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 |
|---|---|---|---|
| 03/15/2019 | 1.0 | Akshat Yadav | Initial draft |
| 03/18/2019 | 2.0 | Akshat Yadav | Changes after first review. |
| | | | |
| | | | |
| | | | |

# Table of Contents

# Purpose of the Technical Safety Concept

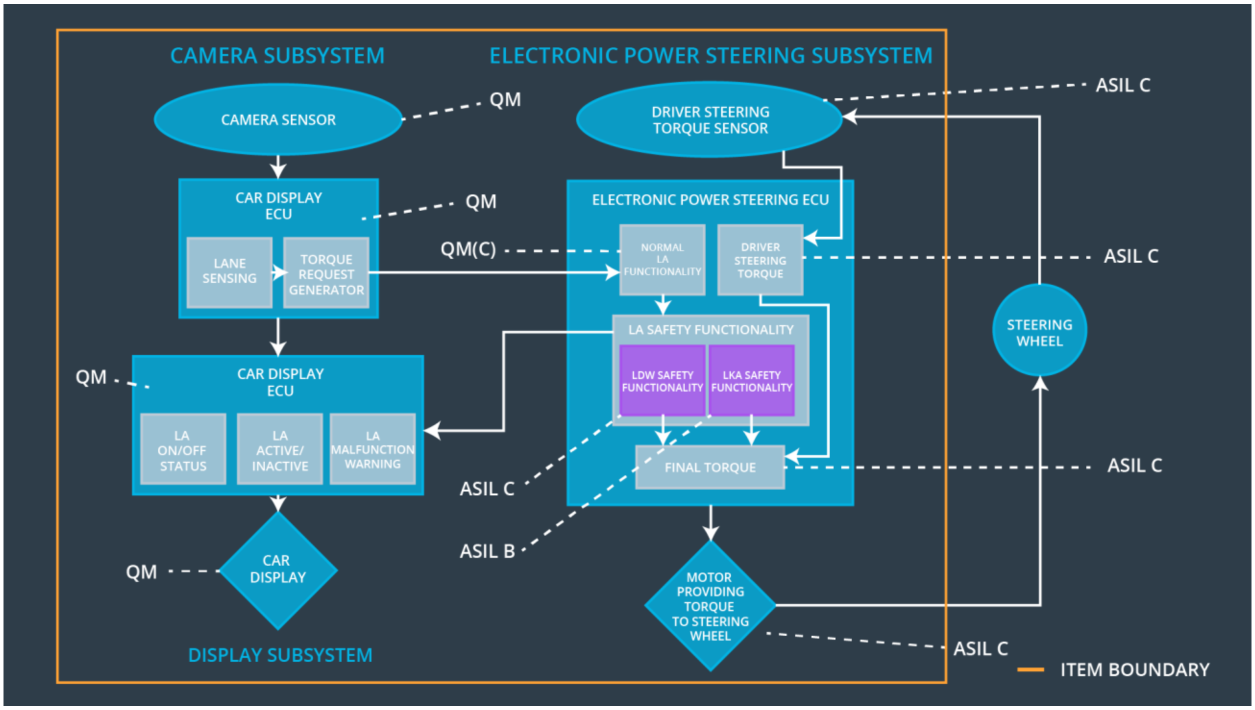
The purpose of the technical safety concept is to specify the realization of the defined functional safety concept and assign them to the system architecture.

