

Technical Safety Concept Lane Assistance

**Document Version: 1.0**



# Document history

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Editor | Description |
| 06/06/2019 | 1.0 | M. Elbanhawi | First submissio |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# 

# 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

**[Instructions: Answer what is the purpose of a technical safety concept?]**

# 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 | Disable system |
| 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 | Disable system |
| Functional  Safety  Requirement  02-01 | The electronic power steering ECU shall limit lane keeping assistance torque for only Max\_Duration | B | 500 ms | Disable system. |

## Refined System Architecture from Functional Safety Concept



### 

### Functional overview of architecture elements

|  |  |
| --- | --- |
| **Element** | **Description** |
| Camera Sensor | Capture images of the road and send to the camera ECU |
| Camera Sensor ECU - Lane Sensing | Software module that processes images to determine lane and position of vehicle in lane |
| Camera Sensor ECU - Torque request generator | Software module the sends a torque request based on the lane sensing output to the power steering ECU |
| Car Display | HMI to the driver, displays light status for LKA and LDW |
| Car Display ECU - Lane Assistance On/Off Status | Indicates the status of Lane Assistance |
| Car Display ECU - Lane Assistant Active/Inactive | Indicates the activity of Lane Assistance |
| Car Display ECU - Lane Assistance malfunction warning | Indicates the functionality of Lane Assistance |
| Driver Steering Torque Sensor | Measures the steering input from the driver |
| Electronic Power Steering (EPS) ECU - Driver Steering Torque | Software block that receives torque input from the driver |
| EPS ECU - Normal Lane Assistance Functionality | Software block that receives torque request from Camera Sensor ECU – Torque request block |
| EPS ECU - Lane Departure Warning Safety Functionality | Software block that constrains the torque amplitude and frequency to Max\_Torque\_Amplitude and Max\_Torque\_Frequency respectively. |
| EPS ECU - Lane Keeping Assistant Safety Functionality | Software block that limits the LKA activity duration to Max\_Duration |
| EPS ECU - Final Torque | Software block that combines torque request from LKA, LDW and send it to the motor |
| Motor | Applies torque request 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 Torque Limiter component shall limit the Limited\_LDW\_Torque\_Request amplitude is below Max\_Torque\_Amplitude | C | 50ms | LDW Safety | Deactivate LDW |
| Technical  Safety  Requirement  02 | The LDW\_Safety\_Output\_Generator component shall limit the LDW\_Torque\_Request amplitude is below Max\_Torque\_Amplitude | C | 50ms | LDW Safety | Deactivate LDW |
| Technical  Safety  Requirement  03 | The Torque Limiter component shall output an error if the Limited\_LDW\_Torque\_Request amplitude is above Max\_Torque\_Amplitude | C | 50ms | LDW Safety | Deactivate LDW |
| Technical  Safety  Requirement  04 | The LDW\_Safety\_Output\_Generator component shall output an error if LDW\_Frequency\_Request amplitude is above Max\_Torque\_Amplitude | C | 50ms | LDW Safety | Deactivate LDW |
| Technical  Safety  Requirement  05 | The LDW\_SAFETY\_ACTIVATION component shall deactivate the EPS\_Torque\_generator when it receives an error | C | 50ms | LDW Safety | Deactivate LDW |
| Technical  Safety  Requirement  06 | The LDW\_SAFETY\_ACTIVATION component shall output a malfunction to the car display when it receives an error | C | 50ms | LDW Safety | Deactivate LDW |

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 Frequency Limiter component shall limit the Limited\_LDW\_Frequency\_Request is below Max\_Torque\_Frequency | C | 50ms | LDW Safety | Deactivate LDW |
| Technical  Safety  Requirement  02 | The LDW\_Safety\_Output\_Generator component shall limit the LDW\_Frequency\_Request frequencyis below Max\_Torque\_Frequency | C | 50ms | LDW Safety | Deactivate LDW |
| Technical  Safety  Requirement  03 | The Torque Limiter component shall output an error if the Limited\_LDW\_Frequency\_Request frequency is above Max\_Torque\_Frequency | C | 50ms | LDW Safety | Deactivate LDW |
| Technical  Safety  Requirement  04 | The LDW\_Safety\_Output\_Generator component shall output an error if LDW\_Frequency\_Request frequency is above Max\_Torque\_Frequency | A | Ignition | LDW Safety | Deactivate LDW |
| Technical  Safety  Requirement  05 | The LDW\_SAFETY\_ACTIVATION component shall deactivate the EPS\_Torque\_generator when it receives an error | C | 50ms | LDW Safety | Deactivate LDW |
| Technical  Safety  Requirement  06 | The LDW\_SAFETY\_ACTIVATION component shall output a malfunction to the car display when it receives an error | C | 50ms | LDW Safety | Deactivate LDW |

