

Technical Safety Concept Lane Assistance

**Document Version: 1.0**



# Document history

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Editor | Description |
| 27/11/2018 | 1.0 | Atul Kumar | Draft version |
| 02/11/2018 | 2.0 | Atul Kumar | Added new feature |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# 

# 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

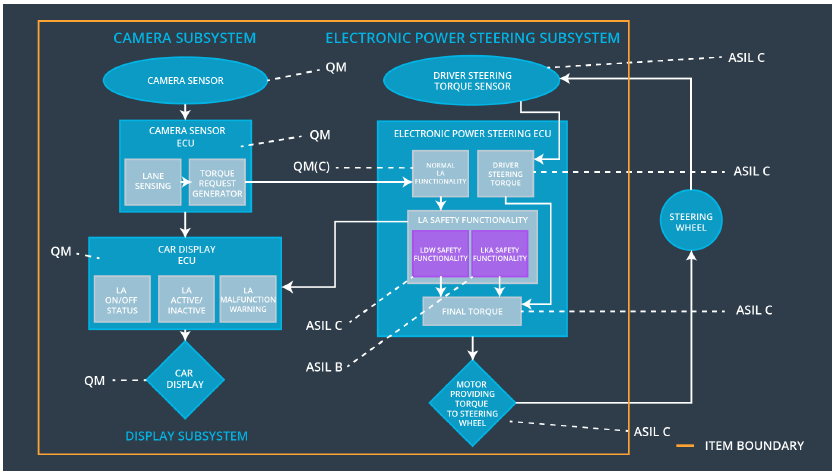
The purpose of the technical safety concept is to identify new requirements and allocate these high-level hardware and software requirements to system diagrams for the lane assistance functional safety project as pertain to the potential malfunctions of the electrical and electronic systems as defined by ISO 26262 standard or tailored version as per organization.

# 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 | 50ms | Set vibration  torque amplitude  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 | 50ms | Set vibration  torque amplitude  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 | 500ms | Set lane keeping  assistance  torque to zero |
| Functional  Safety  Requirement  02-02 | The electronic power steering ECU shall  ensure that the lane keeping assistance  torque is set to zero when the camera  sensor ECU stops detecting road markings  and shall send its off status to the Car  Display. | B | 500ms | Set lane keeping  assistance  torque to zero |

## Refined System Architecture from Functional Safety Concept



### 

### Functional overview of architecture elements

|  |  |
| --- | --- |
| **Element** | **Description** |
| Camera Sensor | Sensor responsible for capturing vehicle driving  condition including detectable lane lines. |
| Camera Sensor ECU - Lane Sensing | Software Module in the Camera Sensor ECU  responsible for detecting lane lines and determining  when the vehicle leaves the lane by mistake. |
| Camera Sensor ECU - Torque request generator | Software Module in the Camera Sensor ECU  responsible for calculating and sending the  additional torque for the LDW and LKA functions. |
| Car Display | Visual display responsible to displaying warning of  lane departures and LKA and LDW activation and  deactivations. |
| Car Display ECU - Lane Assistance On/Off Status | Visual display responsible to displaying LKA and  LDW ON/OFF status. |
| Car Display ECU - Lane Assistant Active/Inactive | Visual display responsible to displaying warning of lane departures, LKA and LDW activation and deactivations. |
| Car Display ECU - Lane Assistance malfunction warning | Visual display responsible to displaying warning of  LKA and LDW malfunctions. |
| Driver Steering Torque Sensor | Sensor responsible for measuring how much force  (steering torque) the driver is applying to the  steering wheel. |
| Electronic Power Steering (EPS) ECU - Driver Steering Torque | Software Module in the electronic power steering  ECU responsible for receiving the Camera Sensor  ECU torque requests. |
| EPS ECU - Normal Lane Assistance Functionality | Software Module in the electronic power steering  ECU responsible for receiving the Driver Steering  torque sensor input from the steering wheel. |
| EPS ECU - Lane Departure Warning Safety Functionality | Software Module in the electronic power steering  ECU responsible for keeping the lane departure  oscillating torque amplitude and frequency below  MAX\_Torque\_Amplitude and  MAX\_Torque\_Fequency respectively. |
| EPS ECU - Lane Keeping Assistant Safety Functionality | Software Module in the electronic power steering  ECU responsible for ensuring the application of the  lane keeping assistance torque does not ever  exceeded Max\_Duration and if lane detection is  lost, the LKA function is deactivated. |
| EPS ECU - Final Torque | Software Module in the electronic power steering  ECU responsible for ensuring the LDW, LKA and  the driver’s steering torque requests are combined  and sent to the Motor. |
| Motor | Actuator responsible for applying requested torque  to the steering column by the Electronic Power  Steering ECU for either the LKA or the LDW  functions. |

