

Technical Safety Concept Lane Assistance

**Document Version: [Version]**

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



# Document history

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Editor | Description |
| 02.04.2018 | 1.0 | Siddarth Kothiwale | First edit |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# 

# 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 is more concrete and gets into the details of the item's technology. It 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 | 50 ms | LKA torque request should 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 | C | 50 ms | LKA torque request 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 | LKA torque request should be set to zero |

## Refined System Architecture from Functional Safety Concept



### Functional overview of architecture elements

|  |  |
| --- | --- |
| **Element** | **Description** |
| Camera Sensor | To sense or record the video of road |
| Camera Sensor ECU - Lane Sensing | To sense the lanes from the video |
| Camera Sensor ECU - Torque request generator | To generate torque request in case the car leaves the road |
| Car Display | To display the warnings |
| Car Display ECU - Lane Assistance On/Off Status | To issue a message to display to show on/off status |
| Car Display ECU - Lane Assistant Active/Inactive | To issue a message to display to show active/inactive |
| Car Display ECU - Lane Assistance malfunction warning | To issue a message to display to show malfunction |
| Driver Steering Torque Sensor | To sense the torque at the steering wheel (may be the driver is providing some torque |
| Electronic Power Steering (EPS) ECU - Driver Steering Torque | To calculate the amount to torque that needs to be applied taking into account the torque applied by driver |
| EPS ECU - Normal Lane Assistance Functionality | To steer by correct amount to keep the car in the lane |
| EPS ECU - Lane Departure Warning Safety Functionality | To provide a vibration to steering wheel to warn the driver and to see that the frequency and the amplitude is below the specified limit. |
| EPS ECU - Lane Keeping Assistant Safety Functionality | To see that the car remains in the lane and the system shuts down after the specified amount of time. |
| EPS ECU - Final Torque | To apply a final torque taking into account the functional safety concepts |
| Motor | To apply the required 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 | LDW torque request amplitude should 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 | LDW torque request amplitude should 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 | LDW torque request amplitude should 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 | LDW Safety | LDW torque request amplitude should 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 | Safety startup | LDW torque request amplitude should 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 | LDW torque request frequency should 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 | LDW torque request frequency should 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 | LDW torque request frequency should 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 | LDW Safety | LDW torque request frequency should 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 | Safety startup | LDW torque request frequency should be set to zero |

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

**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 torque is applied for only Max\_Duration | B | 500 ms | LKA Safety | LKA torque request should 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 | LKA torque request should 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 | LKA torque request should 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 | LKA Safety | LKA torque request should 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 | Safety startup | LKA torque request should be set to zero |

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

## Refinement of the System Architecture

****

## Allocation of Technical Safety Requirements to Architecture Elements

All the technical safety requirements are applied to EPS ECU

## Warning and Degradation Concept

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Degradation Mode** | **Trigger for Degradation Mode** | **Safe State invoked?** | **Driver Warning** |
| WDC-01 | Turn off the function | Amplitude> Max\_Torque\_Amplitude and  Frequency> Max\_Torque\_Frequency | Yes | Warning sign in Driver display system |
| WDC-02 | Turn off the function | If LKA active for time > Max\_Duration | Yes | Warning sign in Driver display system |