

Technical Safety Concept Lane Assistance

**Document Version: [Version]**

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



# Document history

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Editor | Description |
| August 29, 2017 | 1.0 | Microsoft Word | Initial Version |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# 

# 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

A technical safety concept is similar to a functional safety concept in the sense that it defines requirements and allocates them to subsystems. While a functional safety concept provides a bird’s eye view of the system, a technical safety concept goes deeper into the technical details of the system. Technical safety requirements are derived from functional safety requirements.

# 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 warning oscillating torque amplitude is below Max\_Torque\_Amplitude | C | 50ms | Lane Departure warning function is not activated |
| Functional  Safety  Requirement  01-02 | The electronic power steering ECU shall ensure that the lane departure warning oscillating torque frequency is below Max\_Torque\_Frequency | C | 50ms | Lane Departure warning function is not activated |
| 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 system is not activated |

## Refined System Architecture from Functional Safety Concept



### 

### Functional overview of architecture elements

|  |  |
| --- | --- |
| **Element** | **Description** |
| Camera Sensor | Perceives the environment through images which are passed to the camera sensor ECU for processing |
| Camera Sensor ECU - Lane Sensing | Determines if the car is leaving the lane and if so, determines the torque to be sent to the torque request generator |
| Camera Sensor ECU - Torque request generator | Sends a vibrational torque request to the power steering ECU |
| Car Display | Displays a number of visual cues that help the driver understand what the car is doing |
| Car Display ECU - Lane Assistance On/Off Status | Receives a signal from the power steering ECU about the status of the lane departure warning function and conveys the same to the display |
| Car Display ECU - Lane Assistant Active/Inactive | Receives a signal from the power steering ECU about the status of the lane assistance function and conveys the same to the display |
| Car Display ECU - Lane Assistance malfunction warning | Receives a signal from the power steering ECU if there is a malfunction with the lane assistance system and conveys the same to the display |
| Driver Steering Torque Sensor | Senses how much torque is already being applied by the driver |
| Electronic Power Steering (EPS) ECU - Driver Steering Torque | Determines how much torque is already being applied by the driver |
| EPS ECU - Normal Lane Assistance Functionality | Receives the vibrational torque request from the camera ECU |
| EPS ECU - Lane Departure Warning Safety Functionality | Receives the request from the camera subsystem to activate/deactivate the lane departure warning system(i.e. to cause vibrations of the steering wheel) and conveys this request to the steering wheel through the motor |
| EPS ECU - Lane Keeping Assistant Safety Functionality | Receives the request from the camera subsystem to activate/deactivate the lane assistance system(i.e. to apply additional torque to the steering wheel) and conveys this request to the steering wheel through the motor |
| EPS ECU - Final Torque | Computes the final torque needed to be applied to the steering wheel after taking into consideration the torque already being applied by the driver and the torque requested by the camera subsystem and conveys the same to the motor |
| Motor | Applies the final 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 | 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 | 50ms |  | The lane departure warning torque request amplitude shall be set to zero |
| Technical  Safety  Requirement  02 | Validity and Integrity of the data transmission for the *LDW\_Torque\_Request* signal shall be ensured | C | 50ms |  |
| 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 | 50ms |  |
| 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 | 50ms |  |
| Technical  Safety  Requirement  05 | Memory test shall be conducted at the startup of EPS ECU to check for any faults in memory. | A | Ignition cycle |  |

**[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 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 | 50ms |  | The lane departure warning torque request amplitude shall be set to zero |
| Technical  Safety  Requirement  02 | Validity and Integrity of the data transmission for the *LDW\_Torque\_Request* signal shall be ensured | C | 50ms |  |
| 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 | 50ms |  |
| 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 | 50ms |  |
| Technical  Safety  Requirement  05 | Memory test shall be conducted at the startup of EPS ECU to check for any faults in memory. | A | Iginition Cycle |  |

**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 | 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\_torque\_duration | B | 500ms |  | The lane departure warning torque request amplitude shall be set to zero |
| Technical  Safety  Requirement  02 | Validity and Integrity of the data transmission for the *LKA\_Torque\_Request* signal shall be ensured | B | 500ms |  |
| 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 | 500ms |  |
| Technical  Safety  Requirement  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 | 500ms |  |
| Technical  Safety  Requirement  05 | Memory test shall be conducted at the startup of EPS ECU to check for any faults in memory. | A | Ignition Cycle |  |

**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]**

## 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. ]**