# 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 item shall ensure that the lane departure oscillating torque amplitude is below Max_Torque_Amplitude. | C | 50 ms | Vibration torque amplitude below Max_Torque_Amplitude. |
| Functional Safety Requirement 01-02 | The Lane Departure Warning item shall ensure that the lane departure oscillating torque frequency is below Max_Torque_Frequency. | C | 50 ms | Vibration frequency is below Max_Torque_Frequency. |
| Functional Safety Requirement 02-01 | The electronic power steering ECU shall ensure that the Lane Keeping Assistance torque is applied only Max_Duration. | B | 50ms | Lane Keeping Assistance torque is zero. |

# Refined System Architecture from Functional Safety Concept



## Functional overview of architecture elements

| Element | Description |
|---|---|
| Camera Sensor | Capture road images and provide them to the Camera Sensor ECU. |
| Camera Sensor ECU - Lane Sensing | Software Module in the Camera Sensor ECU Responsible for detecting lane lines and determining when the vehicle leaves the lane by mistake.. |
| Camera Sensor ECU - Torque request generator | Software Module in the Camera Sensor ECU responsible for calculating and sending the Additional torque for the LDW and LKA functions. |
| Car Display | Visual display responsible to displaying warning of lane departures and LKA and LDW activation and deactivations. |

| | |
|---|---|
| Car Display ECU - Lane Assistance On/Off Status | Visual display responsible to displaying LKA and LDW ON/OFF status. |
| Car Display ECU - Lane Assistant Active/Inactive | Visual display responsible to displaying warning of lane departures, LKA and LDW Activation and deactivations. |
| Car Display ECU - Lane Assistance malfunction warning | Visual display responsible to displaying warning of LKA and LDW malfunctions. |
| Driver Steering Torque Sensor | Sensor responsible for measuring how much force (Steering torque) the driver is applying to the steering wheel. |
| Electronic Power Steering (EPS) ECU - Driver Steering Torque | Software Module in the electronic power steering ECU responsible for receiving the Camera Sensor ECU torque requests. |
| EPS ECU - Normal Lane Assistance Functionality | Software Module in the electronic power steering ECU responsible for receiving the Driver Steering Torque sensor input from the steering wheel. |
| EPS ECU - Lane Departure Warning Safety Functionality | Software Module in the electronic power steering ECU responsible for keeping the lane departure oscillating torque amplitude and frequency below MAX_Torque_Amplitude and MAX_Torque_Fequency respectively. |
| EPS ECU - Lane Keeping Assistant Safety Functionality | Software Module in the electronic power steering ECU responsible for ensuring the application of the lane keeping assistance torque does not ever exceeded Max_Duration and if lane detection is lost, the LKA function is deactivated. |
| EPS ECU - Final Torque | Software Module in the electronic power steering ECU responsible for ensuring the LDW, LKA and the driver’s steering torque requests are combined and sent to the Motor. |
| Motor | Actuator responsible for applying requested torque to the steering column by the Electronic Power Steering ECU for either the LKA or the LDW functions. |

# 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 01-01-01 | 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 block | Set LDW torque amplitude to zero |
| Technical Safety Requirement 01-01-02 | 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 block | Set LDW torque amplitude to zero |

| | | | | | |
|---|---|---|---|---|---|
| Technical Safety Requirement 01-01-03 | 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 block | Set LDW torque amplitude to zero |
| Technical Safety Requirement 01-01-04 | The validity and integrity of the data transmission for 'LDW_Torque_Request' signal shall be ensured. | C | 50 ms | Data Transmission Integrity Check | Set LDW torque amplitude to zero |
| Technical Safety Requirement 01-01-05 | Memory test shall be conducted at start up of the EPS ECU to check for any faults in memory. | A | Ignition cycle | Memory Test Block | Set LDW torque amplitude 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 01-02-01 | The LDW safety component shall ensure that the fequency of the 'LDW_Torque_Request' sent to the 'Final electronic power steeringTorque' component is below 'Max_Torque_Fequency. | C | 50 ms | LDW Safety block | Set LDW torque frequency to zero |

| | | | | | |
|---|---|---|---|---|---|
| Technical Safety Requirement 01-02-02 | 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 block | Set LDW torque frequency to zero |
| Technical Safety Requirement 01-02-03 | 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 block | Set LDW torque frequency to zero |
| Technical Safety Requirement 01-02-04 | The validity and integrity of the data transmission for 'LDW_Torque_Request' signal shall be ensured. | C | 50 ms | Data Transmission Integrity Check | Set LDW torque frequency to zero |
| Technical Safety Requirement 01-02-05 | Memory test shall be conducted at start up of the EPS ECU to check for any faults in memory. | A | Ignition cycle | Memory Test Block | Set LDW torque frequency to zero |

