Elektrobit

UDACITY

# Technical Safety Concept Lane Assistance

**Document Version: 1.0**
**08-25-2017**

# Document History

| Date | Version | Editor | Description |
|---|---|---|---|
| 08-25-2017 | 1.0 | Neil Hiddink | Technical Safety Concept for Lane Assistance Functionality. |
| | | | |
| | | | |
| | | | |
| | | | |

# Table of Contents


Document history
Table of Contents
Purpose of the Technical Safety Concept
Inputs to the Technical Safety Concept
    Functional Safety Requirements
    Refined System Architecture from Functional Safety Concept
        Functional overview of architecture elements
Technical Safety Concept
    Technical Safety Requirements
    Refinement of the System Architecture
    Allocation of Technical Safety Requirements to Architecture Elements
    Warning and Degradation Concept

# Purpose of the Technical Safety Concept

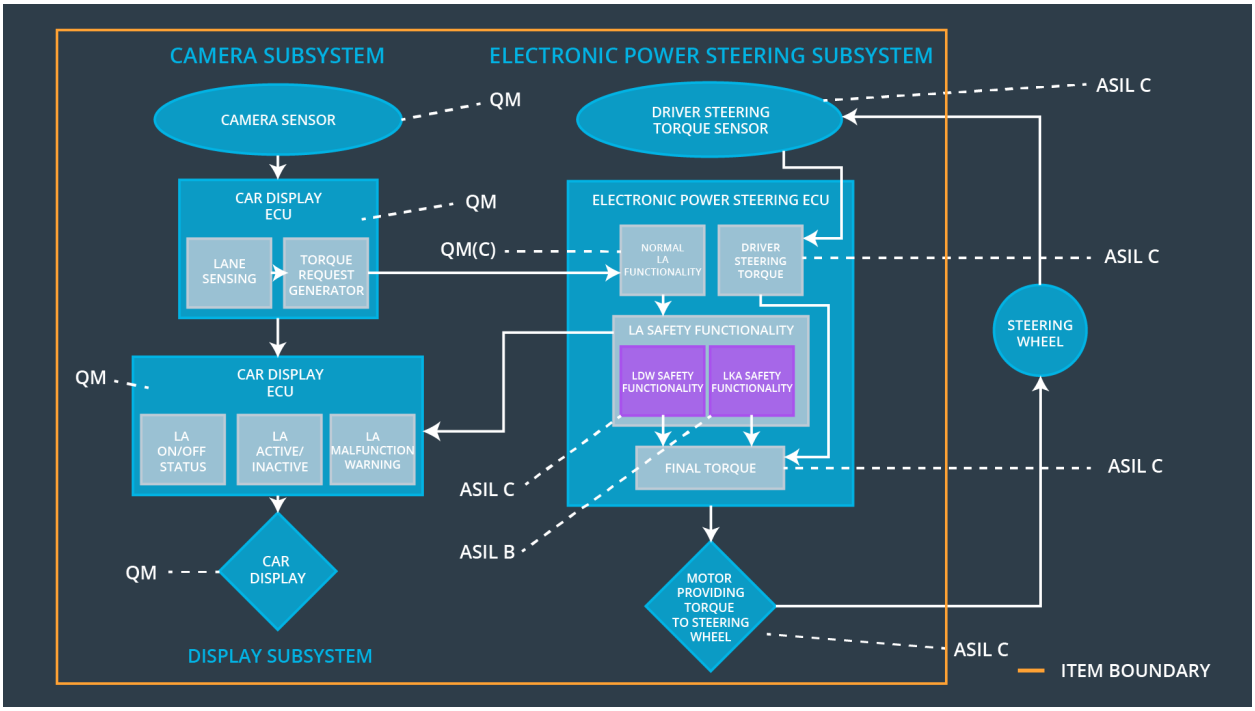
The purpose of this technical safety concept is to provide a detailed overview of the Lane Assistance item's technologies as of the product development phase of its life cycle, presented at the system level.

# 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 EPS ECU shall ensure that the lane departure warning oscillating torque amplitude is below Max_Torque_Amplitude | C | 50 ms | Turn Off System |
| Functional Safety Requirement 01-02 | The EPS ECU shall ensure that the lane departure warning oscillating torque frequency is below Max_Torque_Frequency. | C | 50 ms | Turn Off System |
| Functional Safety Requirement 02-01 | The EPS ECU shall ensure that the lane keeping assistance torque is applied for only Max_Duration. | B | 500 ms | Turn Off System |

# Refined System Architecture from Functional Safety Concept




## Functional Overview of Architecture Elements

| Element | Description |
|---|---|
| Camera Sensor | A sensor (or array of sensors) mounted on the front of the vehicle that collects image and video data. |
| Camera Sensor ECU - Lane Sensing | A computer that warning messages for the car display ECU by interpreting the data collected by the camera sensor. |
| Camera Sensor ECU - Torque request generator | A computer that handles steering corrections for the power steering ECU by interpreting the data collected by the camera sensor. |
| Car Display | A physical display component mounted inside the vehicle that provides visual feedback to the driver. |
| Car Display ECU - Lane Assistance On/Off Status | A computer within the car display component that is responsible for relaying the ON/OFF status of the Lane Assistance item to the driver as received from the camera sensor ECU. |

