

Technical Safety Concept Lane Assistance

**Document Version: [Version]**

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



# Document history

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Editor | Description |
| 25-May-2018 | 1.0 | Nishant Katariya | Initial Draft |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# 

# Table of Contents

[Document history](#_1t3h5sf)

[Table of Contents](#_ktt3lgighckp)

[Purpose of the Technical Safety Concept](#_fulgh8sf1ocg)

[Inputs to the Technical Safety Concept](#_757cx6xm46zb)

[Functional Safety Requirements](#_2f9rjqxbsp2)

[Refined System Architecture from Functional Safety Concept](#_qp3s9pvua9mt)

[Functional overview of architecture elements](#_cqb49updinx4)

[Technical Safety Concept](#_mx8us8onanqo)

[Technical Safety Requirements](#_lnxjuovv6kca)

[Refinement of the System Architecture](#_74udkdvf7nod)

[Allocation of Technical Safety Requirements to Architecture Elements](#_g2lqf7kmbspk)

[Warning and Degradation Concept](#_4w6r8buy4lrp)

# Purpose of the Technical Safety Concept

**[Instructions: Answer what is the purpose of a technical 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 | C | 50ms | Steering torque  Amplitude is  below  Max\_Torque\_A  mplitude |
| Functional  Safety  Requirement  01-02 | The lane keeping item shall ensure that the lane departure oscillating torque frequency is below Max\_Torque\_Frequency | C | 50ms | Oscillation  frequency is  below  Max\_Torque\_Fr  equency. |
| 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 | Lane Assistance Functionality is Off |

## 

## Refined System Architecture from Functional Safety Concept



### 

### Functional overview of architecture elements

|  |  |
| --- | --- |
| **Element** | **Description** |
| Camera Sensor | Camera sensor perceives the vehicle leaving the lane; it sends the signal to the Electronic power steering system request to turn/vibrate the steering wheel.  ECU (Electronic Control Unit) is a microcomputer that contains software and hardware specific to vehicle’s functionality. |
| Camera Sensor ECU - Lane Sensing | Camera Sensor ECU has software block to detect lanes either using deep learning algorithm or sing image processing |
| Camera Sensor ECU - Torque request generator | Camera Sensor ECU has software block which generate torque request which will be sent to EPS ECU. |
| Car Display | Displays the warning and status of the system on Display |
| Car Display ECU - Lane Assistance On/Off Status | A Status light for showing the status on/off of LA |
| Car Display ECU - Lane Assistant Active/Inactive | A Status light for showing the status Active/Inactive of LA |
| Car Display ECU - Lane Assistance malfunction warning | A Warning light for showing malfunction in LA system |
| Driver Steering Torque Sensor | It senses how much steering force is applied by the driver. |
| Electronic Power Steering (EPS) ECU - Driver Steering Torque | ECU Block to process sensor measurement (Steering torque applied by driver) |
| EPS ECU - Normal Lane Assistance Functionality | Receives torque request from Camera sensor ECU and transfer it to safety lane assistance functionality |
| EPS ECU - Lane Departure Warning Safety Functionality | Checks malfunction of LDW and translates torque requests into final torque output. |
| EPS ECU - Lane Keeping Assistant Safety Functionality | Checks malfunction of LKA and translates torque requests into final torque output. |
| EPS ECU - Final Torque | Combine torque from LDW and LKA and send them to motor |
| Motor | It is actuator to generate torque and rotate 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 | LDW Torque request Amplitude shall be set to 0 |
| 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 shall be set to 0 |
| 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 shall be set to 0 |
| 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 | LDW Torque request Amplitude shall be set to 0 |
| 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 | Memory Test | LDW Torque request Amplitude shall be set to 0 |

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 | LDW Torque request Frequency shall be set to 0 |
| 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 Frequency shall be set to 0 |
| 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 Frequency shall be set to 0 |
| 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 | LDW Torque request Frequency shall be set to 0 |
| 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 | Memory Test | LDW Torque request Frequency shall be set to 0 |

