

Technical Safety Concept Lane Assistance

**Document Version: 1.0**

**Released on 2018-05-22**



# Document history

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Editor | Description |
| 21-May-2018 | 0.1 | Venkataraman | Initial Draft |
| 23-May-2018 | 1.0 | Venkataraman | First attempt |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# 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

The functional safety requirements in the functional safety concept is used to establish the Technical safety concept. These new​ ​requirements​ ​are​ ​more​ ​concrete​ ​and​ ​gets​ ​into​ ​details​ ​of​ ​the​ ​item’s​ ​technology​ ​as​ ​specified by​ ​ISO​ ​26262.

The 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 | 50 ms | Vibration torque amplitude 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 | 50 ms | 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 | 500 ms | Lane Assistant torque is zero |
| Functional  Safety  Requirement  02-02 | The electronic power steering ECU shall be deactivated​ ​when​ ​the​ ​electronic​ ​power steering​ ​ECU​ ​detects​ ​the​ ​camera sensor​ ​is​ ​not​ ​working. | B | 50 ms | Function is deactivated |

## Refined System Architecture from Functional Safety Concept



### Functional overview of architecture elements

|  |  |
| --- | --- |
| **Element** | **Description** |
| Camera Sensor | Sensor responsible for capturing road images and provide them to the Camera Sensor ECU |
| Camera Sensor ECU - Lane Sensing | Software module inside camera sensor ECU responsible for detecting the lane line positions from the Camera Sensor images. |
| Camera Sensor ECU - Torque request generator | Software module inside camera sensor ECU responsible for calculating additional torque for LKA and LDW function. This calculated torque will be requested to EPS ECU. |
| Car Display | Car Display is responsible for providing feedback to the driver about the status of lane assistant system |
| Car Display ECU - Lane Assistance On/Off Status | Software module responsible for displaying **On/Off** status of LDW & LKA functions. |
| Car Display ECU - Lane Assistant Active/Inactive | Software module responsible for displaying **Active/Inactive** status of LDW & LKA function. |
| Car Display ECU - Lane Assistance malfunction warning | Software module responsible for displaying warning of malfunctions in LDW & LKA function. |
| Driver Steering Torque Sensor | Sensor responsible for measuring the torque applied on steering wheel |
| Electronic Power Steering (EPS) ECU - Driver Steering Torque | Software module responsible for process data received from Driver Steering Torque Sensor. |
| EPS ECU - Normal Lane Assistance Functionality | Software module responsible for receiving torque request from Camera Sensor ECU and transfers to Safety Lane Assistance Functionality. |
| EPS ECU - Lane Departure Warning Safety Functionality | Software​ ​module​ ​ensuring​ ​the​ ​torque amplitude​ ​is​ ​below​ ​Max\_Torque\_Amplitude and​ ​torque​ ​frequency​ ​is​ ​below Max\_Torque\_Frequency. |
| EPS ECU - Lane Keeping Assistant Safety Functionality | Software module in EPS ECU responsible for ensuring that LKA is not activate more than Max\_duration time and if camera sensor is failed, then LKA will be deactivated. |
| EPS ECU - Final Torque | Combine​ ​the​ ​torque​ ​request​ ​from​ ​the​ ​LKA safety​ ​and​ ​LDW safety functionalities​ ​and​ ​sends​ ​them​ ​to​ ​the​ ​Motor. |
| Motor | An electric motor that applies the torque indicated by the Electronic Power Steering ECU 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  01-01-01 | 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 | LDW\_Torque\_Output is set 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 | LDW\_Torque\_Output is set to zero |
| Technical  Safety  Requirement  01-01-03 | Once the failure in LDW is identified, The LDW feature needs to be deactivate, preventing it from taking control of the vehicle. | C | 50 ms | LDW safety block | LDW\_Torque\_Output is set 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 | LDW\_Activation\_Status is zero |
| Technical  Safety  Requirement  01-01-05 | Memory test shall be conducted at startup of the EPS ECU to check for any faults in memory. | A | Ignition cycle | Memory Test | LDW\_Activation\_Status is zero |

Functional Safety Requirement 01-02 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 frequency of the 'LDW\_Torque\_Request' sent to the 'Final electronic power steering Torque' component is below 'Max\_Torque\_Frequency. | C | 50 ms | LDW safety block | LDW\_Torque\_Output is set to zero |

**Lane Keeping Assistance (LKA) Requirements:**

Functional Safety Requirement 02-01 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  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 amplitude of the 'LKA\_Torque\_Request' sent to the 'Final electronic power steering Torque' component is below 'Max\_Duration’. | C | 50 ms | LKA safety block | LKA\_Torque\_Output is set to zero |
| Technical  Safety  Requirement  02-01-02 | 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 | C | 50 ms | LKA safety block | LKA\_Torque\_Output is set to zero |
| Technical  Safety  Requirement  02-01-03 | 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. | C | 50 ms | LKA safety block | LKA\_Torque\_Output is set 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 | 50 ms | Data Transmission Integrity Check | LKA\_Activation\_Status is zero |
| Technical  Safety  Requirement  02-01-05 | 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 is zero |

Functional Safety Requirement 02-02 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 electronic power steering ECU 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** | **ASIL** | **Fault Tolerant Time Interval** | **Allocation to Architecture** | **Safe State** |
| Technical  Safety  Requirement  02-02-01 | As soon as a failure is detected by the Camera Sensor, it shall deactivate the LKA feature and the 'LKA\_Torque\_Request' shall be set to zero. | C | 50 ms | LKA safety block | LKA\_Activation\_Status is zero |

## Refinement of the System Architecture

****

## Allocation of Technical Safety Requirements to Architecture Elements

For the Lane Assistance item, all technical safety requirements are allocated to the Electronic Power Steering ECU. For the exact allocation within EPS ECU, please refer to the technical safety requirements tables 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,  Malfunction\_02 | Yes | Turn on warning light of the LDW functionality |
| WDC-02 | Turn off LKA functionality | Malfunction\_03,  Malfunction\_04 | Yes | Turn on warning light of the LKA functionality |