

Technical Safety Concept Lane Assistance

**Document Version: [Version]**

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



# Document history

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Editor | Description |
| 06/13/2018 | 1.0 | Swapnil More | First Draft |
| 06/15/2018 | 1.1 | Swapnil More | Updates to First Draft |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# 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 look at the item from a system-level perspective, refine the functional safety requirements as technical safety requirements. It is defined in the product development phase as it is more concrete and gets into the details of the item's technology. It assigns functions to specific sub-level of the systems according to ISO 26262.

# 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 electronic power steering ECU  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 electronic power steering ECU  shall ensure that the lane departure  oscillating torque frequency is below  Max\_Torque\_Frequency. | C | 50 ms | 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\_Assist\_Time | B | 500 ms | Assistance time is below Max\_Assist\_Time |

## Refined System Architecture from Functional Safety Concept



### Functional overview of architecture elements

|  |  |
| --- | --- |
| **Element** | **Description** |
| Camera Sensor | Capture images and send them to the Camera Sensor ECU |
| Camera Sensor ECU - Lane Sensing | Process Images to detect lane lines and calculate vehicle position w.r.t. the lane lines |
| Camera Sensor ECU - Torque request generator | Calculate the torque required to maintain vehicle in the lane. |
| Car Display | Display the Lane Departure Warning and status of the Lane Assistance System |
| Car Display ECU - Lane Assistance On/Off Status | Identify the status of the Lane Assistance System (ON/OFF) |
| Car Display ECU - Lane Assistant Active/Inactive | Identify the status of the Lane Assistance System (Active/Inactive) |
| Car Display ECU - Lane Assistance malfunction warning | Identify Lane Assistance Malfunction |
| Driver Steering Torque Sensor | Measure the torque applied to the steering  wheel by the 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 | Software module ensuring the Lane Keeping  Assistance functionality application is not  activate more than Max\_Assist\_Time time. |
| EPS ECU - Final Torque | Combine the torque request from the Lane  Keeping and Lane Departure Warning  functionalities and sends them to the Motor. |
| Motor | Applies the required torque 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 | Lane  Departure  Warning  Torque Request Amplitude shall be set to  zero. |
| Technical  Safety  Requirement  01-01-02 | When the LDW is  deactivated, the ‘LDW  Safety’ software module  shall send a signal to the  Car Display ECU to turn  on a warning signal. | C | 50 ms | LDW Safety | Lane  Departure  Warning  Torque Request Amplitude shall be set to  zero. |
| Technical  Safety  Requirement  01-01-03 | When a failure is  detected by the Lane  Departure Warning  functionality, it shall  deactivate the Lane  Departure Warning  feature and set  ‘LDW\_Torque\_Request’  to zero. | C | 50 ms | LDW Safety | Lane  Departure  Warning  Torque Request Amplitude shall be 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 | Lane  Departure  Warning  Torque Request Amplitude shall be set to  zero. |
| Technical  Safety  Requirement  01-01-05 | Memory test shall be  conducted at startup of  the EPS ECU to check  for any memory problems | A | Ignition cycle | Memory Test | Lane  Departure  Warning  Torque Request Amplitude shall be set to  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 Lane Departure Warning  safety component shall ensure  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 | Lane  Departure  Warning  Torque Request Frequency shall be set to  zero. |
| Technical  Safety  Requirement  01-02-02 | When the LDW is  deactivated, the ‘LDW  Safety’ software module  shall send a signal to the  Car Display ECU to turn  on a warning signal. | C | 50 ms | LDW Safety | Lane  Departure  Warning  Torque Request Frequency shall be set to  zero. |
| Technical  Safety  Requirement  01-02-03 | When a failure is  detected by the Lane  Departure Warning  functionality, it shall  deactivate the Lane  Departure Warning  feature and set  ‘LDW\_Torque\_Request’  to zero. | C | 50 ms | LDW Safety | Lane  Departure  Warning  Torque Request Frequency shall be set to  zero. |
| Technical  Safety  Requirement  01-02-04 | The validity and integrity  of the data transmission  for  ‘LDW\_Torque\_Request’ signal shall be ensured. | C | 50 ms | Data Transmission Integrity Check | Lane  Departure  Warning  Torque Request Frequency shall be set to  zero. |
| Technical  Safety  Requirement  01-02-05 | Memory test shall be  conducted at startup of  the EPS ECU to check  for any memory problems | A | Ignition cycle | Memory Test | Lane  Departure  Warning  Torque Request Frequency shall be set to  zero. |