**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** | **Architecture Allocation** | **Safe State** |
| Technical  Safety  Requirement  01 | The LKA\_Torque\_Request duration shall be below Max\_Duration. | B | 500ms | LKA Safety | Deactivate LKA |
| Technical  Safety  Requirement  02 | The LKA Safety component shall output an error if the duration LKA\_Torque\_Request is above Max\_Duration. | B | 500ms | LKA Safety | Deactivate LKA |
| Technical  Safety  Requirement  03 | A Safety test shall be conducted on the memory on start up | B | Igniton | LKA Safety | Deactivate LKA |
| Technical  Safety  Requirement  04 | The LKA\_Safety component shall deactivate the EPS\_Torque\_generator when it receives an error | B | 500ms | LKA Safety | Deactivate LKA |
| Technical  Safety  Requirement  05 | The LKA\_Safety component shall output a malfunction to the car display when it receives an error | B | 500ms | LKA Safety | Deactivate LKA |

## Refinement of the System Architecture



## Allocation of Technical Safety Requirements to Architecture Elements

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Technical Safety Requirement** | **Electronic Power Steering ECU** | **Camera ECU** | **Car Display ECU** |
| Technical  Safety  Requirement  01-01-01 | The Torque Limiter component shall limit the Limited\_LDW\_Torque\_Request amplitude is below Max\_Torque\_Amplitude | **X** |  |  |
| Technical  Safety  Requirement  01-01-02 | The LDW\_Safety\_Output\_Generator component shall limit the LDW\_Torque\_Request amplitude is below Max\_Torque\_Amplitude | **X** |  |  |
| Technical  Safety  Requirement  01-01-03 | The Torque Limiter component shall output an error if the Limited\_LDW\_Torque\_Request amplitude is above Max\_Torque\_Amplitude | **X** |  |  |
| Technical  Safety  Requirement  01-01-04 | The LDW\_Safety\_Output\_Generator component shall output an error if LDW\_Frequency\_Request amplitude is above Max\_Torque\_Amplitude | **X** |  |  |
| Technical  Safety  Requirement  01-01-05 | The LDW\_SAFETY\_ACTIVATION component shall deactivate the EPS\_Torque\_generator when it receives an error | **X** |  |  |
| Technical  Safety  Requirement  01-01-06 | The LDW\_SAFETY\_ACTIVATION component shall output a malfunction to the car display when it receives an error | **X** |  |  |
| Technical  Safety  Requirement  01-02-01 | The Frequency Limiter component shall limit the Limited\_LDW\_Frequency\_Request is below Max\_Torque\_Frequency | **X** |  |  |
| Technical  Safety  Requirement  01-02-02 | The LDW\_Safety\_Output\_Generator component shall limit the LDW\_Frequency\_Request frequencyis below Max\_Torque\_Frequency | **X** |  |  |
| Technical  Safety  Requirement  01-02-03 | The Torque Limiter component shall output an error if the Limited\_LDW\_Frequency\_Request frequency is above Max\_Torque\_Frequency | **X** |  |  |
| Technical  Safety  Requirement  01-02-04 | The LDW\_Safety\_Output\_Generator component shall output an error if LDW\_Frequency\_Request frequency is above Max\_Torque\_Frequency | **X** |  |  |
| Technical  Safety  Requirement  01-02-05 | The LDW\_SAFETY\_ACTIVATION component shall deactivate the EPS\_Torque\_generator when it receives an error | **X** |  |  |
| Technical  Safety  Requirement  02-01-01 | The LKA\_Torque\_Request duration shall be below Max\_Duration. | **X** |  |  |
| Technical  Safety  Requirement  02-01-02 | The LKA Safety component shall output an error if the duration LKA\_Torque\_Request is above Max\_Duration. | **X** |  |  |
| Technical  Safety  Requirement  02-01-03 | A Safety test shall be conducted on the memory on start up | **X** |  |  |
| Technical  Safety  Requirement  02-01-04 | The LKA\_Safety component shall deactivate the EPS\_Torque\_generator when it receives an error | **X** |  |  |
| Technical  Safety  Requirement  02-01-05 | The LKA\_Safety component shall output a malfunction to the car display when it receives an error | **X** |  |  |

## Warning and Degradation Concept

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Degradation Mode** | **Trigger for Degradation Mode** | **Safe State invoked?** | **Driver Warning** |
| WDC-01 | Disable LDW | Malfunction\_01,  Malfunction\_02, | Yes | LDW Malfunction Warning on Car Display |
| WDC-02 | Disable LKW | Malfunction\_03, | Yes | LKA Malfunction Warning on Car Display |