

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 |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# 

# 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

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

Purpose of a technical safety concept is to define new requirements and then allocating those requirements to system architecture in a low level. Technical Safety concept is looking at the safety requirements of sensors, control units and actuators.

# Inputs to the Technical Safety Concept

## Functional Safety Requirements

**[Instructions: Provide the functional safety requirements derived in the functional safety concept ]**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **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\_Amplitue | C | 50 ms | LDW will set the oscillating torque to 0. |
| 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 | LDW will set the oscillating torque to 0. |
| 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 Keeping Assistance torque is zero |

## Refined System Architecture from Functional Safety Concept

**[Instructions: Provide the refined system architecture from the functional safety concept]**

### C:\Users\Hiep Truong\Downloads\refined-architecture-01.png

### Functional overview of architecture elements

**[Instructions: Provide a description for each functional safety element; what is each element's purpose in the lane assistance item? ]**

|  |  |
| --- | --- |
| **Element** | **Description** |
| Camera Sensor | Take images from the road |
| Camera Sensor ECU - Lane Sensing | Detecting lane lines and determining when the vehicle leaves the lane |
| Camera Sensor ECU - Torque request generator | request electronic power steering ECU to generate a demand torque, send appropriate messages to the car display ECU |
| Car Display | Display warning messages and system states |
| Car Display ECU - Lane Assistance On/Off Status | Display status of Lane Assistance System, it the system is switched on or off |
| Car Display ECU - Lane Assistant Active/Inactive | Display if the lane Assistance in active or idle mode |
| Car Display ECU - Lane Assistance malfunction warning | Display warnings |
| Driver Steering Torque Sensor | Measure steering torque on the steering wheel, produced by the driver |
| Electronic Power Steering (EPS) ECU - Driver Steering Torque | Monitoring steering torque applied by the driver |
| EPS ECU - Normal Lane Assistance Functionality | Realize normal functionalities of Lane Assistance Item, such as Lane Departure Warning and Land keeping assistance |
| EPS ECU - Lane Departure Warning Safety Functionality | Monitoring the oscillating torque amplitude and frequency |
| EPS ECU - Lane Keeping Assistant Safety Functionality | Monitoring the active duration of Lane Keeping Assistance |
| EPS ECU - Final Torque | Decide which torque will be applied to steering system. |
| Motor | Generate torque to the steering wheel |

# Technical Safety Concept

## Technical Safety Requirements

**[Instructions: Fill in the technical safety requirements for the lane departure warning first functional safety requirement. We have provided the associated functional safety requirement in the first table below. Hint: The technical safety requirements were discussed in the lesson videos. The architecture allocation column should contain element names such as LDW Safety block, Data Transmission Integrity Check, etc. Allocating the technical safety requirements to the "EPS ECU" does not provide enough detail for a technical safety concept.]**

**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 eclectronic power steering Torque’ component is below ‘Max\_Torque\_Ampliture’ | C | 50 ms | LDW Safety functionality | LDW will set the oscillating torque to 0. |
| Technical  Safety  Requirement  01-01-02 | The validity and integrity of the data transmission for ‘LDW\_Torque\_Request’ signal shall be ensured | C | 50 ms | Data Transmission integrity check | LDW will set the oscillating torque to 0. |
| Technical  Safety  Requirement  01-01-03 | As soon as 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 functionality | LDW will set the oscillating torque to 0. |
| Technical  Safety  Requirement  01-01-04 | 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 functioality | LDW will set the oscillating torque to 0. |
| 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 | B | Ignition cycle | Safety startup | LDW will set the oscillating torque to 0. |

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  01-02-01 | The LDW safety component shall ensure that the amplitude of the ‘LDW\_Torque\_Request’ sent to the ‘Final eclectronic power steering Torque’ component is below ‘Max\_Torque\_Frequency’ | C | 50 ms | LDW Safety functionality | LDW will set the oscillating torque to 0. |
| Technical  Safety  Requirement  01-02-02 | The validity and integrity of the data transmission for ‘LDW\_Torque\_Frequency’ signal shall be ensured | C | 50 ms | Data Transmission integrity check | LDW will set the oscillating torque to 0. |
| Technical  Safety  Requirement  01-02-03 | As soon as failure is detected by the LDW function, it shall deactivate the LDW feature and the ‘LDW\_Torque\_Frequency’ shall be set to zero | C | 50 ms | LDW Safety functionality | LDW will set the oscillating torque to 0. |
| 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 | C | 50 ms | LDW Safety functioality | LDW will set the oscillating torque to 0. |
| 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 | B | Ignition cycle | Safety startup | LDW will set the oscillating torque to 0. |

