# Technical Safety Concept Lane Assistance

**Document Version:** [Version]

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

# Document history

| Date | Version | Editor | Description |
|---|---|---|---|
| 24/05/2018 | 1.0 | Krishna | 1st Version of Technical Safety Concept |
| 25/05/2018 | 2.0 | Krishna | 2nd Version of Technical Safety Concept |
| | | | |
| | | | |
| | | | |

# Table of Contents



# Purpose of the Technical Safety Concept

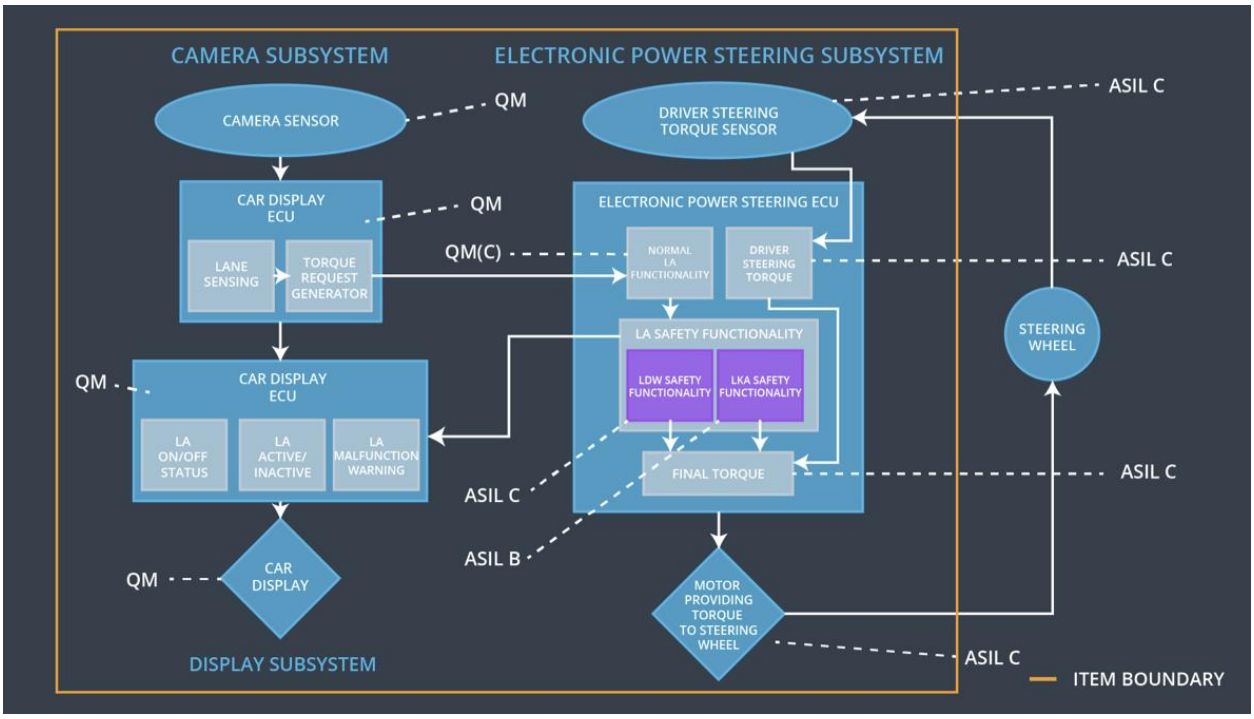
The main purpose of Technical Safety is to identify new requirements and allocate them to the system for lowering risk. In the Technical safety concept, we think of sensors, control units and actuators. In contrast to Functional Safety requirements, which deals with requirements from a perspective of higher level, the Technical safety requirements are general hardware and software requirements but still without getting into specific details.