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

| ID | Validation Acceptance Criteria and Method | Verification Acceptance Criteria and Method |
|---|---|---|
| Technical Safety Requirement 01-01-01 | Validate the Max_Torque_Amplitude is the chosen from the Lane Departure Warning Validation Acceptance Criteria. | Verify the Lane Departure Warning functionality is turned off. |
| Technical Safety Requirement 01-01-02 | Validate that the “TORQUE_LIMITER” in the “LDW Safety” software block sends the error_status_torque_limiter signal to the LDW_SAFETY_ACTIVATION. | Verify the Car Display ECU displays the Lane Departure Warning malfunction warning signal. |
| Technical Safety Requirement 01-01-03 | Validate that the “TORQUE_LIMITER” in the “LDW Safety” software block sends a zero LDW_Torque_Request. | Verify the Final EPS Torque generator receives a 0 LDW_Torque_Request of zero. |

|  |  |  |
|---|---|---|
| Technical Safety Requirement 01-01-04 | Validate the ‘TORQUE_LIMITER’ calculate and sends the correct cyclic redundancy check (CRC) and Alive counter for data transmission validity and integrity. | Verify the functionality is turn off if there is a CRC or Alive counter discrepancy. |
| Technical Safety Requirement 01-01-05 | Validate the Safety Startup Memory test to check memory faults catch memory faults. | Verify the Lane Departure Warning is turned off when the Safety Startup Memory fails. |
| Technical Safety Requirement 01-02-01 | Validate the Max_Torque_Frequency set is the chosen from the Lane Departure Warning Acceptance Criteria. | Verify the functionality is turned off if the ‘LDW_Torque_Request’ frequency exceeds Max_Torque_Request. |

**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 02-01-01 | The LKA safety component shall ensure that the duration of the lane keeping assistance torque applied is less than Max_Duration. | C | 500 ms | LKA Safety Block | Set lane keeping assistance torque to zero |
| Technical | When the Lane Keeping | C | 500 ms | LKA Safety | Set lane |

| | | | | | |
|---|---|---|---|---|---|
| Safety Requirement 02-01-02 | Assistance function deactivates, the ‘LKA Safety’ shall send a signal to the Car Display ECU to turn on a warning light. | | | block | keeping assistance torque to zero |
| Technical Safety Requirement 02-01-03 | When a failure is detected, the Lane Keeping Assistance function shall deactivate and the ‘LKA_Torque_Request’ shall be zero. | C | 500 ms | LKA Safety block | Set lane keeping assistance torque to zero |
| Technical Safety Requirement 02-01-04 | The validity and integrity of the data transmission for 'LKA_Torque_Request' signal shall be ensured. | C | 500 ms | Data Transmission Integrity Check | Set lane keeping assistance torque to zero |
| Technical Safety Requirement 02-01-05 | Memory test shall be conducted at start up of the EPS ECU to check for any faults in memory. | A | Ignition cycle | Memory Test Block | Set lane keeping assistance torque to zero |

Functional Safety Requirement 02-2 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 02-02 | The Lane Keeping assistance shall be deactivated when the electronic power steering ECU detects the camera sensor is not working. | X | | |

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

| **ID** | **Technical Safety Requirement** | **A** | **Fault** | **Allocation to** | **Safe State** |
|---|---|---|---|---|---|

