# Technical Safety Concept Lane Assistance

# Document history

| Date | Version | Editor | Description |
|---|---|---|---|
| Jan 5th 2018 | 1.0 | Tarun Kandala | First draft/submission |
| Jan 6th 2018 | 1.1 | Tarun Kandala | Revised based on feedback |
| | | | |
| | | | |
| | | | |

# Table of Contents

# Purpose of the Technical Safety Concept

A technical safety concept, part of the product development phase, is more concrete and gets into the details of the item's technology when compared to a Functional safety concept.

# 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 | B | 50ms | LDW Torque Request Amplitude shall be set to zero |
| Functional Safety Requirement 01-02 | The lane keeping item shall ensure that the lane departure oscillating torque frequency is below Max_Torque_Frequency | B | 50ms | LDW Torque Request Frequency shall 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 | 500ms | LKA Torque Request shall be set to zero |

# Refined System Architecture from Functional Safety Concept
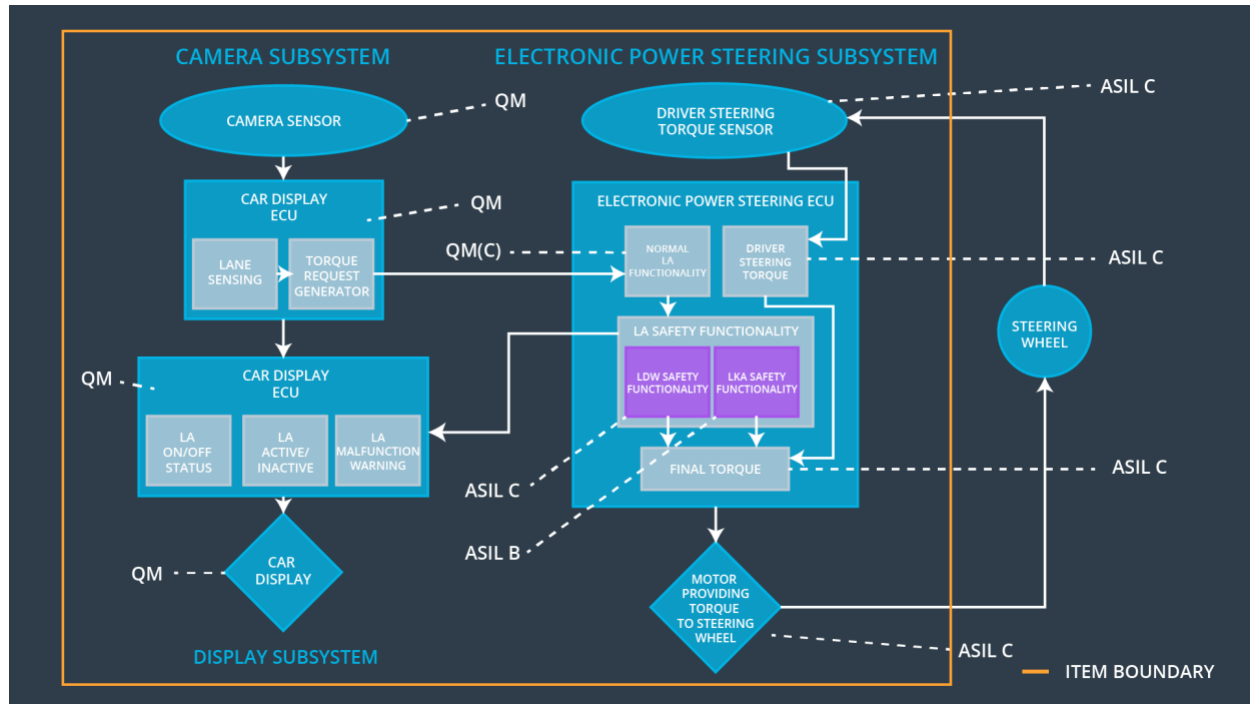


## Functional overview of architecture elements

| Element | Description |
|---|---|
| Camera Sensor | Captures lanes data |
| Camera Sensor ECU - Lane Sensing | Detects any lane changes |
| Camera Sensor ECU - Torque request generator | Sends required torque requests to bring the car back to ego lane |
| Car Display | Displays warnings or any other alerts to the driver |
| Car Display ECU - Lane Assistance On/Off Status | Shows the status of the Lane Assistance function |
| Car Display ECU - Lane Assistant Active/Inactive | Shows the status of the Lane Assistance function's current active status – if lane assistance is triggered or not |
| Car Display ECU - Lane Assistance malfunction warning | Shows if there is a malfunction in the Lane Assistance function |

| | |
|---|---|
| Driver Steering Torque Sensor | Gets the current torque applied by the driver |
| Electronic Power Steering (EPS) ECU - Driver Steering Torque | Calculates the amount of torque applied by the driver |
| EPS ECU - Normal Lane Assistance Functionality | Calculates the amount of torque generated by the Camera Sensor ECU - Torque request generator and makes sure it is within torque limits |
| EPS ECU - Lane Departure Warning Safety Functionality | Monitors the oscillating torque applied to the steering and makes sure it is within set limits |
| EPS ECU - Lane Keeping Assistant Safety Functionality | Monitors any misuse by the driver as an autonomous mode and restricts the time the LKA is applied |
| EPS ECU - Final Torque | Applies the final required torque with inputs from EPS ECU - Normal Lane Assistance Functionality and EPS ECU - Driver Steering Torque |
| Motor | Applies final torque to the steering wheel |