# 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 keeping item shall ensure that the lane departure oscillating torque amplitude is below Max_Torque_Amplitude | C | 50 mS | The LDW torque amplitude should be below Max_Torque_Amplitude and if fault occurs its value should be set to zero |
| Functional Safety Requirement 01-02 | The lane keeping item shall ensure that the lane departure oscillati9ng torque frequency ids below Max_Torque_Frequency | C | 50 mS | The LDW torque frequency should be below Max_Torque_Frequency and if fault occurs its value should be set to zero |
| 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 mS | Lane Keeping Assistance System torque should be set to zero. |

# Refined System Architecture from Functional Safety Concept




## Functional overview of architecture elements

| Element | Description |
|---|---|
| Camera Sensor | It takes visual feedback for the lane detection. It captures images and feeds the images to the Camera Sensor ECU |
| Camera Sensor ECU - Lane Sensing | It analyses the camera images using computer vision or some other techniques. It determines whether the car is going out of the lane. |
| Camera Sensor ECU - Torque request generator | Generates a torque request to the power steering ECU |
| Car Display | It displays whether the lane keeping and departure assistance system is on/off. So, basically it is a visual feedback for the driver. |

| | |
|---|---|
| Car Display ECU - Lane Assistance On/Off Status | Receives a signal from the power steering ECU to determine the status of the Lane Assistance System whether it is on/off. |
| Car Display ECU - Lane Assistant Active/Inactive | Receives a signal from the power steering ECU to determine the status of the Lane Assistance System whether it is active/inactive and sends the signal to display |
| Car Display ECU - Lane Assistance malfunction warning | Receives a signal from the power steering ECU to determine whether there is a malfunction in the Lane Assistance System |
| Driver Steering Torque Sensor | Detects the amount of torque provided on the steering |
| Electronic Power Steering (EPS) ECU - Driver Steering Torque | Processes the data coming from the Driver Steering Torque Sensor |
| EPS ECU - Normal Lane Assistance Functionality | Receives torque request from Camera sensor ECU |
| EPS ECU - Lane Departure Warning Safety Functionality | Ensures that the vibrational torque and frequency during lane departure is below the Maximum Torque and Maximum Frequency respectively |
| EPS ECU - Lane Keeping Assistant Safety Functionality | Ensures that the Lane Keeping Assistance Function is not active more than Max_duration time. |
| EPS ECU - Final Torque | Combines the torque from the Lane Keeping Assistance and Lane Departure system and sends it to motor |
| Motor | Receives the torque signal from the EPS ECU and rotates the steering wheel accordingly |

# 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 | LDW torque request amplitude is 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 | LDW Safety | LDW torque request amplitude is 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 ms | LDW Safety | LDW torque request amplitude is set 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 | Data Transmission Integrity Check | N/A |
| Technical Safety | Memory test shall be conducted at start-up of the EPS ECU to | A | Ignition Cycle | Memory Test | LDW torque request |

| | | | | | |
|---|---|---|---|---|---|
| Requirement 05 | check for any faults in memory. | | | | amplitude is 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 frequency of the 'LDW_Torque_Request' sent to the 'Final electronic power steering Torque' component is below 'Max_Torque_Frequency+ | C | 50 ms | LDW Safety | LDW torque request amplitude is 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 | LDW Safety | LDW torque request amplitude is set to zero |
| Technical Safety | As soon as a failure is detected by the LDW function, it shall deactivate | C | 50 ms | LDW Safety | LDW torque |

| | | | | | |
|---|---|---|---|---|---|
| Requirement 03 | the LDW feature and the 'LDW_Torque_Request' shall be set to zero. | | | | request amplitude is set 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 | Data Transmission Integrity Check | N/A |
| 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 is set to zero |

