

Technical Safety Concept Lane Assistance

**Document Version: [Version]**

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



# Document history

**[Instructions: Fill in the date, version and description fields. You can fill out the Editor field with your name if you want to do so. Keep track of your editing as if this were a real world project.**

**For example, if this were your first draft or first submission, you might say version 1.0. If this is a second submission attempt, then you'd add a second line with a new date and version 2.0]**

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Editor | Description |
| 26/12/2018 | 1.0 | Manjunath Gasthi | Initial version |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# 

# Table of Contents

**[Instructions: We have provided a table of contents. If the table of contents is not showing up correctly in your word processor of choice, please update it. The table of contents should show each section of the document and page numbers or links. Most word processors can do this for you. In** [**Google Docs**](https://support.google.com/docs/answer/116338?co=GENIE.Platform%3DDesktop&hl=en)**, you can use headings for each section and then go to Insert > Table of Contents.** [**Microsoft Word**](https://support.microsoft.com/en-us/help/285059/how-to-create-a-table-of-contents-by-marking-text-in-word) **has similar capabilities]**

[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

In this document new requirements are defined and assigned to the system architecture. These

requirements are more concrete and gets into details of the item’s technology as specified by

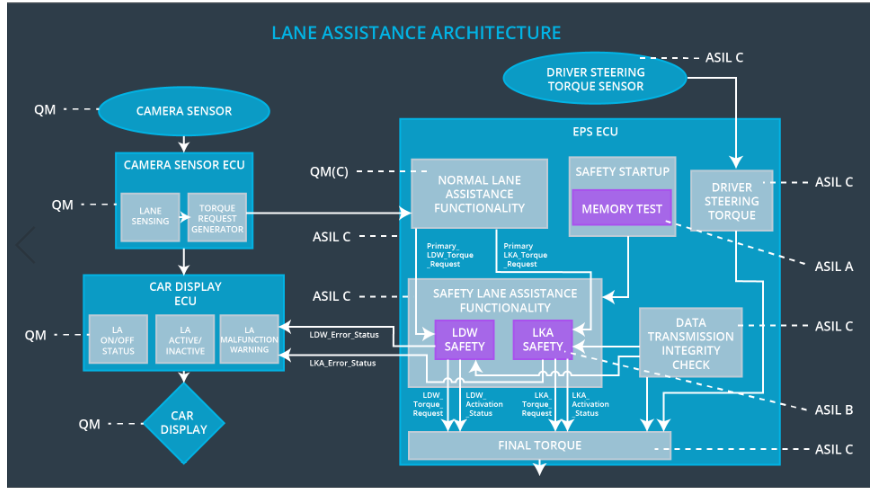
ISO 26262.

# 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 | Test and validate that the  Max\_Torque\_Amplitude chosen is low  enough that the driver does not loose  control over the car. | C | 50mS | Vibration torque  amplitude is  below  Max\_Torque\_Am  plitude. |
| Functional  Safety  Requirement  01-02 | Test and validate that the  Max\_Torque\_Frequency chosen is low  enough that the driver does not loose  control over the car. | C | 50mS | Vibration  frequency is  below  Max\_Torque\_Fre  quency. |
| 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 | Lane Keeping  Assistance  torque is zero. |

## Refined System Architecture from Functional Safety Concept



### 

### Functional overview of architecture elements

|  |  |
| --- | --- |
| **Element** | **Description** |
| Camera Sensor | Capture road images and provide them to the  Camera Sensor ECU. |
| Camera Sensor ECU - Lane Sensing | Software module detecting the lane line  positions from the Camera Sensor images. |
| Camera Sensor ECU - Torque request generator | Software module calculating the necessary  torque to be requested to the Electronic Power  Steering ECU. |
| Car Display | Display warning for the driver. |
| Car Display ECU - Lane Assistance On/Off Status | Indicate the status of the Lane Assistance  functionality (On/Off.) |
| Car Display ECU - Lane Assistant Active/Inactive | Indicate if the Lane Assistance functionality is  properly functioning (Active/Inactive.) |
| Car Display ECU - Lane Assistance malfunction warning | Indicate a malfunction on the Lane Assistance  functionality. |
| 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\_duration 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  wheels. |