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

|  |  |  |
| --- | --- | --- |
| **ID** | **Validation Acceptance Criteria**  **and Method** | **Verification Acceptance Criteria**  **and Method** |
| Technical  Safety  Requirement  01-01-01 | Validate the  Max\_Torque\_Amplitude is the  chosen from the Lane Departure  Warning Validation | Verify the Lane Departure Warning  functionality is turned off. |
| Technical  Safety  Requirement  01-01-02 | Validate the ‘TORQUE\_LIMITER’  sends the error\_status\_torque\_limiter signal  to the  LDW\_SAFETY\_ACTIVATION. | Verify the Car Display ECU  displays the Lane Departure  Warning malfunction warning  signal. |
| Technical  Safety  Requirement  01-01-03 | Validate the ‘TORQUE\_LIMITER’  sends ‘LDW\_Torque\_Request’ with  zero. | Verify the Final EPS Torque  generator receives a  LDW\_Torque\_Request of zero. |
| Technical  Safety  Requirement  01-01-04 | Validate the ‘TORQUE\_LIMITER’  calculate and sends the correct  cyclic redundancy check (CRC)  and Alive counter for data  transmission validity and integrity. | Verify the functionality is turn off if  there is a CRC or Alive counter  discrepancy. |
| Technical  Safety  Requirement  01-01-05 | Validate the Safety Startup  Memory test to check memory  faults catch memory faults. | Verify the Lane Departure Warning  is turned off when the Safety  Startup Memory fails. |
| Technical  Safety  Requirement  01-02-01 | Validate the  Max\_Torque\_Frequency set is chosen from the Lane Departure  Warning Acceptance Criteria. | Max\_Torque\_Request. |

**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  02-01-01 | The Lane Keeping Assistance safety component shall ensure the duration of the lane keeping assistance torque is applied for less than Max\_Duration | B | 500 ms | LKA Safety | Lane Keeping Assistance Torque shall be set to zero. |
| Technical  Safety  Requirement  02-01-02 | When the Lane Keeping Assistance function deactivates, the ‘LKA Safety’ shall send a signal to the Car Display ECU to turn on a warning light. | B | 500 ms | LKA Safety | Lane Keeping Assistance Torque shall be set to zero. |
| Technical  Safety  Requirement  02-01-03 | When a failure is detected, the Lane Keeping Assistance function shall deactivate and the ‘LKA\_Torque\_Request’ shall be zero. | B | 500 ms | LKA Safety | Lane Keeping Assistance Torque shall be 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. | B | 500 ms | Data Transmission Integrity Check | Lane Keeping Assistance Torque shall be set to zero. |
| Technical  Safety  Requirement  02-01-05 | Memory test shall be conducted at startup of the EPS ECU to check for any memory problems | A | Ignition cycle | Memory Test | Lane Keeping Assistance Torque shall be set 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  02-01-01 | Validate the Max\_Duration is set to the chosen value from LKA Validation Assistance Criteria | Verify the functionality is turned off after it is applied for Max\_Duration. |
| Technical  Safety  Requirement  02-01-02 | Validate the ‘TORQUE\_LIMITER’ sends the error\_status\_torque\_limiter signal to the LKA\_SAFETY\_ACTIVATION. | Verify the Car Display ECU displays the Lane Keeping Assistance malfunction warning signal. |
| Technical Safety Requirement  02-01-03 | Validate the ‘TORQUE\_LIMITER’ sends ‘LKA\_Torque\_Request’ with zero. | Verify the Final EPS Torque generator receives a LKA\_Torque\_Request of zero. |
| Technical Safety Requirement 02-01-04 | Validate the ‘TORQUE\_LIMITER’ calculate and sends the correct cyclic redundancy check (CRC) and Alive counter for data transmission validity and integrity. | Verify the functionality is turn off if there is a CRC or Alive counter discrepancy. |
| Technical Safety Requirement  02-01-05 | Validate the Safety Startup Memory test to check memory faults catch memory faults. | Verify the Lane Keeping Assistance is turned off when the Safety Startup Memory fails. |

## 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 Lane Departure Warning 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  01-01-02 | When the Lane Departure Warning is deactivated, the ‘LDW Safety’ software module shall send a signal to the Car Display ECU to turn on a warning signal. | **X** |  |  |
| Technical  Safety  Requirement  01-01-03 | When a failure is detected by the Lane Departure Warning functionality, it shall deactivate the Lane Departure Warning feature and set ‘LDW\_Torque\_Request’ to zero. | **X** |  |  |
| Technical  Safety  Requirement  01-01-04 | The validity and integrity of the data transmission for ‘LDW\_Torque\_Request’ signal shall be ensured. | **X** |  |  |
| Technical  Safety  Requirement  01-01-05 | Memory test shall be conducted at startup of the EPS ECU to check for any memory problems | **X** |  |  |
| Technical  Safety  Requirement  01-02-01 | The Lane Departure Warning safety component shall ensure the frequency of the ‘LDW\_Torque\_Reques’ sent to the ‘Final electronic power steering Torque’ component is below ‘Max\_Torque\_Frequency.’ | **X** |  |  |
| Technical  Safety  Requirement  02-01-01 | The Lane Keeping Assistance safety component shall ensure the duration of the lane keeping assistance torque is applied for less than Max\_Duration | **X** |  |  |
| Technical  Safety  Requirement  02-01-02 | When the Lane Keeping Assistance function deactivates, the ‘LKA Safety’ shall send a signal to the Car Display ECU to turn on a warning light. | **X** |  |  |
| Technical  Safety  Requirement  02-01-03 | When a failure is detected, the Lane Keeping Assistance function shall deactivate and the ‘LKA\_Torque\_Request’ shall be zero. | **X** |  |  |
| Technical  Safety  Requirement  02-01-04 | The validity and integrity of the data transmission for ‘LKA\_Torque\_Request’ signal shall be ensured. | **X** |  |  |
| Technical  Safety  Requirement  02-01-05 | Memory test shall be conducted at start up of the EPS ECU to check for any memory problems | **X** |  |  |

## Warning and Degradation Concept

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