## Functional Overview of Architecture Elements (Cont.)

| Element | Description |
|---|---|
| Car Display ECU - Lane Assistant Active/Inactive | A computer within the car display component that is responsible for relaying warning messages to the driver as received from the camera sensor ECU. |
| Car Display ECU - Lane Assistance malfunction warning | A computer within the car display component that is responsible for relaying a message that alerts the driver that a malfunction has occurred as received from the camera sensor ECU. |
| Driver Steering Torque Sensor | A sensor that measures the torque applied to the steering wheel by the driver. |
| Electronic Power Steering (EPS) ECU - Driver Steering Torque | A computer within the power steering column that converts torque applied by the driver to appropriate steering actions for the vehicle. |
| EPS ECU - Normal Lane Assistance Functionality | A computer within the power steering column that is responsible for controlling the torque applied to the steering wheel when the Lane Assistance functionality is operating normally in response to an under- and/or over-compensation of torque by the driver. |
| EPS ECU - Lane Departure Warning Safety Functionality | A computer within the power steering column that is responsible for relaying a signal to the car display ECU to warn the driver that they are departing the current lane. |
| EPS ECU - Lane Keeping Assistant Safety Functionality | A computer within the power steering column that is responsible for oscillating the torque applied to the steering wheel to produce a warning haptic or vibration in response to an under- and/or over-compensation of torque by the driver. |
| EPS ECU - Final Torque | A computer within the power steering column that converts torque calculated by the Lane Assistance functionality to return to the center of the current lane to appropriate steering actions for the vehicle. |
| Motor | The component responsible for applying the work required to produce the torque required to execute actions delivered to the 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 | ✓ | | |

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 | EPS ECU LDW Safety Functionality | Turn Off System |
| 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 | EPS ECU LDW Safety Functionality | Turn Off System |

Technical Safety Requirements related to Functional Safety Requirement 01-01 (Cont.)

| ID | Technical Safety Requirement | ASIL | Fault Tolerant Time Interval | Architecture Allocation | Safe State |
|---|---|---|---|---|---|
| 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 | EPS ECU LDW Safety Functionality | Turn Off System |
| 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 | Turn Off System |
| 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 | EPS ECU Memory Test | Turn Off System |

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 | ✓ | | |

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 EPS Torque component is below Max_Torque_Frequency. | C | 50 ms | EPS ECU LDW Safety Functionality | Turn Off System |
| Technical Safety Requirement 02 | As soon as the LDW function deactivates the LDW feature, the LDW Safety software block shall send a LDW_Error_Status to the car display ECU to turn on a warning light. | C | 50 ms | EPS ECU LDW Safety Functionality | Turn Off System |
| 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 | EPS ECU LDW Safety Functionality | Turn Off System |
| 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 | Turn Off System |
| 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 | EPS ECU Memory Test | Turn Off System |

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

| ID | Validation Acceptance Criteria and Method | Verification Acceptance Criteria and Method |
|---|---|---|
| Technical Safety Requirement 01 | Collect a series of LDW_Torque_Request values sent to the Final EPS Torque component to ensure they are below maximum values. | The collected LDW_Torque_Request values sent to the Final EPS Torque component are below maximum values. |
| Technical Safety Requirement 02 | Test to prove signals are sent to ECU to request a warning light. | A warning light appears as soon as the LDW function deactivates the LDW feature. |
| Technical Safety Requirement 03 | Test to prove signals are sent to the ECU to request a zero torque. | The applied torque is reduced to zero as soon as the function deactivates the LDW feature. |
| Technical Safety Requirement 04 | Test to prove out that the connection for data transfer is constant and reliable. | Data is transmitted to the ECU at a predictable rate. |
| Technical Safety Requirement 05 | Test for the presence of memory faults. | There are no memory faults during operation. |

**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. | ✓ | | |

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

| ID | Technical Safety Requirement | ASIL | Fault Tolerant Time Interval | Architecture Allocation | Safe State |
|---|---|---|---|---|---|
| Technical Safety Requirement 01 | The LKA Safety component shall ensure that the time elapsed following the receipt of an LKA_Torque_Request sent to the Final EPS Torque component is below Max_Duration. | B | 500 ms | EPS ECU LDW Safety Functionality | Turn Off System |
| Technical Safety Requirement 02 | As soon as a failure is detected by the LKA function, it shall deactivate the LKA feature and the LKA_Error_Status shall update the car display to display a malfunction warning light. | B | 500 ms | EPS ECU LDW Safety Functionality | Turn Off System |

Technical Safety Requirements related to Functional Safety Requirement 02-01 (Cont.):

| ID | Technical Safety Requirement | ASIL | Fault Tolerant Time Interval | Architecture Allocation | Safe State |
|---|---|---|---|---|---|
| Technical Safety Requirement 03 | As soon as the LKA function deactivates the LKA feature, the LKA Safety software block shall send an LKA_Activation_Status to the car display ECU to set the item to inactive status. | B | 500 ms | EPS ECU LDW Safety Functionality | Turn Off System |
| Technical Safety Requirement 04 | The validity and integrity of the data transmission for the LKA Safety software block shall be ensured. | B | 500 ms | Data Transmission Integrity Check | Turn Off System |
| 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 | EPS ECU Memory Test | Turn Off System |