# 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 electronically  power steering Torque‘  component is below  'Max\_Torque\_Amplitude’. | C | 50 mS | LDW Safety | LDW Torque  Request  Amplitude  shall be set to  zero. |
| Technical  Safety  Requirement  02 | The validity and integrity of the  data transmission for  'LDW\_Torque\_Request’ signal  shall be ensured. | C | 50 mS | LDW Safety | LDW Torque  Request  Amplitude  shall be 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 | LDW Torque  Request  Amplitude  shall be set to  zero. |
| Technical  Safety  Requirement  04 | 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 | LDW Torque  Request  Amplitude  shall be 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 | Data  Transmission  Integrity  Check | LDW Torque  Request  Amplitude  shall be set 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 electronically power  steering Torque‘ component is  below 'Max\_Torque\_Frequency’. | C | 50 mS | LDW Safety | LDW  Torque  Request  Frequency  shall be  set to  zero. |
| Technical  Safety  Requirement  02 | The validity and integrity of the  data transmission for  'Max\_Torque\_Frequency’ signal  shall be ensured. | C | 50 mS | LDW Safety | LDW  Torque  Request  Frequency  shall be  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 'Max\_Torque\_Frequency‘ shall  be set to zero. | C | 50 mS | LDW Safety | LDW  Torque  Request  Frequency  shall be  set to  zero. |
| Technical  Safety  Requirement  04 | 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 | LDW  Torque  Request  Frequency  shall be  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 | Data  Transmissio  n Integrity  Check | LDW  Torque  Request  Frequency  shall be  set to  zero. |

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

Functional Safety Requirement 02-1 with its associated system elements

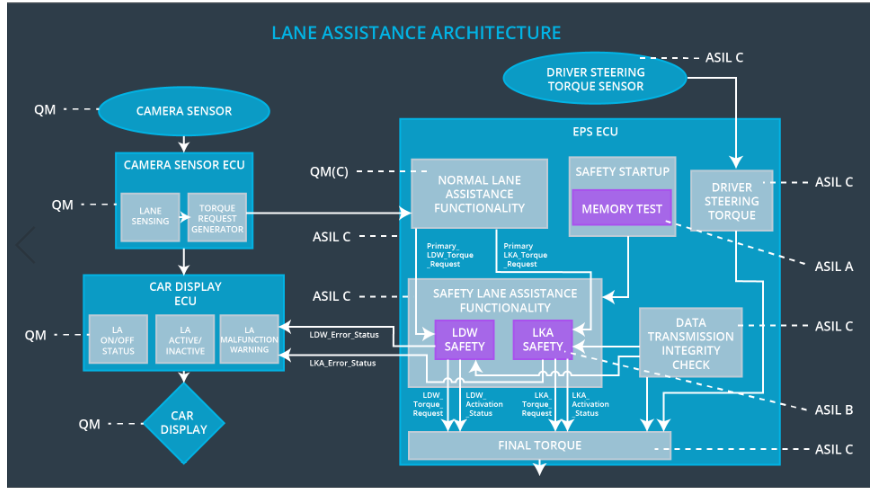
(derived in the functional safety concept)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **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 Lane Keeping  Assistance safety  component shall ensure the  duration of the lane keeping  assistance torque is applied  for less than Max\_Duration | C | 500 ms | LKA Safety | Lane  Keeping  Assistance  torque to  zero. |
| Technical  Safety  Requirement  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. | C | 500 ms | LKA Safety | Lane  Keeping  Assistance  torque to  zero. |
| Technical  Safety  Requirement  03 | When a failure is detected,  the Lane Keeping  Assistance function shall  deactivate and the  ‘LKA\_Torque\_Request’ shall  be zero. | C | 500 ms | LKA Safety | Lane  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 | 500 ms | LKA Safety | Lane  Keeping  Assistance  torque to  zero. |
| Technical  Safety  Requirement  05 | Memory test shall be  conducted at start up of the  EPS ECU to check for any  memory problems | A | Ignition  cycle | Data  Transmission  Integrity  Check | Lane  Keeping  Assistance  torque to  zero. |

## 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 LDW safety component shall  ensure that the amplitude of the  'LDW\_Torque\_Request‘ sent to  the ‘Final electronically power  steering Torque‘ component is  below 'Max\_Torque\_Amplitude’. | X |  |  |
| Technical  Safety  Requirement  01-01-02 | The validity and integrity of the  data transmission for  'LDW\_Torque\_Request’ signal  shall be ensured. | X |  |  |
| Technical  Safety  Requirement  01-01-03 | 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  01-01-04 | 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  01-01-05 | Memory test shall be  conducted at start up of the  EPS ECU to check for any  memory problems | 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 electronically power  steering Torque‘ component is  below 'Max\_Torque\_Frequency’. | X |  |  |
| Technical  Safety  Requirement  01-02-02 | The validity and integrity of the  data transmission for  'Max\_Torque\_Frequency’ signal  shall be ensured. | 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 'Max\_Torque\_Frequency‘  shall be set to zero. | X |  |  |
| Technical  Safety  Requirement  01-02-04 | 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  01-02-05 | 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 the duration of the lane  keeping assistance torque is  applied for less than  Max\_Duration. | X |  |  |
| Technical  Safety  Requirement  02-01-02 | The validity and integrity of the  data transmission for  ‚LKA\_Torque\_Request’ signal  shall be ensured. | 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 | 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  02-01-05 | 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 | Turn system off. | Malfunction\_01  Malfunction\_02 | Yes | Warning light on  the dashboard |
| WDC-02 | Turn system off. | Malfunction\_03 | Yes | Warning light on  the dashboard |