# Technical Safety Concept

## Technical Safety Requirements

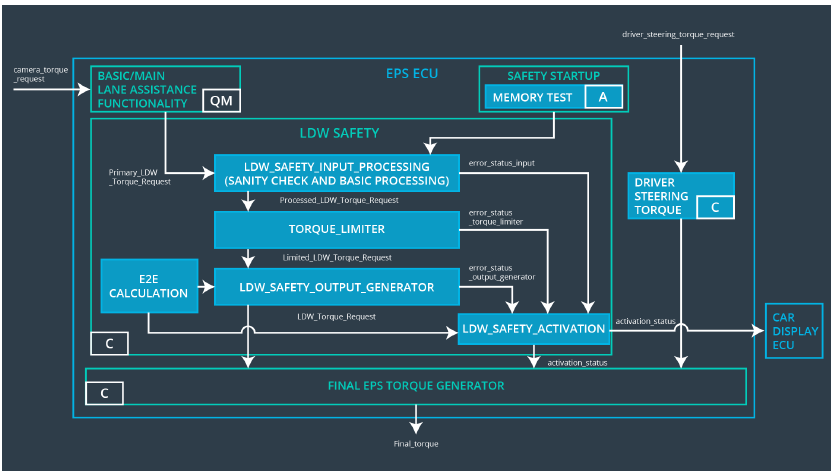
**Lane Departure Warning (LDW) Requirements:**

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:

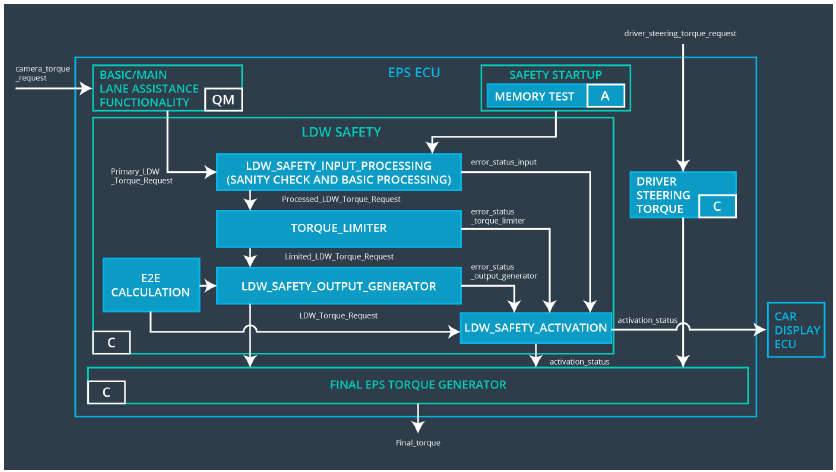


|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **ID** | **Technical Safety Requirement** | **ASIL** | **Fault Tolerant Time Interval** | **Architecture Allocation** | **Safe State** |
| Technical  Safety  Requirement-  01 | The LDW safety component  shall ensure that the amplitude  of the 'LDW\_Torque\_Request'  sent to the 'Final electronic power steering Torque’ component is below ‘MAX\_TORQUE\_Amplitude. | C | 50ms | LDW Safety block. | Set lane  departure  warning  torque 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 | 50ms | LDW Safety block | Set lane  departure  warning  torque 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 | 50ms | LDW Safety block | Set lane  departure  warning  torque to zero. |
| Technical  Safety  Requirement  04 | The validity and integrity of the  data transmission for  'LDW\_Torque\_Request' signal  shall be ensured. | C | 50ms | LDW Safety block. | Set lane  departure  warning  torque to zero. |
| 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 | Data Transmission Integrity Check. | Set lane  departure  warning  torque 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 frequency of the  'LDW\_Torque\_Request' sent to the  'Final electronic power steering  Torque' component is below  'Max\_Torque\_Fequency. | C | 50ms | LDW Safety block | Set lane departure warning torque to zero. |

