude shall be set to zero. |

| | | | | | |
|---|---|---|---|---|---|
| Technical Safety Requirement 02 | The validity and integrity of the data transmission for 'LDW_Torque_Request' signal shall be ensured. | C | 50 msec | Data Transmission Integrity Check | LDW 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 | 50 msec | LDW Safety | LDW 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 | 50 msec | LDW Safety | LDW Torque Request Amplitude shall be 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 | Memory Test | LDW 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 | The LDW safety component shall | C | 50 msec | LDW Safety | LDW |

| | | | | | |
|---|---|---|---|---|---|
| Safety Requirement 01 | ensure that the frequency of the ‘LDW Torque Request’ sent to the ‘Final electronic power steering Torque’ is below ‘Max_Torque_Frequency.’ | | | | Torque Request Amplitude shall be set to zero. |
| Technical Safety Requirement 02 | The validity and integrity of the data transmission for ‘LDW_Torque_Request’ signal shall be ensured. | C | 50 msec | Data Transmission Integrity Check | LDW 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 | 50 msec | LDW Safety | LDW 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 | 50 msec | LDW Safety | LDW Torque Request Amplitude shall be 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 | Memory Test | LDW Torque Request Amplitude shall be set to zero. |

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

**[OPTIONAL: For each technical safety requirement, identify both the verification and validation acceptance criteria. “Validation” asks whether or not you chose the appropriate parameters. “Verification” involves testing to make sure the vehicle behaves as expected when the parameter value is crossed. There is not necessarily one right**

**answer. Look at your verification and validation acceptance criteria from the functional safety concept for inspiration.]**

**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:

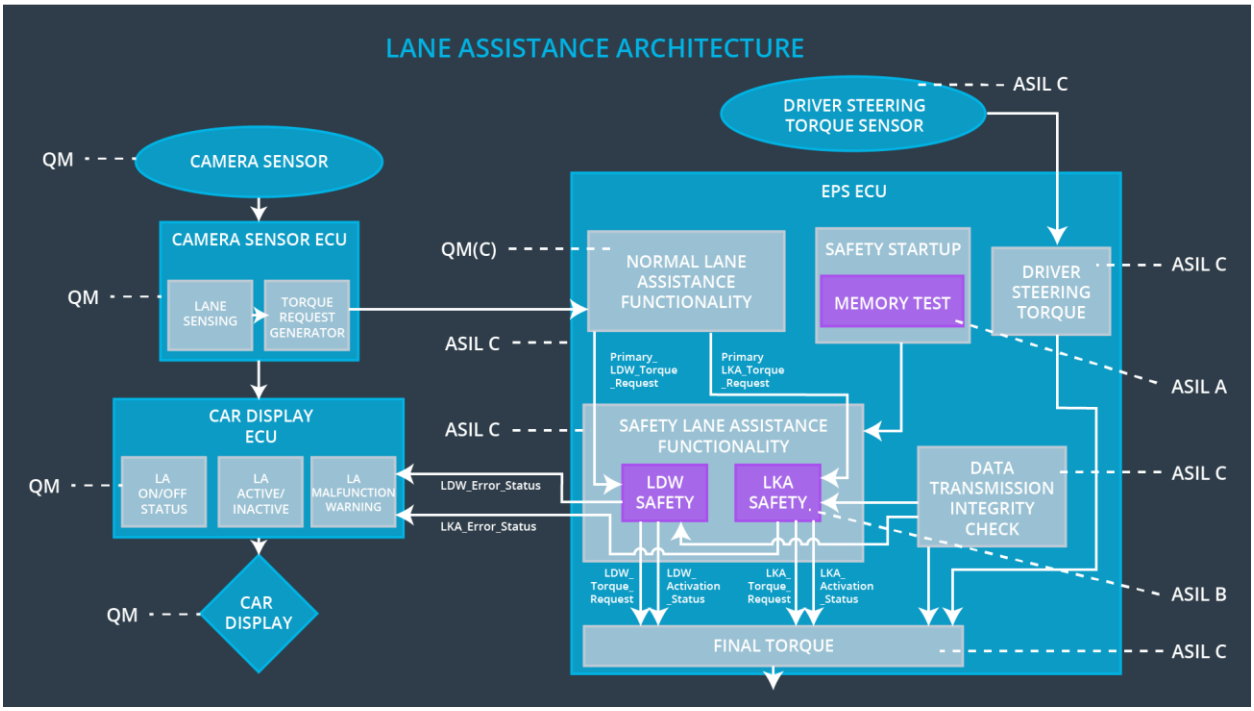
| ID | Technical Safety Requirement | ASIL | Fault Tolerant Time Interval | Allocation to Architecture | Safe State |
|---|---|---|---|---|---|
| Technical Safety Requirement 01 | The LKA safety component shall ensure that the time duration of the 'LKA Torque Request' sent to the 'Final electronic power steering Torque' is below 'Max_Duration.' | B | 500 msec | LKA Safety | LKA Torque Request Amplitude shall be set to zero. |
| Technical Safety Requirement 02 | The validity and integrity of the data transmission for 'LKA_Torque_Request' signal shall be ensured. | B | 500 msec | Data Transmission Integrity Check | LKA Torque Request Amplitude shall be set to zero. |
| Technical Safety | As soon as a failure is detected by the LKA function, it shall | B | 500 msec | LKA Safety | LKA Torque Request |

| | | | | | |
|---|---|---|---|---|---|
| Requirement 03 | deactivate the LKA feature and the LKA_Torque_Request shall be set to zero. | | | | Amplitude 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 | 500 msec | LKA Safety | LKA Torque Request Amplitude shall be 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 | Memory Test | LKA Torque Request Amplitude shall be set to zero. |

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

**[OPTIONAL: For each technical safety requirement, identify both the verification and validation acceptance criteria. "Validation" asks whether or not you chose the appropriate parameters. "Verification" involves testing to make sure the vehicle behaves as expected when the parameter value is crossed. There is not necessarily one right answer. Look at your verification and validation acceptance criteria from the functional safety concept for inspiration.]**

## 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 | LDW off | Malfunction 01 Too high Amplitude<br><br>Malfunction 02 Too high Frequency | Yes | LDW error light, LDW operation light off |
| WDC-02 | LKA off | Malfunction 03 Max Time Duration Exceeded | Yes | LKA error light, LKA operation light off |