

Functional 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](#_Toc495524351)

[Table of Contents 3](#_Toc495524352)

[Purpose of the Functional Safety Concept 4](#_Toc495524353)

[Inputs to the Functional Safety Concept 5](#_Toc495524354)

[Safety goals from the Hazard Analysis and Risk Assessment 5](#_Toc495524355)

[Preliminary Architecture 5](#_Toc495524356)

[Description of architecture elements 6](#_Toc495524357)

[Functional Safety Concept 7](#_Toc495524358)

[Functional Safety Analysis 7](#_Toc495524359)

[Functional Safety Requirements 7](#_Toc495524360)

[Refinement of the System Architecture 9](#_Toc495524361)

[Allocation of Functional Safety Requirements to Architecture Elements 9](#_Toc495524362)

[Warning and Degradation Concept 10](#_Toc495524363)

# Purpose of the Functional Safety Concept

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

# Inputs to the Functional Safety Concept

## Safety goals from the Hazard Analysis and Risk Assessment

|  |  |
| --- | --- |
| **ID** | **Safety Goal** |
| Safety\_Goal\_01 | Oscillating steering torque should be limited for the Lane Departure Warning. |
| Safety\_Goal\_02 | Steering torque should be time limited for the Lane Keep Assistance. |
| Safety\_Goal\_03 | Steering torque should be disabled when the vehicle is driving backwards. |

## Preliminary Architecture

*Figure 1* shows an overall Lane Assistance System Architecture, presenting how the systems are connected between them and the Steering Wheel.



Figure - Lane Assistance System Architecture

### Description of architecture elements

|  |  |
| --- | --- |
| **Element** | **Description** |
| Camera Sensor | A sensor positioned in the front of the car which will capture images and send to the system. |
| Camera Sensor ECU | The Electronic Central Unit responsible to process the image from the Camera Sensor and convert this image into useful data for the other systems. |
| 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 | Electronic Central Unit that collects data from other systems and decide which kind of signal the Car Display needs to show. |
| Driver Steering Torque Sensor | Sensor that measures the steering torque that the driver is applying on the steering wheel. |
| Electronic Power Steering ECU | Electronic Central Unit that process the data collected by the Driver Steering Torque Sensor. |
| Motor | Receives the command from the Electronic Power Steering ECU and converts to torque on the steering wheel. |

# Functional Safety Concept

The functional safety concept consists of:

* Functional safety analysis
* Functional safety requirements
* Functional safety architecture
* Warning and degradation concept

## Functional Safety Analysis

|  |  |  |  |
| --- | --- | --- | --- |
| **Malfunction ID** | **Main Function of the Item Related to Safety Goal Violations** | **Guidewords (NO, WRONG, EARLY, LATE, MORE, LESS)** | **Resulting Malfunction** |
| Malfunction\_01 | Lane Departure Warning (LDW) function shall apply an oscillating steering torque to provide the driver a haptic feedback | MORE | The lane keeping item shall ensure that the lane departure oscillating torque amplitude is below Max\_Torque\_Amplitude |
| Malfunction\_02 | Lane Departure Warning (LDW) function shall apply an oscillating steering torque to provide the driver a haptic feedback | MORE | The lane keeping item shall ensure that the lane departure oscillating torque frequency is below Max\_Torque\_Frequency |
| Malfunction\_03 | Lane Keeping Assistance (LKA) function shall apply the steering torque when active in order to stay in ego lane | NO | The lane keeping item shall ensure that the lane keeping assistance torque is applied for only Max\_Duration |

## Functional Safety Requirements

Lane Departure Warning (LDW) 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. |

Lane Departure Warning (LDW) Verification and Validation Acceptance Criteria:

|  |  |  |
| --- | --- | --- |
| **ID** | **Validation Acceptance**  **Criteria and Method** | **Verification Acceptance**  **Criteria and Method** |
| Functional  Safety  Requirement  01-01 | Test the LDW with torque amplitude above Max\_Torque\_Amplitude and assure that the LDW function is turned off and indicated by a lighted icon and/or sound to the driver. | Verify the LDW function with values less than Max\_Torque\_Amplitude.  Verify the LDW function turn off and the driver is alerted by a lighted icon and/or sound. |
| Functional  Safety  Requirement  01-02 | Test the LDW with torque amplitude above Max\_Torque\_Frequency and assure that the LDW function is turned off and indicated by a lighted icon and/or sound to the driver. | Verify the LDW function with values less than Max\_Torque\_Frequency.  Verify the LDW function turn off and the driver is alerted by a lighted icon and/or sound. |

Lane Keeping Assistance (LKA) Requirements:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Functional Safety Requirement** | **ASIL** | **Fault Tolerant Time Interval** | **Safe State** |
| 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. |

Lane Keeping Assistance (LKA) Verification and Validation Acceptance Criteria:

|  |  |  |
| --- | --- | --- |
| **ID** | **Validation Acceptance**  **Criteria and Method** | **Verification Acceptance**  **Criteria and Method** |
| Functional  Safety  Requirement  02-01 | Test the LKA for a time above Max\_Duration and assure that the LKA function is turned off and indicated by a lighted icon and/or sound to the driver. | Verify the LKA function with duration less than Max\_Duration.  Verify the LKA function turn off and the driver is alerted by a lighted icon and/or sound. |

## Refinement of the System Architecture

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

****

Figure - Refined System Architecture

## Allocation of Functional Safety Requirements to Architecture Elements

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Functional Safety Requirement** | **Electronic Power Steering ECU** | **Camera ECU** | **Car Display ECU** |
| Functional  Safety  Requirement  01-01 | The Electronic Power Steering ECU shall ensure that the lane departure oscillating torque amplitude is below Max\_Torque\_Amplitude. | **X** |  |  |
| Functional  Safety  Requirement  01-02 | The Electronic Power Steering ECU shall ensure that the lane departure oscillating torque frequency is below Max\_Torque\_Amplitude. | **X** |  |  |
| 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. | **X** |  |  |

## 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. |