

Technical Safety Concept Lane Assistance

**Document Version: [Version]**

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



# Document history

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Editor | Description |
| 3/2/18 | 1.0 | Ken Overholt | Initial draft |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# 

# Table of Contents

Table of Contents

[Document history 2](#_Toc508233109)

[Table of Contents 2](#_Toc508233110)

[Purpose of the Technical Safety Concept 2](#_Toc508233111)

[Inputs to the Technical Safety Concept 3](#_Toc508233112)

[Functional Safety Requirements 3](#_Toc508233113)

[Refined System Architecture from Functional Safety Concept 4](#_Toc508233114)

[Functional overview of architecture elements 4](#_Toc508233115)

[Technical Safety Concept 5](#_Toc508233116)

[Technical Safety Requirements 5](#_Toc508233117)

[Refinement of the System Architecture 10](#_Toc508233118)

[Allocation of Technical Safety Requirements to Architecture Elements 10](#_Toc508233119)

[Warning and Degradation Concept 11](#_Toc508233120)

# Purpose of the Technical Safety Concept

The technical Safety Concept defines how the subsystems interact at the message level and describes how the ECUs communicate with each other. It turns functional safety requirements into technical safety requirements and allocates technical safety requirements to the system architecture.

# 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 | 50 ms | No torque is being applied |
| 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 | 50 ms | No torque is being applied |
| 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 | No torque is being applied |

## Refined System Architecture from Functional Safety Concept



### 

### Functional overview of architecture elements

|  |  |
| --- | --- |
| **Element** | **Description** |
| Camera Sensor | The Camera Sensor reads in images from the road. |
| Camera Sensor ECU - Lane Sensing | The Camera Sensor ECU identifies when the vehicle has accidentally departed its lane and sends the appropriate torque request to the Electronic Power Steering ECU as well as sending a message to the Car Display ECU. |
| Camera Sensor ECU - Torque request generator |  |
| Car Display | The Car Display shows a sign in indicating the car has veered from its lane. |
| Car Display ECU - Lane Assistance On/Off Status | The Car Display ECU controls a light that tells the driver if the Lane Keeping system is on or off. It also controls a light that tells the driver that the Lane Departure Warning is activated. |
| Car Display ECU - Lane Assistant Active/Inactive |  |
| Car Display ECU - Lane Assistance malfunction warning |  |
| Driver Steering Torque Sensor |  |
| Electronic Power Steering (EPS) ECU - Driver Steering Torque |  |
| EPS ECU - Normal Lane Assistance Functionality |  |
| EPS ECU - Lane Departure Warning Safety Functionality |  |
| EPS ECU - Lane Keeping Assistant Safety Functionality |  |
| EPS ECU - Final Torque |  |
| Motor | The motor receives the torque request from the Driver Steering Torque Sensor and moves 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 | 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 | Lane Departure Warning Torque Request Amplitude shall be set to zero |
| Technical  Safety  Requirement  02 | 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 | Lane Departure Warning Torque Request Amplitude shall be set to zero |
| Technical  Safety  Requirement  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. | C | 50 ms | LDW Safety | Lane Departure Warning Torque Request Amplitude shall be 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 |  | Lane Departure Warning Torque Request Amplitude shall be set to zero |
| Technical  Safety  Requirement  05 | Memory test shall be conducted at startup of the EPS ECU to check for any faults in memory. | A | Ignition cycle |  | Lane Departure Warning 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 amplitude of the 'LDW\_Torque\_Request' sent to the 'Final electronic power steering Torque' component is below ' Max\_Torque\_Frequency. | B | 500 ms | LDW Safety | Lane Departure Warning Torque Request Amplitude shall be set to zero |
| Technical  Safety  Requirement  02 | 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. | B | 500 ms | LDW Safety | Lane Departure Warning Torque Request Amplitude shall be set to zero |
| Technical  Safety  Requirement  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. | B | 500 ms | LDW Safety | Lane Departure Warning Torque Request Amplitude shall be set to zero |
| Technical  Safety  Requirement  04 | The validity and integrity of the data transmission for Max\_Torque\_Frequency signal shall be ensured. | B | 500 ms |  | Lane Departure Warning Torque Request Amplitude shall be set to zero |
| Technical  Safety  Requirement  05 | Memory test shall be conducted at startup of the EPS ECU to check for any faults in memory. | A | Ignition cycle |  | Lane Departure Warning Torque Request Amplitude shall be set to zero |

**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 |  |  |  |  |  |
| Technical  Safety  Requirement  02 |  |  |  |  |  |
| Technical  Safety  Requirement  03 |  |  |  |  |  |
| Technical  Safety  Requirement  04 |  |  |  |  |  |
| Technical  Safety  Requirement  05 |  |  |  |  |  |

## Refinement of the System Architecture

**A screenshot of a video game

Description generated with high confidence**

## Allocation of Technical Safety Requirements to Architecture Elements

For this particular item, all technical safety requirements are allocated to the Electronic Power Steering ECU

## Warning and Degradation Concept

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Degradation Mode** | **Trigger for Degradation Mode** | **Safe State invoked?** | **Driver Warning** |
| WDC-01 | Turn off the functionality | lane departure warning function applies an oscillating torque with very high torque frequency and amplitude | Yes | The owner’s manual will state that the feature will be turned off if it becomes too forceful. The driver will see a warning light on the dashboard when the system malfunctions. |
| WDC-02 | Turn off the functionality | Oscillating torque has reached the max\_duration value | Yes | The owner’s manual will state that the vehicle is not to be used for autonomous driving and that this feature will only be active for a short period before turning off. The driver will see a warning light on the dashboard when the lane keeping assistance is activated and it will disappear when not activated. |