

Technical Safety Concept Lane Assistance

**Document Version: 1.0**

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



# Document history

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Editor | Description |
| 11/10/2017 | 1.0 | Ibis Prevedello | First draft |

# Table of Contents

[Document history 2](#_Toc495608673)

[Table of Contents 3](#_Toc495608674)

[Purpose of the Technical Safety Concept 4](#_Toc495608675)

[Inputs to the Technical Safety Concept 5](#_Toc495608676)

[Functional Safety Requirements 5](#_Toc495608677)

[Refined System Architecture from Functional Safety Concept 5](#_Toc495608678)

[Functional overview of architecture elements 6](#_Toc495608679)

[Technical Safety Concept 8](#_Toc495608680)

[Technical Safety Requirements 8](#_Toc495608681)

[Refinement of the System Architecture 12](#_Toc495608682)

[Allocation of Technical Safety Requirements to Architecture Elements 13](#_Toc495608683)

[Warning and Degradation Concept 13](#_Toc495608684)

# Purpose of the Technical Safety Concept

The purpose of the functional safety concept is to avoid accidents by reducing risks to acceptable levels.

# 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 | LDW is turned off with a lighted icon on the car display and/or sound warning to the driver. |
| Functional  Safety  Requirement  01-02 | The Electronic Power Steering ECU shall ensure that the lane departure oscillating torque frequency is below Max\_Torque\_Amplitude. | C | 50 ms | LDW is turned off with a lighted icon on the car display and/or sound warning to the driver. |
| Functional  Safety  Requirement  02-01 | The Electronic Power Steering ECU shall ensure that the lane assistance torque is applied for a maximum of Max\_Duration. | B | 50 ms | LKA is turned off with a lighted icon on the car display and/or sound warning to the driver. |

## Refined System Architecture from Functional Safety Concept

*Figure 2* presents a refined system architecture including all the ASIL labels of each subsystem of the systems used.



Figure - Refined System Architecture

### 

### Functional overview of architecture elements

|  |  |
| --- | --- |
| **Element** | **Description** |
| Camera Sensor | A sensor positioned in the front of the car which will capture images and sends to the Camera Sensor ECU. |
| Camera Sensor ECU - Lane Sensing | The Camera Sensor ECU receives the images from the Camera Sensor, process it to determine Lane Sensing and outputs information for the Car Display ECU. |
| Camera Sensor ECU - Torque request generator | The Camera Sensor ECU receives the images from the Camera Sensor, process it to determine the torque necessary to steer the vehicle and send it to the Electronic Power Steering. |
| Car Display | Display that takes data from the Car Display ECU and shows to the driver in form of lighted icons and audio warnings. |
| Car Display ECU - Lane Assistance On/Off Status | This function determines if Lane Assistance is On/Off, it illuminates if function is activated. For this function the driver has autonomy to switch it on or off. |
| Car Display ECU - Lane Assistant Active/Inactive | This function determines if Lane Assistance is Active/Inactive, it illuminates if function is activated; if it is inactive, the driver cannot turn it on. |
| Car Display ECU - Lane Assistance malfunction warning | If any problem happen, a malfunction warning will be presented for the driver, it illuminates if warning is presented. |
| Driver Steering Torque Sensor | Sensor that measures the steering torque that the driver is applying on the steering wheel. |
| Electronic Power Steering (EPS) ECU - Driver Steering Torque | EPS ECU takes an input from the Driver Steering Torque Sensor and process the data. |
| EPS ECU - Normal Lane Assistance Functionality | EPS ECU sends the output to the Motor. It also limits to the torque do not exceed Max\_torque. |
| EPS ECU - Lane Departure Warning Safety Functionality | EPS ECU assures that the amplitude and frequency are below Max\_Torque\_Frequency and Max\_torque\_Amplitude and sends the output to the Motor. |
| EPS ECU - Lane Keeping Assistant Safety Functionality | EPS ECU assures that the duration of the applied torque is below Max\_Duration. |
| EPS ECU - Final Torque | After all the safety requirements satisfied, the final torque will be calculated and send to the Motor. |
| Motor | Receives the command from the Electronic Power Steering ECU and converts to torque on 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 | 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 | Electronic Power Steering ECU  (Includes the LDW safety block) | LDW is turned off with a lighted icon on the car display and/or sound warning to the driver. |
| 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 | Data Transmission Integrity Test  (Includes the LDW safety block) | LDW is turned off with a lighted icon on the car display and/or sound warning to the driver. |
| 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 | Electronic Power Steering ECU  (Includes the LDW safety block) | LDW is turned off with a lighted icon on the car display and/or sound warning to the driver. |
| Technical  Safety  Requirement  04 | The validity and integrity of the data transmission for ‘LDW\_Torque\_Request’ signal shall be ensured. | C | 50 ms | Electronic Power Steering ECU  (Includes the LDW safety block) | LDW is turned off with a lighted icon on the car display and/or sound warning to the driver. |
| 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 | Separate External Block of Memory  (Includes the LDW safety block) | LDW is turned off with a lighted icon on the car display and/or sound warning to the driver. |