# 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 Software component | LDW Torque Request Amplitude shall be 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 Software component | 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 ms | LDW Safety Software component | LDW Torque Request Amplitude shall be 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 software block | 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 | External Safety Startup Memory Test software block | 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 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 | 50 ms | LDW Safety Software component | LDW Torque Request Frequency shall be 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 Software component | LDW Torque Request Frequency 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 ms | LDW Safety Software component | LDW Torque Request Frequency shall be 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 software block | 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 | External Safety Startup Memory Test software block | LDW Torque Request Frequency 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:**

[Instructions: Fill in the technical safety requirements for the lane keeping assistance functional safety requirement 02-01. We have provided the associated functional safety requirement in the table below. Hint:. You can reuse the technical safety requirements from functional safety requirement 01-01. But you need to change the language because we are now looking at a different system. The ASIL and Fault Tolerant Time Interval are different as well.]

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 | A | Fault | Allocation to | Safe State |
|---|---|---|---|---|---|

| | | S I L | Tolerant Time Interval | Architecture | |
|---|---|---|---|---|---|
| Technical Safety Requirement 01 | The LKA safety component shall ensure that the Torque of the 'LKA_Torque_Request' sent to the 'Final electronic power steering Torque' component is applied for only 'Max_Duration'. | B | 500 ms | LKA Safety Software component | LKA Torque Request shall be 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 Software component | LKA Torque Request shall be 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 Software component | LKA Torque Request shall be 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 software block | 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 | External Safety Startup Memory Test software block | LKA Torque Request 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
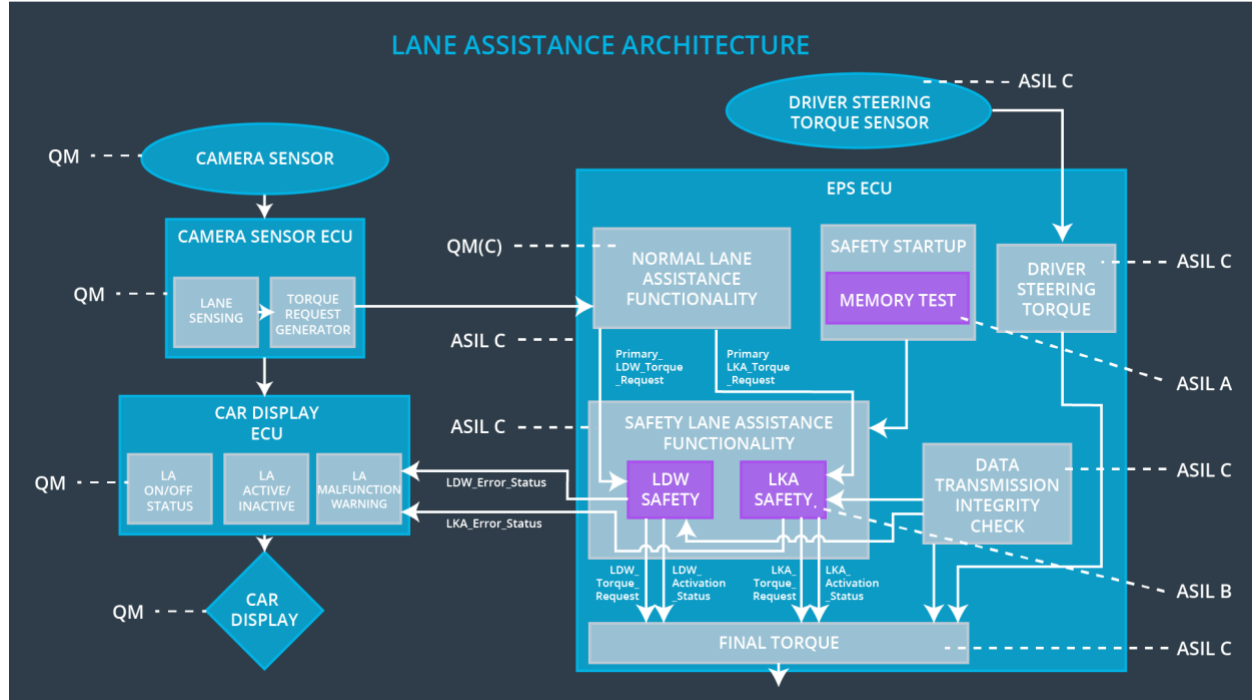


# Allocation of Technical Safety Requirements to Architecture Elements

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 | Turn off Lane Departure warning function | When the oscillating torque amplitude and frequency go beyond limit | Yes | The driver will see a warning light on the dashboard when the system malfunctions |
| WDC-02 | Turn off Lane Keeping assistance function | When the lane keeping assistance goes beyond the set time limit | Yes | The driver will see a warning light on the dashboard when the system malfunctions |