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

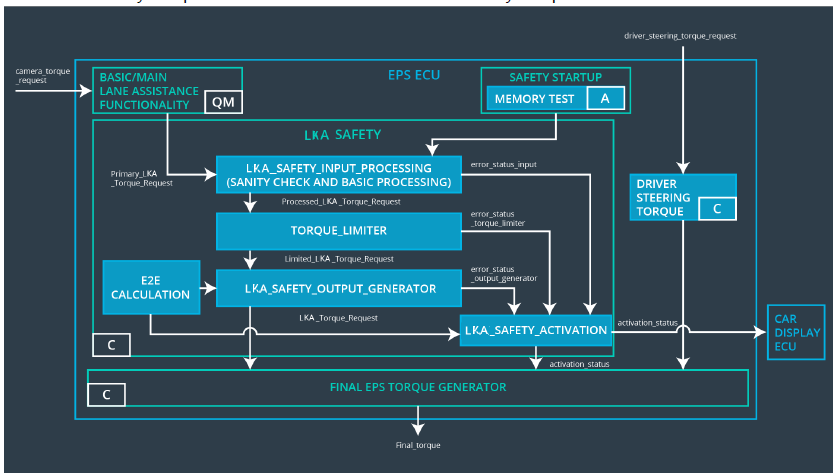
**Lane Keeping Assistance (LKA) Requirements:**

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 |  |  |

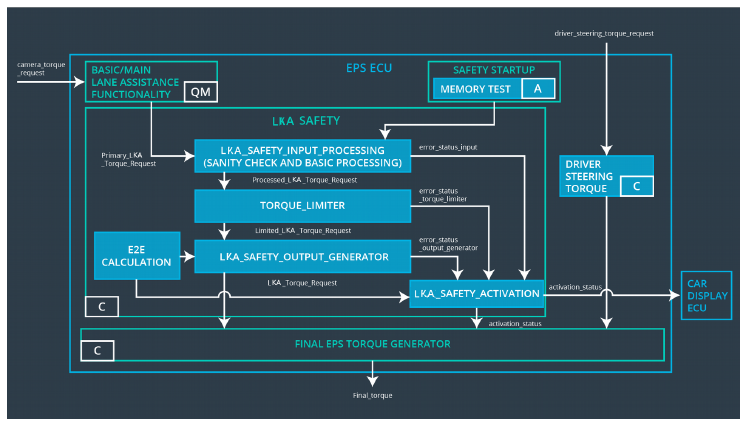
Technical Safety Requirements related to Functional Safety Requirement 02-01 are:



|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **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 duration of the  lane keeping assistance torque  applied is less than  Max\_Duration.\_time. | C | 500ms | LKA Safety Block | Set Keeping assistance torque 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 | C | 500ms | LKA Safety Block | Set Keeping assistance torque 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. | C | 500ms | LKA Safety Block | Set Keeping assistance torque to zero |
| Technical  Safety  Requirement  04 | The validity and integrity of the  data transmission for  'LKA\_Torque\_Request' signal  shall be ensured. | C | 500ms | LKA Safety Block | Set Keeping assistance torque to zero |
| Technical  Safety  Requirement  05 | Memory test shall be conducted  at startup of the EPS ECU to  check for any faults in memory | C | Ignition cycle | Data Transmission Integrity Check | Set lane Keeping assistance torque to 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  01 | The electronic power steering  ECU shall ensure that the lane  keeping assistance torque is set  to zero when the camera sensor  ECU stops detecting road  markings and shall send its off  status to the Car Display. | X |  |  |