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

**[OPTIONAL]**

**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 |  |  |

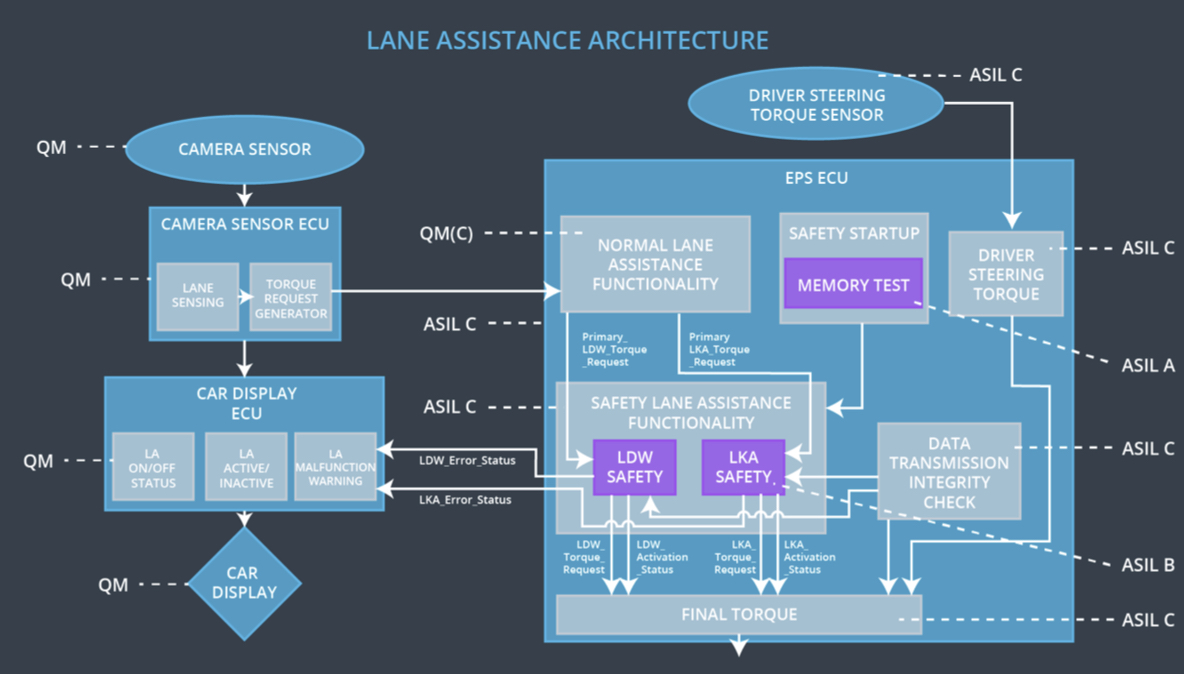
Technical Safety Requirements related to Functional Safety Requirement 02-01 are:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **ID** | **Technical Safety Requirement** | **ASIL** | **Fault Tolerant Time Interval** | **Architecture Allocation** | **Safe State** |
| Technical  Safety  Requirement  01 | The LKA safety component shall ensure that the of the 'LKA\_Torque\_Request' sent to the 'Final electronic power steering Torque' component for only 'Max\_Duration’. | B | 500 ms | LKA Safety | LKA\_Activation\_Status shall be set to 0 |
| 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\_Activation\_Status shall be set to 0 |
| 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\_Activation\_Status shall be set to 0 |
| 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 | LKA\_Activation\_Status shall be set to 0 |
| 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 | Memory Test | LKA\_Activation\_Status shall be set to 0 |

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

**[OPTIONAL]**

## Refinement of the System Architecture

****

## Allocation of Technical Safety Requirements to Architecture Elements

All Technical safety requirements were allocated to the Electronic Power Steering ECU. For exact allocation check the technical requirements mentioned above.

## Warning and Degradation Concept

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Degradation Mode** | **Trigger for Degradation Mode** | **Safe State invoked?** | **Driver Warning** |
| WDC-01 | Turn Off LDW functionality | Malfunction\_01 | Yes | LDW malfunction warning on Car display |
| WDC-02 | Turn Off LDW functionality | Malfunction\_02 | Yes | LDW malfunction warning on Car display |
| WDC-03 | Turn Off LKA functionality | Malfunction\_03 | Yes | LKA malfunction warning on Car display |