

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](#_Toc495526504)

[Table of Contents 3](#_Toc495526505)

[Purpose of the Technical Safety Concept 4](#_Toc495526506)

[Inputs to the Technical Safety Concept 5](#_Toc495526507)

[Functional Safety Requirements 5](#_Toc495526508)

[Refined System Architecture from Functional Safety Concept 5](#_Toc495526509)

[Functional overview of architecture elements 5](#_Toc495526510)

[Technical Safety Concept 7](#_Toc495526511)

[Technical Safety Requirements 7](#_Toc495526512)

[Refinement of the System Architecture 11](#_Toc495526513)

[Allocation of Technical Safety Requirements to Architecture Elements 11](#_Toc495526514)

[Warning and Degradation Concept 11](#_Toc495526515)

# 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 | 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 | 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 | LDW is turned off with a lighted icon on the car display and/or sound warning to the driver. |
| Technical  Safety  Requirement  04 | As soon as the LDW function deactivates de 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 | Electronic Power Steering ECU | 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 start up of the EPS ECU to check for any faults in memory. | A | 50 ms | Ignition Cycle | LDW torque output is set to 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 |  |  |  |  |  |
| Technical  Safety  Requirement  02 |  |  |  |  |  |
| Technical  Safety  Requirement  03 |  |  |  |  |  |
| Technical  Safety  Requirement  04 |  |  |  |  |  |
| Technical  Safety  Requirement  05 |  |  |  |  |  |

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

**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. ]**