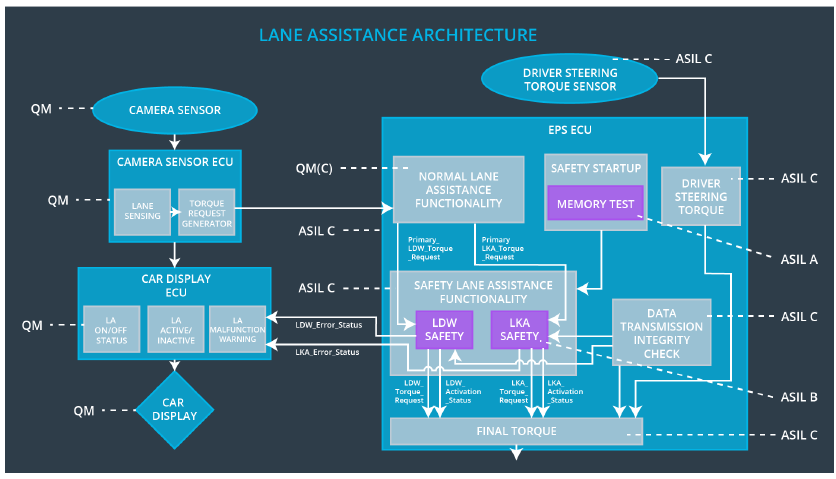


|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **ID** | **Functional Safety Requirement** | **A**  **S**  **I**  **L** | **Electronic Power Steering ECU** | **Camera ECU** | **Car Display ECU** |
| Functional  Safety  Requirement  01 | The LKA safety component shall  ensure that the loss of camera  sensor torque request  transmission will deactivate the  LKA feature and the  'LKA\_Torque\_Request' shall be  set to zero | C | 500ms | LKA Safety block | Set lane keeping assistance torque to zero |

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

|  |  |  |
| --- | --- | --- |
| **ID** | **Validation Acceptance Criteria and Method** | **Verification Acceptance Criteria and Method** |
| Technical  Safety  Requirement  01 | Validate that the Max\_Duration set is the chosen from LKA Validation Acceptance Criteria. | Verify that the system really does turn  off if the lane keeping assistance  'LKA\_Torque\_Request' ever exceeded  Max\_Duration |
| Technical  Safety  Requirement  02 | Validate that the “TORQUE\_LIMITER” in  the “ LKA Safety” software block sends the error\_status\_torque\_limiter signal to the LKA\_SAFETY\_ACTIVATION. | Verify that the Car Display ECU  displays the LKA malfunction warning  light. |
| Technical  Safety  Requirement  03 | Validate that the “TORQUE\_LIMITER” in  the “ LKA Safety” software block sends a zero LKA\_Torque\_Request | Verify that the Final EPS TORQUE  Generator receives a 0  LKA\_Torque\_Request |
| Technical  Safety  Requirement  04 | Validate that the “TORQUE\_LIMITER” in the “ LKA Safety” software block  calculate and sends a correct CRC and Alive counter for data transmission validity and integrity. | Verify that the system really does turn  off if the lane keeping assistance  “LKA\_Torque\_Request” ever has an invalid CRC or Alive counter. |
| Technical  Safety  Requirement  05 | Validate that the Safety Startup Memory  test to check memory faults will catch  memory faults. | Verify that the LKA system really does  turn off if the Safety Startup Memory  test fails. |
| Technical  Safety  Requirement  06 | Validate that the camera ECU sends zero ‘LKA\_Torque\_Request’ when it fails to detect lane lines and stop Alive counter for data transmission validity and integrity. | Verify that the system really does turn  off if the lane keeping assistance  'LKA\_Torque\_Request' ever has an  invalid CRC or Alive counter failure  from the camera ECU. |

