

Technical Safety Concept Lane Assistance

**Document Version: 1.0**

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



# Document history

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Editor | Description |
| 208/27/2018 | 1.0 | [NOT\_PUBLIC] | First submission of completed 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

The technical safety concept is similar to the functional safety concept. However, the ISO 26262 standard places the functional safety concept in the concept phase while the technical safety concept is part of the product development phase. This is because the technical safety concept is more concrete and gets into the details of the item’s technology. The technical safety concept involves turning functional safety requirements into technical safety requirements and allocating those to the system architecture. When multiple subsystems are involved, the technical safety concept might be divided into more than one document.

# 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 | Lane Assistance functionality deactivated |
| 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 | Lane Assistance functionality deactivated |
| 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 | 500 ms | Lane Assistance functionality deactivated |

## Refined System Architecture from Functional Safety Concept



### Functional overview of architecture elements

|  |  |
| --- | --- |
| **Element** | **Description** |
| Camera Sensor | Captures images and provides them to the Camera Sensor ECU. |
| Camera Sensor ECU - Lane Sensing | Software module that detects the lane lines in the image provided by the Camera Sensor. |
| Camera Sensor ECU - Torque request generator | Software module that calculates the torque to be requested to the Electronic Power Steering ECU in order to get the center of the ego lane. |
| Car Display | Provides visual feedback (warning light) to the driver in the display dashboard. |
| Car Display ECU - Lane Assistance On/Off Status | Software module that controls the warning lamp indicating whether the Lane Assistance System is on or off. |
| Car Display ECU - Lane Assistant Active/Inactive | Software module that controls the warning lamp indicating whether the Lane Assistance System is working properly. |
| Car Display ECU - Lane Assistance malfunction warning | Software module that controls the warning lamp indicating that a malfunction in the Lane Assistance System has occurred. |
| Driver Steering Torque Sensor | Senses the torque already applied to the steering wheel by the driver. |
| Electronic Power Steering (EPS) ECU - Driver Steering Torque | Software module that processes the received torque request from the driver. |
| EPS ECU - Normal Lane Assistance Functionality | Software module that receives the torque request from the Camera Sensor ECU and performs no safety critical tasks. |
| EPS ECU - Lane Departure Warning Safety Functionality | Software module that checks for malfunction (exceeding Max\_Torque\_Amplitude or Max\_Torque\_Frequency) and calculates final torque request |
| EPS ECU - Lane Keeping Assistant Safety Functionality | Software module that ensures duration is below Max\_Duration. |
| EPS ECU - Final Torque | Software module that sends the final torque request to the motor. |
| Motor | Applies the torque calculated by the Electronic Power Steering ECU 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 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 | Torque request amplitude set 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 | 50 ms | LDW Safety | Torque request amplitude set 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 | 50 ms | LDW Safety | Torque request amplitude set to zero |
| Technical  Safety  Requirement  04 | The validity and integrity of the data transmission for 'LDW\_Torque\_Request' signal shall be ensured. | C | 50 ms | LDW Safety | Torque request amplitude set to zero |
| Technical  Safety  Requirement  05 | Memory test shall be conducted at start up of the EPS ECU to check for any faults in memory. | A | Ignition cycle | LDW Safety | Torque request amplitude 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 | 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\_Frequency’. | C | 50 ms | LDW Safety | Torque request frequency set 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 | 50 ms | LDW Safety | Torque request frequency set 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 | 50 ms | LDW Safety | Torque request frequency set to zero |
| Technical  Safety  Requirement  04 | The validity and integrity of the data transmission for 'LDW\_Torque\_Request' signal shall be ensured. | C | 50 ms | LDW Safety | Torque request frequency set to zero |
| Technical  Safety  Requirement  05 | Memory test shall be conducted at start up of the EPS ECU to check for any faults in memory. | A | Ignition cycle | LDW Safety | Torque request frequency set to 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 the duration of the 'LKA\_Torque\_Request' sent to the 'Final electronic power steering Torque' component is below 'Max\_Duration’. | B | 500 ms | LKA Safety | Torque request set 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. | B | 500 ms | LKA Safety | Torque request set 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. | B | 500 ms | LKA Safety | Torque request set to zero |
| Technical  Safety  Requirement  04 | The validity and integrity of the data transmission for 'LKA\_Torque\_Request' signal shall be ensured. | B | 500 ms | LKA Safety | Torque request set to zero |
| Technical  Safety  Requirement  05 | Memory test shall be conducted at start up of the EPS ECU to check for any faults in memory. | A | Ignition cycle | LKA Safety | Torque request set to zero |

## Refinement of the System Architecture

****

## Allocation of Technical Safety Requirements to Architecture Elements

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Functional Safety Requirement** | **Electronic Power Steering ECU** | **Camera ECU** | **Car Display ECU** |
| 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’. | X | **–** | **–** |
| Technical Safety Requirement 01-01-02 | 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 01-01-03 | 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 01-01-04 | 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 start up of the EPS ECU to check for any faults in memory. | X | **–** | **–** |
| Technical Safety Requirement 01-02-01 | 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\_Frequency’. | X | **–** | **–** |
| Technical Safety Requirement 01-02-02 | 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 01-02-03 | 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 01-02-04 | The validity and integrity of the data transmission for 'LDW\_Torque\_Request' signal shall be ensured. | X | **–** | **–** |
| Technical Safety Requirement 01-02-05 | Memory test shall be conducted at start up of the EPS ECU to check for any faults in memory. | X | **–** | **–** |
| Technical Safety Requirement 02-01-01 | The LKA safety component shall ensure that the duration of the 'LKA\_Torque\_Request' sent to the 'Final electronic power steering Torque' component is below 'Max\_Duration’. | X | **–** | **–** |
| Technical Safety Requirement 02-01-02 | 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. | X | **–** | **–** |
| Technical Safety Requirement 02-01-03 | 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. | 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 faults in memory. | X | **–** | **–** |

## Warning and Degradation Concept

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Degradation Mode** | **Trigger for Degradation Mode** | **Safe State invoked?** | **Driver Warning** |
| WDC-01 | Deactivate the system | Malfunction\_01  Malfunction\_02 | Yes | Warning light on display dashboard |
| WDC-02 | Deactivate the system | Malfunction\_03 | Yes | Warning light on display dashboard |