

Technical Safety Concept Lane Assistance

**Document Version: [1.0]**

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



# Document history

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Editor | Description |
| 27/11/2018 | 1.0 | Archit Rastogi | First pass |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# 

# 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

Technical safety concept involves:

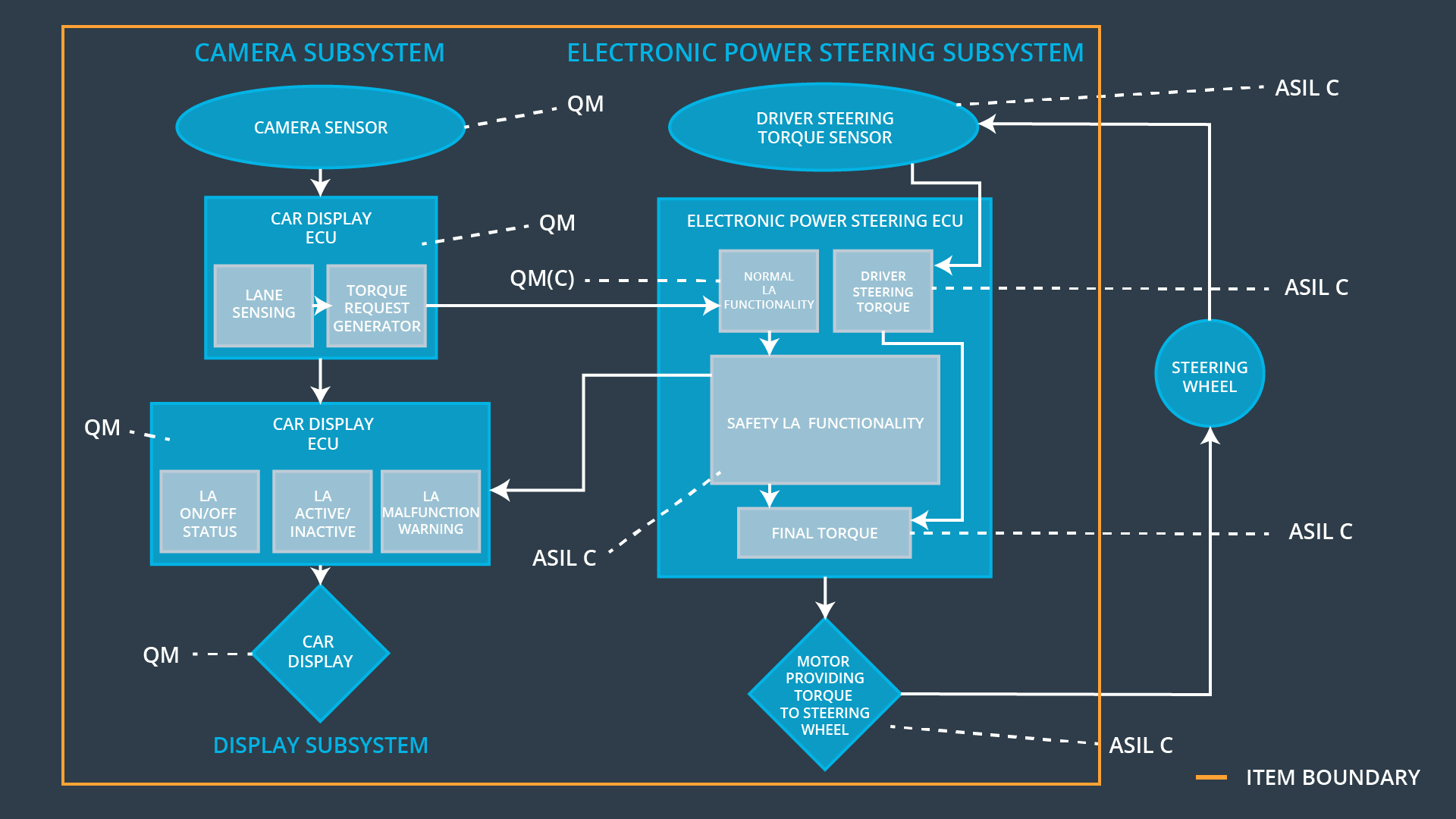
* Turning functional safety requirements into technical safety requirements
* Allocating technical safety requirements to the system architecture

