

Technical Safety Concept Lane Assistance

**Document Version: 1.0**

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



# Document history

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Editor | Description |
| 1/2/2018 | 1.0 | Joshua Schoenfield | First submission |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# 

# 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 technical safety concept defines how the subsystems interact at the message level and describes how the ECUs communicate with each other. It will be defining new specific technical safety requirements, based on the functional safety requirements outlined in the functional safety concept, and allocating these requirements to parts of 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 oscillating torque amplitude is below Max\_Torque\_Amplitude | C | 50 ms | Lane assistance output is set to zero, and the driver is able to steer. |
| Functional  Safety  Requirement  01-02 | The electronic power steering ECU **shall** ensure that the lane departure oscillating torque frequency is below Max\_Torque\_Frequency | C | 50 ms | Lane assistance output is set to zero, and the driver is able to steer. |
| 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 assistance output is set to zero, and the driver is able to steer. |

## Refined System Architecture from Functional Safety Concept

A diagram of the refined system architecture from the functional safety concept can be found in the following image:



### 

### Functional overview of architecture elements

|  |  |
| --- | --- |
| **Element** | **Description** |
| Camera Sensor | The camera sensor reads in images from the road and reports these images to the Camera Sensor ECU |
| Camera Sensor ECU - Lane Sensing | The camera sensor ECU – Lane Sensing module identifies when the vehicle’s position within its lane and sends that information to the Torque request generator. |
| Camera Sensor ECU - Torque request generator | The Camera Sensor ECU – Torque request generator element takes the information about the car’s position within its lane and generates the appropriate torque to request from the Electronic Steering ECU |
| Car Display | Displays information about the status of the Lane Assistance System to the driver |
| Car Display ECU - Lane Assistance On/Off Status | Summarizes the on/off status of the Lane Assistance Item, in preparation for display to the driver by the Car Display Element |
| Car Display ECU - Lane Assistant Active/Inactive | Summarizes the active/inactive status of the Lane Assistance Item, in preparation for display to the driver by the Car Display Element |
| Car Display ECU - Lane Assistance malfunction warning | Generates a warning for display to the Driver on the Car Display in the event of a detected malfunction with the Lane Assistance item |
| Driver Steering Torque Sensor | Senses the torque provided to the steering wheel by the driver and provides that information to the Electronic Power Steering ECU – Driver Steering Torque module |
| Electronic Power Steering (EPS) ECU - Driver Steering Torque | Processes the messages from the Driver Steering Torque Sensor for use by the EPS ECU Final Torque Element |
| EPS ECU - Normal Lane Assistance Functionality | Processes the messages from the Driver Steering Torque Sensor for use by the Camera ECU Torque Request Generator Element. Sends the normal lane assistance functionality for processing by the Lane Assistance Functional Safety Element |
| EPS ECU - Lane Departure Warning Safety Functionality | Implements the safety goals associated with the Lane Departure Warning, by modulating the final torque requested and by sending status messages to the Car Display ECU |
| EPS ECU - Lane Keeping Assistant Safety Functionality | Implements the safety goals associated with the Lane Keeping Assistant, by modulating the final torque requested and by sending status messages to the Car Display ECU |
| EPS ECU - Final Torque | Calculates the total torque required to be provided by the Motor, taking into account the safe values provided by the LA Safety Functionality elements and the torque already being provided by the driver. |
| Motor | Receives the final torque value from the EPS ECU and applies it to the steering wheel. |

# 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  01-01 | 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 Block | Lane assistance output is set to zero |
| Technical  Safety  Requirement  01-02 | 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 Block | Lane assistance output is set to zero |
| Technical  Safety  Requirement  01-03 | 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 Block | Lane assistance output is set to zero |
| Technical  Safety  Requirement  01-04 | The validity and integrity of the data transmission for 'LDW\_Torque\_Request' signal shall be ensured. | C | 50 ms | Data Transmission Integrity Check | Lane assistance output is set to zero |
| Technical  Safety  Requirement  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: Memory Test Block | Lane assistance output is 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  02-01 | The 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 | 50 ms | LDW Safety Block | Lane assistance output is set to zero |
| Technical  Safety  Requirement  02-02 | 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 Block | Lane assistance output is set to zero |
| Technical  Safety  Requirement  02-03 | 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 Block | Lane assistance output is set to zero |
| Technical  Safety  Requirement  02-04 | The validity and integrity of the data transmission for 'LDW\_Torque\_Request' signal shall be ensured. | C | 50 ms | Data Transmission Integrity Check | Lane assistance output is set to zero |
| Technical  Safety  Requirement  02-05 | Memory test shall be conducted at start up of the EPS ECU to check for any faults in memory. | A | Ignition cycle | Safety Startup: Memory Test Block | Lane assistance output is 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:**

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  03-01 | The LKA safety component shall ensure that the total continuous duration over which the 'LKA\_Torque\_Request' sent to the 'Final electronic power steering Torque' is non zero is shorter than 'Max\_Duration. | B | 500 ms | LKA Safety Block | Lane assistance output is set to zero |
| Technical  Safety  Requirement  03-02 | 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 Block | Lane assistance output is set to zero |
| Technical  Safety  Requirement  03-03 | 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 Block | Lane assistance output is set to zero |
| Technical  Safety  Requirement  03-04 | The validity and integrity of the data transmission for 'LKA\_Torque\_Request' signal shall be ensured. | B | 500 ms | Data Transmission Integrity Check | Lane assistance output is set to zero |
| Technical  Safety  Requirement  03-05 | Memory test shall be conducted at start up of the EPS ECU to check for any faults in memory. | A | Ignition cycle | Safety Startup: Memory Test Block | Lane assistance output is set to 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

The Refined System architecture, including all the relevant components ASIL labels can be found in the following figure:

****

## Allocation of Technical Safety Requirements to Architecture Elements

For this item, all technical safety requirements are allocated to the Electronic Power Steering ECU. Details of the allocation can be found in the technical requirement tables.

## Warning and Degradation Concept

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Degradation Mode** | **Trigger for Degradation Mode** | **Safe State invoked?** | **Driver Warning** |
| WDC-01 | LDW System Turns Off | Malfunction\_01 or Malfunction\_02 | Yes | Lane Assistance Malfunction Warning Appears on Car Display |
| WDC-02 | LKA System Turns Off | Malfunction\_03 | Yes | Lane Assistance Malfunction Warning Appears on Car Display |