**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 high enough to warn the driver but not too high, so that the driver loses control | Verify that the the lane assistance output is set to zero with within the 50 ms fault tolerant time interval, when when the torque amplitude crosses the limit |
| Technical  Safety  Requirement  01-01-02 | N.A. | Verify that LDW will set the oscillating torque to 0 when an invalid LDW\_Torque\_Request is detected |
| Technical  Safety  Requirement  01-01-03 | N.A. | Verify that LDW\_Torque\_Request will be set to 0 when a failure is detected |
| Technical  Safety  Requirement  01-01-04 | N.A. | Verify that the car display ECU turns on a warning light when the LDW function is deactivated |
| Technical  Safety  Requirement  01-01-05 | N.A. | Verify that memory test is conducted and any memory faults will be detected |
| Technical  Safety  Requirement  01-02-01 | Validate the Max\_Torque\_Frequency is high enough to be detected by the driver but not too high, so that the driver loses control | Verify that the the lane assistance output is set to zero with within the 50 ms fault tolerant time interval, when when the torque frequency crosses the limit |
| Technical  Safety  Requirement  01-02-02 | LDW\_Torque\_Frequency | Verify that LDW will set the oscillating torque to 0 when an invalid LDW\_Torque\_Frequency is detected |
| Technical  Safety  Requirement  01-02-03 | N.A. | Verify that LDW\_Torque\_Frequency will be set to 0 when a failure is detected |
| Technical  Safety  Requirement  01-02-04 | N.A. | Verify that the car display ECU turns on a warning light when the LDW function is deactivated |
| Technical  Safety  Requirement  01-02-05 | N.A. | Verify that memory test is conducted and any memory faults will be detected |

**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 LKA 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 is  zero. |
| Technical  Safety  Requirement  02-01-02 | The validity and integrity of the  data transmission for  ‚LKA\_Torque\_Request’ signal  shall be ensured. | B | 500 ms | LKA Safety | Lane  Keeping  Assistance  torque is  zero. |
| 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. | B | 500 ms | LKA Safety | Lane  Keeping  Assistance  torque is  zero. |
| 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. | B | 500 ms | LKA Safety | Lane  Keeping  Assistance  torque is  zero. |
| 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. | A | Ignition cycle | Safety startup | Lane  Keeping  Assistance  torque is  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 chosen Max\_Duration not allow the driver to misuse the LKA as autonomous driving | Verify that the LKA will be deactivated if the active time exceeded Max\_Duration |
| Technical  Safety  Requirement  02-01-02 | N.A. | Verify that the LKA sets torque to 0 when errors are detected by Data Transmission Integrity Check |
| Technical  Safety  Requirement  02-01-03 | N.A. | Verify that LKA will be deactivated and LKA\_Torque\_request is 0 after a failure was detected |
| Technical  Safety  Requirement  02-01-04 | N.A | Verify if the car displays warning light when LKA function is deactivated. |
| Technical  Safety  Requirement  02-01-05 | N.A | Verify that memory test is conducted and any memory faults will be detected |

## 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 eclectronic power steering Torque’ component is below ‘Max\_Torque\_Ampliture’ | **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 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 | 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  01-01-05 | 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 amplitude of the ‘LDW\_Torque\_Request’ sent to the ‘Final eclectronic 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 ‘LDW\_Torque\_Frequency’ signal shall be ensured | **x** |  |  |
| Technical  Safety  Requirement  01-02-03 | As soon as failure is detected by the LDW function, it shall deactivate the LDW feature and the ‘LDW\_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 | Lane departure warning shall be turned off | Malfunction\_01  Malfunction\_02 | yes | Warning on car display |
| WDC-02 | Lane keeping assistance shall be turned off | Malfunction\_03 | yes | Warning on car display |