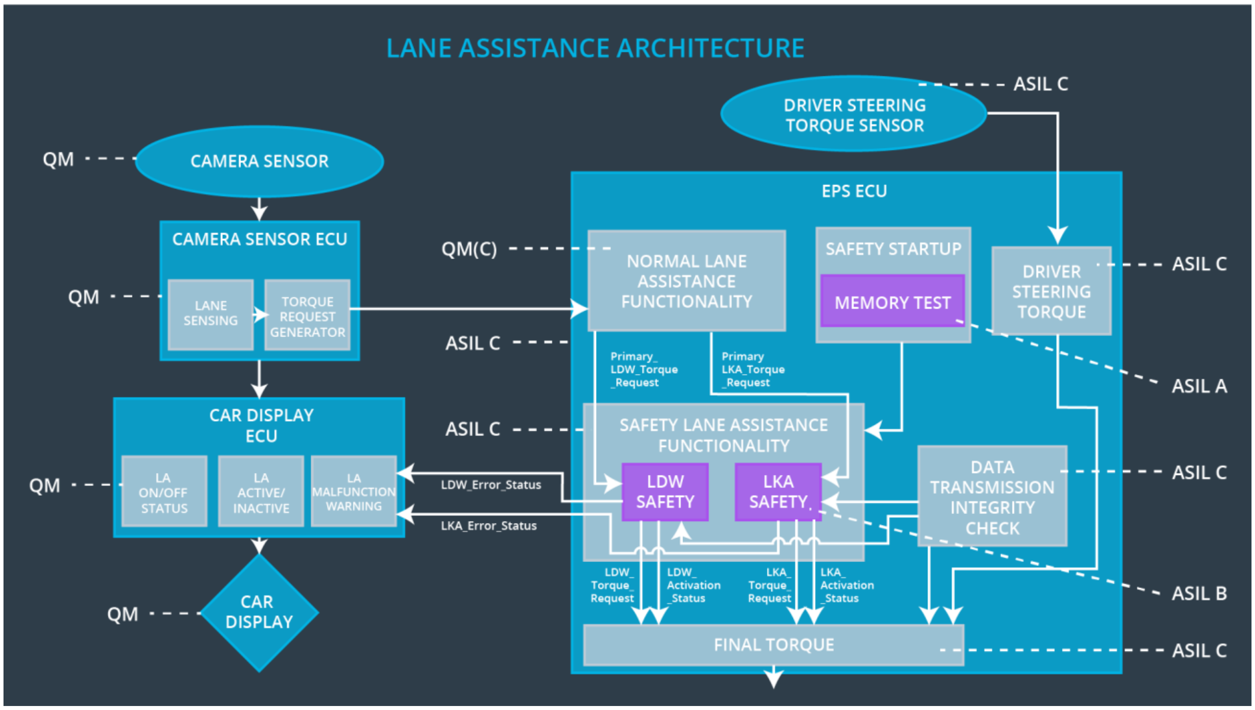
|  |  | SIL | Tolerant Time Interval | Architecture |  |
|---|---|---|---|---|---|
| Technical Safety Requirement 02-02-01 | The LKA safety component shall ensure that the loss of camera sensor torque request transmission will deactivate the LKA feature and the 'LKA_Torque_Request' shall be set to zero. | C | 500 ms | LKA Safety block | Set lane keeping assistance torque to zero |

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

| ID | Validation Acceptance Criteria and Method | Verification Acceptance Criteria and Method |
|---|---|---|
| Technical Safety Requirement 02-01-01 | Validate the Max_Duration is set to the chosen value from LKA Validation Assistance Criteria | Verify the functionality is turned off after it is applied for Max_Duration. |
| Technical Safety Requirement 02-01-02 | Validate the ‘TORQUE_LIMITER’ sends the error_status_torque_limiter signal to the LKA_SAFETY_ACTIVATION. | Verify the Car Display ECU displays the Lane Keeping Assistance malfunction warning signal. |
| Technical Safety Requirement 02-01-03 | Validate the ‘TORQUE_LIMITER’ sends ‘LKA_Torque_Request’ with zero. | Verify the Final EPS Torque generator receives a LKA_Torque_Request of zero. |
| Technical Safety Requirement 02-01-04 | Validate the ‘TORQUE_LIMITER’ calculate and sends the correct cyclic redundancy check (CRC) and Alive counter for data transmission validity and integrity. | Verify the functionality is turn off if there is a CRC or Alive counter discrepancy. |
| Technical Safety Requirement 02-01-05 | Validate the Safety Startup Memory test to check memory faults catch memory faults. | Verify the Lane Keeping Assistance is turned off when the Safety Startup Memory fails. |
| Technical Safety | Validate that the camera ECU sends zero ‘LKA_Torque_Request’ when it | Verify that the system really does turn off if the lane keeping assistance |

