

Functional Safety Concept Lane Assistance

**Document Version: [Version]**

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



# Document history

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Editor | Description |
| 12-02-2018 | 1.0 | Fuqiang Huang | First Attempt for Submission |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# Table of Contents

Table of Contents

[Document history 2](#_Toc531854400)

[Table of Contents 3](#_Toc531854401)

[Purpose of the Functional Safety Concept 4](#_Toc531854402)

[Inputs to the Functional Safety Concept 5](#_Toc531854403)

[Safety goals from the Hazard Analysis and Risk Assessment 5](#_Toc531854404)

[Preliminary Architecture 5](#_Toc531854405)

[Description of architecture elements 6](#_Toc531854406)

[Functional Safety Concept 7](#_Toc531854407)

[Functional Safety Analysis 7](#_Toc531854408)

[Functional Safety Requirements 8](#_Toc531854409)

[Refinement of the System Architecture 10](#_Toc531854410)

[Allocation of Functional Safety Requirements to Architecture Elements 11](#_Toc531854411)

[Warning and Degradation Concept 11](#_Toc531854412)

# Purpose of the Functional Safety Concept

The functional safety concept is composed of the following information:

* Refine the safety goals in what are called functional safety requirements defining the vehicle’s functions.
* Allocate these safety requirements to the relevant parts of the system diagram. This could involve expanding the system architecture with new element blocks.
* Refine the system architecture to handle the new requirements with a few more attributes, including the ASIL level, the fault tolerant time interval and the safe state.
* Discuss validation and verification, which is how to prove that the system actually meets the requirements.

The functional safety concept is looking at the item from a high level and does not go into technical details. The functional safety concept looks at the general functionality of the item; the technical safety concept looks at the technical implementation of the item. In practice, developing these two documents is an iterative process where new functional requirements could lead to new technical requirements which could lead back to new functional requirements.

# Inputs to the Functional Safety Concept

## Safety goals from the Hazard Analysis and Risk Assessment

|  |  |
| --- | --- |
| **ID** | **Safety Goal** |
| Safety\_Goal\_01 | The oscillating steering torque from the lane departure warning function shall be limited. |
| Safety\_Goal\_02 | The LKA function shall be time limited and the additional steering torque shall end after a given time interval so that the driver cannot misuse the system for autonomous driving. |
| Safety\_Goal\_03 | The LDW function shall be disabled in low visibility environment. |
| Safety\_Goal\_04 | The LDW function shall be deactivated automatically and promptly when the drive applies the brake. |

## Preliminary Architecture



### Description of architecture elements

|  |  |
| --- | --- |
| **Element** | **Description** |
| Camera Sensor | Captures road and vehicle images for the Camera Sensor ECU. |
| Camera Sensor ECU | Detects lane departures based on images captured, sends a signal to the electronic power steering system asking to turn and vibrate the steering wheel, and requests a warning light in the car display dashboard. |
| Car Display | Provides a warning light in the car display dashboard to let the driver know whether the lane assistance system is active, and provides a button on the dashboard so that the driver can turn off the system completely if in need. |
| Car Display ECU | Gets the request signal from the Camera Sensor ECU to control the warning light, and receives the on/off signal from the Car Display to ask for activating/deactivating the assistance system. |
| Driver Steering Torque Sensor | Detects how much the driver is already turning the steering wheel. |
| Electronic Power Steering ECU | Receives the request from Camera Sensor ECU and then sends a control signal to Motor to vibrate the steering wheel to give a warning to the driver, and calculates extra steering torque needed to help the driver move back towards the center of the lane. |
| Motor | Vibrates the steering wheel to give a warning to the driver based on the information from Electronic Power Steering ECU, and applies the extra torque to the steering wheel to draw the vehicle back to the center of the lane. |

# 

# 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 departure warning function applies an oscillating torque with very high torque amplitude (above limit). |
| Malfunction\_02 | Lane Departure Warning (LDW) function shall apply an oscillating steering torque to provide the driver a haptic feedback | MORE | The lane departure warning function applies an oscillating torque with very high torque frequency (above limit) |
| 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 assistance function is not limited in time duration which leads to misuse as an autonomous driving function |

## 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 lane keeping item shall ensure that the lane departure oscillating torque amplitude is below Max\_Torque\_Amplitude. | C | 50 ms | The system shall be switched off. |
| Functional  Safety  Requirement  01-02 | The lane keeping item shall ensure that the lane departure oscillating torque frequency is below Max\_Torque\_Frequency. | C | 50 ms | The system shall be switched off. |

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 and validate that the Max\_Torque\_Amplitude chosen is appropriate that the driver does not lose control over the car. | Verify that the system does turn off in time if Max\_Torque\_Amplitude crosses the limit. |
| Functional  Safety  Requirement  01-02 | Test and validate that the Max\_Torque\_Frequency chosen is appropriate that the driver does not lose control over the car. | Verify that the system does turn off in time if Max\_Torque\_Frequency crosses the limit. |

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 keeping assistance torque is applied for only Max\_Duration | B | 500 ms | The system shall be switched off. |

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 and validate that the Max\_Duration chosen is appropriate so that it helps prevent drivers from taking their hands off the wheel. | Verify that the system does turn off if the lane keeping assistance duration exceeded Max\_Duration. |

## Refinement of the 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\_Frequency. | **x** |  |  |
| Functional  Safety  Requirement  02-01 | The electronic power steering ECU shall ensure that the lane keeping assistance torque is applied for only Max\_Duration. | **x** |  |  |

## Warning and Degradation Concept

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Degradation Mode** | **Trigger for Degradation Mode** | **Safe State invoked?** | **Driver Warning** |
| WDC-01 | Turn off the functionality. | Malfunction\_01  Malfunction\_02 | Yes | Warning light on the dashboard |
| WDC-02 | Turn off the functionality. | Malfunction\_03 | Yes | Warning light on the dashboard |