

Technical Safety Concept Lane Assistance

**Document Version: [1.1]**

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



# Document history

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Editor | Description |
| 20 June, 2018 | 1.0 | Akhil Suri | Initial Submission |
| 22 June, 2018 | 1.1 | Akhil Suri | Corrected typos |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# 

# 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 refine the functional safety requirements established in the functional safety concept into technical safety requirements. This is a crucial step before developing reliable hardware and software. As part of product development technical safety concept involves:

* Turning functional safety requirements into technical safety requirements
* Allocating technical safety requirements to the system architecture

As a subsequent step technical safety requirements will be considered within software and hardware implementation.

# 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 | To provide the images captured from camera to the camera Sensor ECU. |
| Camera Sensor ECU - Lane Sensing | Images will be analyzed and will calculate the car position and detect the lane lines. |
| Camera Sensor ECU - Torque request generator | Generating torque request to the Electronic Power Steering ECU. |
| Car Display | It will display warning to the driver. |
| Car Display ECU - Lane Assistance On/Off Status | Indicates if the Lane Assistance function is turned on. |
| Car Display ECU - Lane Assistant Active/Inactive | Indicates if the Lane Assistance function is active at that time. |
| Car Display ECU - Lane Assistance malfunction warning | Indicates if the Lane Assistance is having malfunction. |
| Driver Steering Torque Sensor | It will be measuring the steering torque which will be applied by the driver to the steering wheel. |
| Electronic Power Steering (EPS) ECU - Driver Steering Torque | Input from Driver Steering Torque is processed. |
| EPS ECU - Normal Lane Assistance Functionality | Request from the Camera Sensor ECU torque will be received by this module. |
| EPS ECU - Lane Departure Warning Safety Functionality | It will check if Lane Departure Warning function is having malfunction and will translate the request to final torque output. |
| EPS ECU - Lane Keeping Assistant Safety Functionality | It will check if Lane Keeping Assistant function is having malfunction and will translate the request to final torque output. |
| EPS ECU - Final Torque | Generates final torque from torque requests received from LDW and LKA safety. |
| Motor | The component is responsible for applying the work required to produce the torque required to execute actions delivered to the power steering ECU. |

# 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 | LDW Torque Amplitude to be set as 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 | LDW Torque Amplitude to be set as 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 Amplitude to be set as 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 | LDW Torque Amplitude to be set as 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 Amplitude to be set as zero |

**[Instructions: Fill in the technical safety requirements for the lane departure warning second functional safety requirement. We have provided the associated functional safety requirement in the table below. Hint:. Most of the technical safety requirements will be the same. At least one technical safety requirement will have to be slightly modified because we are talking about frequency instead of amplitude. These requirements were not given in the lessons]**

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 | LDW safety components should ensure that frequency of LDW\_Torque\_Request sent to the Final Power steering torque should be below Max\_Torque\_Frequency | C | 50 ms | LDW Safety | Lane Departure Warning Torque Request Frequency shall be set to zero. |
| Technical  Safety  Requirement  02 | Integrity and validity of the Max\_Torque\_Frequency should be ensured. | C | 50 ms | LDW Safety | Lane Departure Warning Torque Request Frequency shall be set to zero. |
| Technical  Safety  Requirement  03 | As soon as the LKA function deactivates the LKA feature, it should set the Max\_Torque\_Frequency to zero. | C | 50 ms | LDW Safety | Lane Departure Warning Torque Request Frequency shall be set to zero |
| Technical  Safety  Requirement  04 | When the LKA feature is deactivated by the LKA function, then the signal needs to be send to the display ECU for turning on the warning light. | C | 50 ms | LDW Safety | Lane Departure Warning Torque Request Frequency shall be set to zero |
| Technical  Safety  Requirement  05 | Memory test shall be conducted to check for any faults in the memory at start of the EPS ECU. | A | Ignition cycle | Data Transmission and Integrity Check | Lane Departure Warning Torque Request Frequency shall be set to zero |

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

**[OPTIONAL: For each technical safety requirement, identify both the verification and validation acceptance criteria. “Validation” asks whether or not you chose the appropriate parameters. “Verification” involves testing to make sure the vehicle behaves as expected when the parameter value is crossed. There is not necessarily one right answer. Look at your verification and validation acceptance criteria from the functional safety concept for inspiration.]**

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

**[Instructions: Fill in the technical safety requirements for the lane keeping assistance functional safety requirement 02-01. We have provided the associated functional safety requirement in the table below. Hint:. You can reuse the technical safety requirements from functional safety requirement 01-01. But you need to change the language because we are now looking at a different system. The ASIL and Fault Tolerant Time Interval are different as well.]**

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 or time taken by the lane keeping assistance LKA torque applied is less than Max\_Duration | B | 500 ms | LKA Safety | Set LKA torque to be zero |
| Technical  Safety  Requirement  02 | When the LKA feature is deactivated by the LKA function, then the signal needs to be send to the display ECU for turning on the warning light. | B | 500 ms | LKA Safety | Set LKA torque to be zero |
| Technical  Safety  Requirement  03 | As soon as the LKA function deactivates the LKA feature, it should set the LKA\_Torque\_Request to zero. | B | 500 ms | LKA Safety | Set LKA torque to be zero |
| Technical  Safety  Requirement  04 | Integrity and validity of the LKA\_Torque\_Request should be ensured. | B | 500 ms | LKA Safety | Set LKA torque to be zero |
| Technical  Safety  Requirement  05 | Memory test shall be conducted to check for any faults in the memory at start of the EPS ECU. | A | Ignition cycle | Data Transmission Integrity Check | Set LKA torque to be zero |

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

**[OPTIONAL: For each technical safety requirement, identify both the verification and validation acceptance criteria. “Validation” asks whether or not you chose the appropriate parameters. “Verification” involves testing to make sure the vehicle behaves as expected when the parameter value is crossed. There is not necessarily one right answer. Look at your verification and validation acceptance criteria from the functional safety concept for inspiration.]**

## Refinement of the System Architecture

**[Instructions: Include the refined system architecture. Hint: The refined system architecture should include the system architecture from the end of the technical safety lesson, including all of the ASIL labels.]**

****

## Allocation of Technical Safety Requirements to Architecture Elements

**[Instructions: We already included the allocation as part of the technical requirement tables. Here you can state that for this particular item, all technical safety requirements are allocated to the Electronic Power Steering ECU]**

The technical safety requirements will be allocated to different software elements such as the "LDW Safety Functionality" block, the "Data Transmission Integrity Check", or other relevant blocks inside the EPS ECU.

## Warning and Degradation Concept

**[Instructions: We've already identified that for any system malfunction, the lane assistance functions will be turned off and the driver will receive a warning light indication. The technical safety requirements have not changed how functionality will be degraded or what the warning will be.**

**So in this case, the warning and degradation concept is the same for the technical safety requirements as for the functional safety requirements. You can copy the functional safety warning and degradation concept here.**

**Oftentimes, a technical safety analysis will lead to a more detailed warning and degradation concept. ]**

WDC-01 is for Lane Departure Warning function

WDC-02 is for Lane Keeping assistance function

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Degradation Mode** | **Trigger for Degradation Mode** | **Safe State invoked?** | **Driver Warning** |
| WDC-01 | Turn off the functionality | Malfunction\_01  Malfunction\_02 | Yes | a warning light on the dashboard |
| WDC-02 | Turn off the functionality | Malfunction\_03 | Yes | a warning light on the dashboard |