# 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 keeping item shall ensure that the lane departure oscillating torque amplitude is below Max\_Torque\_Amplitude | C | 50ms | Vibration Torque Amplitude below  Max\_Torque\_Amplitude |
| 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 | Vibration Torque frequency below Max\_Torque\_Frequency |
| 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 Keeping Assistance Torque is zero |

## Refined System Architecture from Functional Safety Concept



### 

### Functional overview of architecture elements

|  |  |
| --- | --- |
| **Element** | **Description** |
| Camera Sensor | Captures Image and provides the data to the Camera ECU |
| Camera Sensor ECU - Lane Sensing | Detects Lane line from the images |
| Camera Sensor ECU - Torque request generator | Generates torque request based on the lane lines and position of vehicle to be sent to EPS ECU |
| Car Display | Show warning to the driver |
| Car Display ECU - Lane Assistance On/Off Status | Indicates if the LA functionality is off or on |
| Car Display ECU - Lane Assistant Active/Inactive | Indicates if the LA functionality is active/ inactive based on lane detection |
| Car Display ECU - Lane Assistance malfunction warning | Indicates any malfunction in the LA system |
| Driver Steering Torque Sensor | Measures the steering torque applied by the driver |
| Electronic Power Steering (EPS) ECU - Driver Steering Torque | Process input from Driver Steering Torque Sensor |
| EPS ECU - Normal Lane Assistance Functionality | Receives Camera Sensor Torque request and pass it to safety lane assistance functionality module |
| EPS ECU - Lane Departure Warning Safety Functionality | Ensures if the LDW is working properly and the functional safety requirements are met |
| EPS ECU - Lane Keeping Assistant Safety Functionality | Ensures if the LKA is working properly and the functional safety requirements are met |
| EPS ECU - Final Torque | Combines the torque request from LDW, LKA and also the driver steering torque and send it to the motor |
| Motor | Applies the final torque received from Electronic Power Steering ECU to 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 | 50ms | LDW Safety | LDW\_Torque\_Request Amplitude to 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 | 50ms | LDW Safety | LDW\_Torque\_Request Amplitude to 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 | 50ms | LDW Safety | LDW\_Torque\_Request Amplitude to 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 | 50ms | Data Transmission and Integrity | LDW\_Torque\_Request Amplitude to be set to zero |
| 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 to 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 frequency of the 'LDW\_Torque\_Request' sent to the 'Final electronic power steering Torque' component is below 'Max\_Torque\_Frequency | C | 50ms | LDW Safety | LDW\_Torque\_Request Frequency to 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 | 50ms | LDW Safety | LDW\_Torque\_Request Frequency to 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 | 50ms | LDW Safety | LDW\_Torque\_Request Frequency to 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 | 50ms | Data Transmission and Integrity | LDW\_Torque\_Request Frequency to be set to zero |
| 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 Frequency to be 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 safety component shall ensure that the 'LDW\_Torque\_Request' is sent to the 'Final electronic power steering Torque' component only for 'Max\_Duration’ | B | 500ms | LKA Safety | LKA\_Torque\_Request to 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 | 500ms | LKA Safety | LKA\_Torque\_Request to 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 | 500ms | LKA Safety | LKA\_Torque\_Request to 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 | 500ms | Data Transmission and Integrity | LKA\_Torque\_Request to be set to zero |
| 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 to be 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

## Warning and Degradation Concept

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Degradation Mode** | **Trigger for Degradation Mode** | **Safe State invoked?** | **Driver Warning** |
| WDC-01 | System off | Malfunction 01, 02 | Yes | Warning on Car Display |
| WDC-02 | System off | Malfunction 03 | Yes | Warning on Car Display |