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 frequency of the ‘LDW\_Torque\_Request’ sent to the ‘Final electronic power steering Torque’ component is below ‘Max\_Torque\_Frequency. | C | 50 ms | Electronic Power Steering ECU  (Includes the LDW safety block) | LDW is turned off with a lighted icon on the car display and/or sound warning to the driver. |
| 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 | Data Transmission Integrity Test  (Includes the LDW safety block) | LDW is turned off with a lighted icon on the car display and/or sound warning to the driver. |
| 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 | Electronic Power Steering ECU  (Includes the LDW safety block) | LDW is turned off with a lighted icon on the car display and/or sound warning to the driver. |
| Technical  Safety  Requirement  04 | The validity and integrity of the data transmission for ‘LDW\_Torque\_Request’ signal shall be ensured. | C | 50 ms | Electronic Power Steering ECU  (Includes the LDW safety block) | LDW is turned off with a lighted icon on the car display and/or sound warning to the driver. |
| 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 | Separate External Block of Memory  (Includes the LDW safety block) | LDW is turned off with a lighted icon on the car display and/or sound warning to the driver. |

**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  01 | The LKA safety component shall ensure that the lane assistance torque is applied for only Max\_Duration. | C | 500 ms | Electronic Power Steering ECU  (Includes the LKA safety block) | LKA is turned off with a lighted icon on the car display and/or sound warning to the driver. |
| Technical  Safety  Requirement  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. | C | 500 ms | Data Transmission Integrity Test  (Includes the LKA safety block) | LKA is turned off with a lighted icon on the car display and/or sound warning to the driver. |
| Technical  Safety  Requirement  03 | As soon as a failure is detected by the LKA function, it shall deactivate the LDW feature and the ‘LKA \_Torque\_Request’ shall be set to zero. | C | 500 ms | Electronic Power Steering ECU  (Includes the LKA safety block) | LKA is turned off with a lighted icon on the car display and/or sound warning to the driver. |
| Technical  Safety  Requirement  04 | The validity and integrity of the data transmission for ‘LKA \_Torque\_Request’ signal shall be ensured. | C | 500 ms | Electronic Power Steering ECU  (Includes the LKA safety block) | LKA is turned off with a lighted icon on the car display and/or sound warning to the driver. |
| 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 | Separate External Block of Memory  (Includes the LKA safety block) | LKA is turned off with a lighted icon on the car display and/or sound warning to the driver. |

## Refinement of the System Architecture

Figure 2 shows the system architecture after the safety technical requirements are applied.



Figure - Lane Assistance Architecture

## Allocation of Technical Safety Requirements to Architecture Elements

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 | LDW is turned off with a lighted icon on the car display and/or sound warning to the driver. | LDW torque exceeds Max\_Torque\_Amplitude or Max\_Torque\_Frequency | YES | Lighted icon on the car display and/or sound warning to the driver. |
| WDC-02 | LKA is turned off with a lighted icon on the car display and/or sound warning to the driver. | LKA torque is applied for a time longer than Max\_Duration | YES | Lighted icon on the car display and/or sound warning to the driver. |