

Technical Safety Concept Lane Assistance

**Document Version: 1.0**

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



# Document history

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Editor | Description |
| 24-Aug-2018 | 1.0 | Mohamed ZIEDAN | Initial Release |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# 

# 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 technical safety concept defines how the subsystems interact at the message level and describes how the ECUs communicate with each other.

# 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 | Electronic Power Steering ECU shall ensure that the lane departure oscillating torque amplitude is below *Max\_Torque\_Amplitude* | C | 50ms | LDW will set the oscillating torque amplitude to 0 |
| Functional  Safety  Requirement  01-02 | Electronic Power Steering ECU shall ensure that the lane departure oscillating torque frequency is below *Max\_Torque\_Frequency* | C | 50ms | LDW will set the oscillating torque frequency to 0 |
| Functional  Safety  Requirement  02-01 | Electronic Power Steering ECU shall ensure that the lane keeping assistance torque is applied for only *Max\_Duration* | B | 500ms | LKA will set the oscillating torque Duration to 0 |

## Refined System Architecture from Functional Safety Concept



### Functional overview of architecture elements

|  |  |
| --- | --- |
| **Element** | **Description** |
| Camera Sensor | Take images of the road |
| Camera Sensor ECU - Lane Sensing | Detects lanes on road, and lane departures |
| Camera Sensor ECU - Torque request generator | tells the Electronic Power Steering ECU how hard to turn , and Car Display ECU to display a warning` |
| Car Display | show a warning for the driver |
| Car Display ECU - Lane Assistance On/Off Status | receives a warning from Electronic Power Steering (EPS) ECU, show Lane Assistance status |
| Car Display ECU - Lane Assistant Active/Inactive | receives a warning from Electronic Power Steering (EPS) ECU, show Lane Assistant Activity state |
| Car Display ECU - Lane Assistance malfunction warning | receives a warning from Electronic Power Steering (EPS) ECU, show Warning on Lane Assistance malfunction |
| Driver Steering Torque Sensor | Detect how hard the driver is turning the steering  Wheel |
| Electronic Power Steering (EPS) ECU - Driver Steering Torque | Analyze how hard the driver is turning the steering  wheel, and contribute at the 'FINAL TORQUE' |
| EPS ECU - Normal Lane Assistance Functionality | receives a warning from Camera  Sensor ECU, it then decides the vibration required to warn driver and how much steering torque is required |
| EPS ECU - Lane Departure Warning Safety Functionality | Analyze and decides the vibration required to warn driver and how much steering torque is required, then send contribute at the 'FINAL TORQUE', and alert Car Display ECU |
| EPS ECU - Lane Keeping Assistant Safety Functionality | Analyze and decides the duration required to run the LKA item, then send contribute at the 'FINAL TORQUE' and Alert Car Display ECU |
| EPS ECU - Final Torque | Receives inputs from LKA Safety, LDW Safety , and Driver Steering Torque to product the FINAL TORQUE amount that will be passed to steering Motor |
| Motor | motor will provide the torque 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 | Lane Assistance Safety Functionality | Deactivate functionality (reset Amplitude 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 | 50ms | LDW Safety Functionality | Deactivate functionality (reset Amplitude 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 | 50ms | LDW Safety Functionality | Deactivate functionality (reset Amplitude to 0) |
| Technical  Safety  Requirement  04 | The validity and integrity of the data transmission for '*LDW\_Torque\_Request*' signal shall be ensured | C | 50ms | Data Transmission Integrity Check | Deactivate functionality (reset Amplitude 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 | SAFETY STARTUP | *Max\_Torque\_Amplitude* is correct and Deactivate Functionality will reset Amplitude 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 Frequency of the '*LDW\_Frequency\_Request*' sent to the 'Final electronic power steering Torque' component is below *Max\_Torque\_Frequency* | C | 50ms | Lane Assistance Safety Functionality | Deactivate functionality (reset Frequency 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 | 50ms | LDW Safety Functionality | Deactivate functionality (reset Frequency 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\_Frequency\_Request*' shall be set to zero | C | 50ms | LDW Safety Functionality | Deactivate functionality (reset Frequency to 0) |
| Technical  Safety  Requirement  04 | The validity and integrity of the data transmission for '*LDW\_Frequency\_Request*' signal shall be ensured | C | 50ms | Data Transmission Integrity Check | Deactivate functionality (reset Frequency 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 | SAFETY STARTUP | *Max\_Torque\_Frequency* is correct & Deactivate Functionality will reset Frequency to 0 |

**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 Duration of the '*LKA\_Duration\_Request*' sent to the 'Final electronic power steering Torque' component is below *Max\_Duration* | C | 50ms | Lane Assistance Safety Functionality | Deactivate functionality (reset Duration 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 | C | 50ms | LKA Safety Functionality | Deactivate functionality (reset Duration 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\_Duration\_Request*' shall be set to zero | C | 50ms | LKA Safety Functionality | Deactivate functionality (reset Duration to 0) |
| Technical  Safety  Requirement  04 | The validity and integrity of the data transmission for '*LKA\_Duration\_Request*' signal shall be ensured | C | 50ms | Data Transmission Integrity Check | Deactivate functionality (reset Duration 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 | SAFETY STARTUP | Max\_ Duration is correct, and Deactivate Functionality will reset Duration to 0 |

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

## 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 | turn off the functionality | Functional  Safety  Requirement  01-01 is violated | YES | Display Warning on display system, and different Haptic feedback on the steering wheel |
| WDC-02 | turn off the functionality | Functional  Safety  Requirement  02-01 is violated | YES | Display Warning on display system, and beep sound. |