| | | |
|---|---|---|
| Requirement 02-02-01 | fails to detect lane lines and stop Alive counter for data transmission validity and integrity. | 'LKA_Torque_Request' ever has an invalid CRC or Alive counter failure from the camera ECU. |

## Refinement of the System Architecture



## Allocation of Technical Safety Requirements to Architecture Elements

| ID | Technical Safety Requirement | Electronic Power Steering ECU | Camera ECU | Car Display ECU |
|---|---|---|---|---|
| Technical Safety Requirement 01-01-01 | The Lane Departure Warning 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.' | X | | |

| | | | | |
|---|---|---|---|---|
| Technical Safety Requirement 01-01-02 | When the Lane Departure Warning is deactivated, the ‘LDW Safety’ software module shall send a signal to the Car Display ECU to turn on a warning signal. | **X** | | |
| Technical Safety Requirement 01-01-03 | When a failure is detected by the Lane Departure Warning functionality, it shall deactivate the Lane Departure Warning feature and set ‘LDW_Torque_Request’ to zero. | **X** | | |
| Technical Safety Requirement 01-01-04 | The validity and integrity of the data transmission for ‘LDW_Torque_Request’ signal shall be ensured. | **X** | | |
| Technical Safety Requirement 01-01-05 | Memory test shall be conducted at start up of the EPS ECU to check for any memory problems | **X** | | |
| Technical Safety Requirement 01-02-01 | The Lane Departure Warning safety component shall ensure the frequency of the ‘LDW_Torque_Reques’ sent to the ‘Final electronic power steering Torque’ component is below ‘Max_Torque_Frequency.’ | **X** | | |
| Technical Safety Requirement 02-01-01 | The Lane Keeping Assistance safety component shall ensure the duration of the lane keeping assistance torque is applied for less than Max_Duration | **X** | | |
| Technical Safety Requirement 02-01-02 | When the Lane Keeping Assistance function deactivates, the ‘LKA Safety’ shall send a signal to the Car Display ECU to turn on a warning light. | **X** | | |
| Technical Safety | When a failure is detected, the | **X** | | |

| | | | | |
|---|---|---|---|---|
| Requirement 02-01-03 | Lane Keeping Assistance function shall deactivate and the ‘LKA_Torque_Request’ shall be zero. | | | |
| Technical Safety Requirement 02-01-04 | The validity and integrity of the data transmission for ‘LKA_Torque_Request’ signal shall be ensured. | **X** | | |
| Technical Safety Requirement 02-01-05 | Memory test shall be conducted at start up of the EPS ECU to check for any memory problems | **X** | | |
| Technical Safety Requirement 02-02-01 | The LKA safety component shall ensure that the loss of camera sensor torque request transmission will deactivate the LKA feature and the 'LKA_Torque_Request' shall be set to zero. | **X** | | |

## Warning and Degradation Concept

| **ID** | **Degradation Mode** | **Trigger for Degradation Mode** | **Safe State invoked?** | **Driver Warning** |
|---|---|---|---|---|
| WDC-01 | Turn off Lane Departure Warning functionality | Malfunction_01, Malfunction_02, Malfunction_04 | Yes | Lane Departure Warning Malfunction Warning on Car Display |
| WDC-02 | Turn off Lane Keeping Assistance functionality | Malfunction_03, Malfunction_05 | Yes | Lane Keeping Assistance Malfunction Warning on Car Display |