

Technical Safety Concept Lane Assistance

**Document Version: [Version]**

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



# Document history

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Editor | Description |
| 24 May 2018 | 1.0 | Vivekkumar Mehta | First version of technical safety concept |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# 

# 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 requirements are general hardware and software requirements but still without getting into specific details. The technical safety concept looks at the technical implementation of the item. New requirements are defined and assigned 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 | 50ms | Vibration torque  amplitude  below  Max\_Torque\_A  mplitude. |
| 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 | 50ms | Vibration  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 only  Max\_Duration. | B | 500ms | Lane Keeping  Assistance  torque is zero. |

## Refined System Architecture from Functional Safety Concept

### 



### Functional overview of architecture elements

**[Instructions: Provide a description for each functional safety element; what is each element's purpose in the lane assistance item? ]**

|  |  |
| --- | --- |
| **Element** | **Description** |
| Camera Sensor | Provides visual input to camera sensor ECU |
| Camera Sensor ECU - Lane Sensing | Software module detecting the ego lane line  positions from the Camera Sensor images. |
| Camera Sensor ECU - Torque request generator | Software module calculating the necessary  torque to be requested to the Electronic Power  Steering ECU. |
| Car Display | Gives visual feedback to driver |
| Car Display ECU - Lane Assistance On/Off Status | Displays the status of the Lane Assistance  functionality (On/Off). |
| Car Display ECU - Lane Assistant Active/Inactive | Displays if the Lane Assistance functionality is  properly functioning (Active/Inactive). |
| Car Display ECU - Lane Assistance malfunction warning | Displays a malfunction on the Lane Assistance  functionality. |
| Driver Steering Torque Sensor | Gives steering torque input to electronic power steering ECU given by driver |
| Electronic Power Steering (EPS) ECU - Driver Steering Torque | Software module receiving the driver’s torque  request from the steering wheel. |
| EPS ECU - Normal Lane Assistance Functionality | Software module receiving the Camera Sensor  ECU torque request. |
| 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 | Checks for malfunction of Lane Keeping Assistant  and transfers torque request to final torque output. |
| EPS ECU - Final Torque | Generates final torque from torque requests  received from LDW and LKA safety. |
| Motor | Receives final torque and applies it 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 ‘LDW\_Torque\_Request’ sent  to the ‘Final electronic power  steering Torque’ component is  below ‘Max\_Torque\_Amplitude’. | C | 50ms | LDW Safety | LDW\_Activati  on\_Status is  zero |
| Technical  Safety  Requirement  02 | As soon as a failure is detected  by the LDW function, it shall  deactivate the LDW feature and  the ‘LDW\_Torque\_Request’  shall e set to zero. | C | 50ms | LDW Safety | LDW\_Activati  on\_Status is  zero |
| Technical  Safety  Requirement  03 | As soons 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\_Error\_S  tatus is zero |
| Technical  Safety  Requirement  04 | data transmission for  ‘LDW\_Torque\_Request’ signal  shall be ensured. | C | 50ms | Data Transmission  Integrity  Check | NA |
| Technical  Safety  Requirement  05 | Memory test shall be conducted  at start up of the EPS ECU to  check for any faults in mermory. | A | ignition  cycle | Memory Test | LDW\_Activati  on\_Status is  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 ‘LDW\_Torque\_Request’ sent to the ‘Final electronic power steering Torque’ component is below ‘Max\_Torque\_Frequency’. | C | 50 ms | LDW Safety | LDW\_Activation\_Status is zero |
| Technical  Safety  Requirement  02 | As soon as a failure is detected by the LDW function, it shall deactivate the LDW feature and the ‘LDW\_Torque\_Request’ shall e set to zero. | C | 50 ms | LDW Safety | LDW\_Activation\_Status is zero |
| Technical  Safety  Requirement  03 | As soons 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\_Error\_Status is zero |
| 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\_Activation\_Status is zero |
| Technical  Safety  Requirement  05 | Memory test shall be conducted at start up of the EPS ECU to check for any faults in mermory. | A | ignition cycle | Memory Test | LDW\_Activation\_Status is 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 ‘LKA\_Torque\_Request’ is sent to the ‘Final electronic power steering Torque’ component for only ‘Max\_Duration’. | B | 500 ms | LKA Safety | LKA\_Activation\_Status is zero |
| Technical  Safety  Requirement  02 | As soon as a failure is detected by the LKA function, it shall deactivate the LKA feature and the ‘LKA\_Torque\_Request’ shall e set to zero. | B | 500 ms | LKA Safety | LKA\_Activation\_Status is zero |
| Technical  Safety  Requirement  03 | As soons 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\_Error\_Status is zero |
| 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 is zero |
| Technical  Safety  Requirement  05 | Memory test shall be conducted at start up of the EPS ECU to check for any faults in mermory. | A | ignition cycle | Memory Test | LKA\_Activation\_Status is zero |

## 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.

## Warning and Degradation Concept

For any system malfunction, the lane assistance functions will be turned off and the driver will receive a warning light indication.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Degradation Mode** | **Trigger for Degradation Mode** | **Safe State invoked?** | **Driver Warning** |
| WDC-01 | Turn off Lane Assistant functionality | Malfunction\_01 | Yes | Lane Assistant Malfunction Warning on Car Display |
| WDC-02 | Turn off Lane Assistant functionality | Malfunction\_02 | Yes | Lane Assistant Malfunction Warning on Car Display |
| WDC-03 | Turn off Lane Assistant functionality | Malfunction\_03 | Yes | Lane Assistant Malfunction Warning on Car Display |
| WDC-04 | Turn off Lane Assistant functionality | Malfunction\_04 | Yes | Lane Assistant Malfunction Warning on Car Display |
| WDC-05 | Turn off Lane Assistant functionality | Malfunction\_05 | Yes | Lane Assistant Malfunction Warning on Car Display |