## Refinement of the System Architecture



|  |  |
| --- | --- |
| **Element** | **Description** |
| Camera Sensor | Sensor responsible for capturing vehicle driving condition including detectable lane lines. |
| Camera Sensor ECU - Lane Sensing | Software Module in the Camera Sensor ECU responsible for detecting lane lines and determining when the vehicle leaves the lane by mistake. |
| Camera Sensor ECU - Torque request generator | Software Module in the Camera Sensor ECU responsible for calculating and sending the additional torque for the LDW and LKA functions with CRC and Alive counter for data transmission validity and integrity check. |
| Car Display | Visual display responsible to displaying warning of  lane departures and LKA and LDW activation and  deactivations. |
| Car Display ECU - Lane Assistance On/Off Status | Visual display responsible to displaying LKA and  LDW ON/OFF status. |
| Car Display ECU - Lane Assistant  Active/Inactive | Visual display responsible to displaying warning of lane departures, LKA and LDW activation and deactivations. |
| Car Display ECU - Lane Assistance malfunction warning | Visual display responsible to displaying warning of  LKA and LDW malfunctions. |
| Driver Steering Torque Sensor | Sensor responsible for measuring how much force  (steering torque) the driver is applying to the  steering wheel. |
| Electronic Power Steering (EPS) ECU -Driver Steering Torque | Software Module in the electronic power steering  ECU responsible for receiving the Camera Sensor  ECU torque requests. |
| EPS ECU - Normal Lane Assistance Functionality | Software Module in the electronic power steering  ECU responsible for receiving the Driver Steering  torque sensor input from the steering wheel |
| ESP ECU – Safety Startup – Memory Test | Software Module in the electronic power steering  ECU responsible for the memory test conducted at  startup of the EPS ECU to check for any faults in  memory. |
| EPS ECU - Lane Departure Warning Safety Functionality | Software Module in the electronic power steering  ECU responsible for keeping the lane departure  oscillating torque amplitude and frequency below  MAX\_Torque\_Amplitude and  MAX\_Torque\_Fequency respectively |
| EPS ECU - Lane Keeping Assistant Safety Functionality | Software Module in the electronic power steering  ECU responsible for ensuring the application of the  lane keeping assistance torque does not ever  exceeded Max\_Duration and if lane detection is  lost, the LKA function is deactivated. |
| ESP ECU – Data Transmission Integrity  Check | Software Module in the electronic power steering  ECU responsible for checking the data validity and  integrity of the data transmission |
| EPS ECU - Final Torque | Software Module in the electronic power steering  ECU responsible for ensuring the LDW, LKA and  the driver’s steering torque requests are combined  and sent to the Motor. |
| Motor | Actuator responsible for applying requested torque  to the steering column by the Electronic Power  Steering ECU for either the LKA or the LDW  functions. |

## Allocation of Technical Safety Requirements to Architecture Elements

All Technical Safety requirement has been allocated to the Electronic Power Steering ECU. The table summarize what already identified in the technical safety requirement section.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Technical safety Requirement** | **Electronic Power Steering ECU** | **Camera ECU** | **Car Display ECU** |
| Technical  Safety  Requirement  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. | X |  |  |
| Technical  Safety  Requirement  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. | X |  |  |
| Technical  Safety  Requirement  01-03 | 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. | X |  |  |
| Technical  Safety  Requirement  01-04 | The validity and integrity of the  data transmission for  'LDW\_Torque\_Request' signal  shall be ensured. | X |  |  |
| Technical  Safety  Requirement  01-05 | Memory test shall be conducted  at startup of the EPS ECU to  check for any faults in memory. | X |  |  |
| Technical  Safety  Requirement  01-06 | The LDW safety component shall  ensure that the fequency of the  'LDW\_Torque\_Request' sent to  the 'Final electronic power  steering Torque' component is  below 'Max\_Torque\_Fequency. | X |  |  |

## Warning and Degradation Concept

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Degradation Mode** | **Trigger for Degradation Mode** | **Safe State invoked** | **Driver Warning** |
| WDC-01 | Turn off LDW functionality | Malfuntion\_01, Malfunction\_02 | Yes, LDW torque  shall be set to  zero | Lane Assist  Inactive and  Malfunction  Warning will be  set in the Car  Display ECU |
| WDC-02 | Turn off LKA functionality | Malfunction\_04,Malfunction\_05 | Yes, LKA torque  shall be set to  zero | Lane Assist  Inactive and  Malfunction  Warning will be  set in the Car  Display ECU |