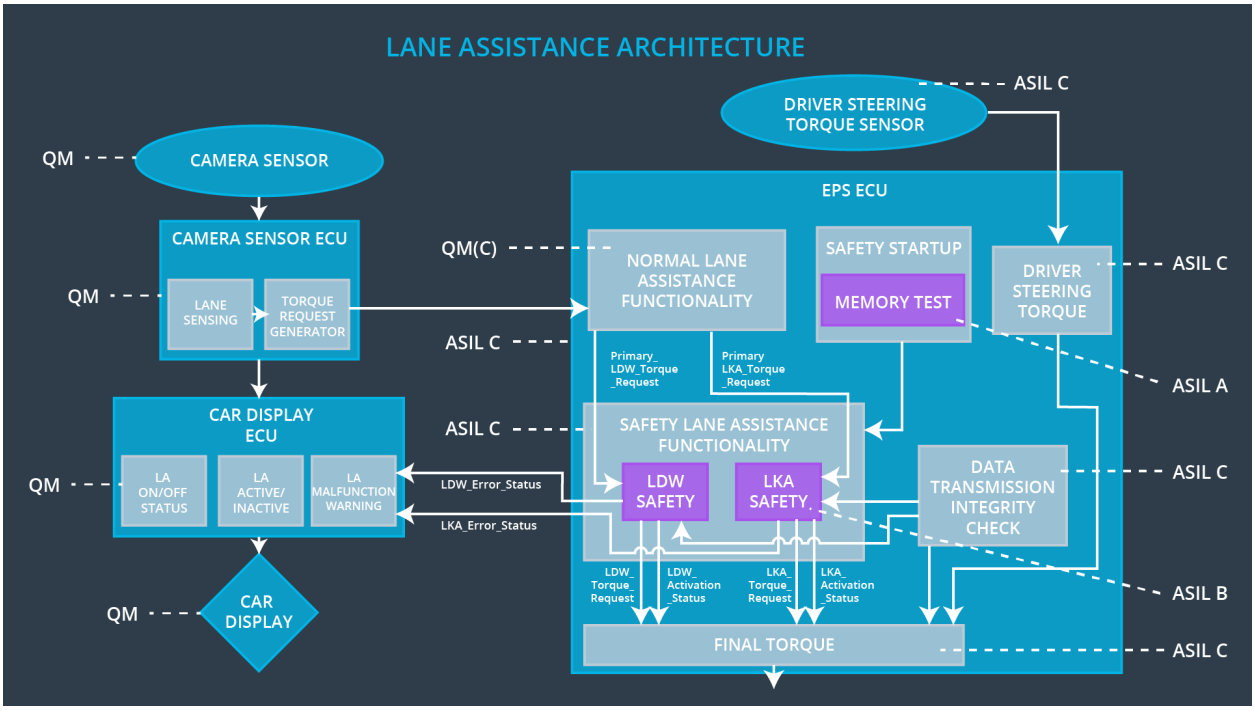
**Lane Keeping Assistance (LKA) Verification and Validation Acceptance Criteria:**

| ID | Validation Acceptance Criteria and Method | Verification Acceptance Criteria and Method |
|---|---|---|
| Technical Safety Requirement 01 | Collect a series of LKA_Torque_Request values sent to the Final EPS Torque component to ensure they are below maximum values. | The collected LKA_Torque_Request values sent to the Final EPS Torque component are below maximum values. |
| Technical Safety Requirement 02 | Test to prove signals are sent to ECU to request a warning light. | A warning light appears as soon as the LKA function deactivates the LKA feature. |
| Technical Safety Requirement 03 | Test to prove signals are sent to the ECU to request inactivity. | The applied torque is reduced to zero as soon as the function deactivates the LKA feature. |

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

| ID | Validation Acceptance Criteria and Method | Verification Acceptance Criteria and Method |
|---|---|---|
| Technical Safety Requirement 04 | Test to prove out that the connection for data transfer is constant and reliable. | Data is transmitted to the ECU at a predictable rate. |
| Technical Safety Requirement 05 | Test for the presence of memory faults. | There are no memory faults during operation. |

## Refinement of the System Architecture




## Allocation of Technical Safety Requirements to Architecture Elements

For the Lane Assistance item, all technical safety requirements are allocated to the Electronic Power Steering ECU. For further details, please refer to the preceding technical safety requirements tables.

# Warning and Degradation Concept

For the Lane Assistance item, the warning and degradation concept is the same for the technical safety requirements as for the functional safety requirements, as shown below:

| ID | Degradation Mode | Trigger for Degradation Mode | Safe State Invoked? | Driver Warning |
|---|---|---|---|---|
| WDC-01 | Turn off the functionality. | Malfunction_01<br><br>Malfunction_02 | Yes | Car Display |
| WDC-02 | Turn off the functionality. | Malfunction_03 | Yes | Car Display |