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

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

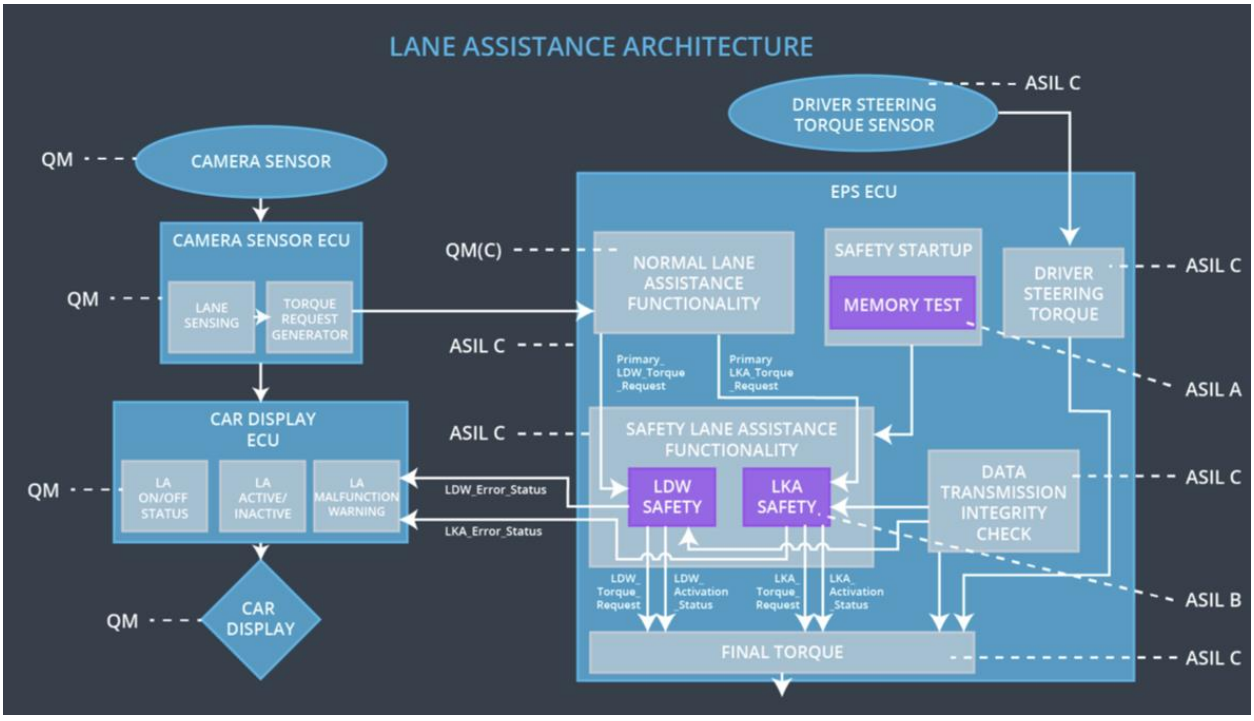
| ID | Functional Safety Requirement | Electronic Power Steering ECU | Camera ECU | Car Display ECU |
|---|---|---|---|---|
| Functional Safety Requirement 02-01 | The lane keeping item shall ensure that the lane keeping assistance torque is applied for only Max_Duration | X | | |

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 system shall ensure that the duration of LKA_Torque_Request sent to the final electronic power steering torque is below the Max_Duration. | B | 500 ms | LKA safety | LKA torque request is 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 | 500 ms | LKA safety | LKA torque request is 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 | 500 ms | LKA safety | LKA torque request is set to zero |
| Technical Safety Requirement 04 | The validity and integrity of the data transmission for 'LKA_Torque_Request' signal shall be ensured. | B | 500 ms | Data Transmission Integrity Check | N/A |
| 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 is set to zero |

## 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. For more details on the allocation of the EPS ECU, check the tables above.

## Warning and Degradation Concept

The warning and degradation concept for Technical Safety is the same as the Functional Safety requirements. The Warning and Degradation concept for the Lane Departure and Lane Assistance System are given in the below table:

| ID | Degradation Mode | Trigger for Degradation Mode | Safe State invoked? | Driver Warning |
|---|---|---|---|---|
| WDC-01 | Turn off the functionality | The malfunction of steering wheel vibrating too high or with more frequency | Yes | Display will show the warning light on |
| WDC-02 | Turn off the functionality | The malfunction of lane keeping assistance applied for long duration | Yes | Display will show the warning on |