

Functional Safety Concept Lane Assistance

**Document Version: [Version]**

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



# Document history

E2 - Low probability

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Editor | Description |
| 08/13/2017 | 1.0 | Yuesong Xie | First Commit |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# Table of Contents

Contents

[Document history 1](#_Toc490397058)

[Table of Contents 2](#_Toc490397059)

[Purpose of the Functional Safety Concept 2](#_Toc490397060)

[Inputs to the Functional Safety Concept 2](#_Toc490397061)

[Safety goals from the Hazard Analysis and Risk Assessment 2](#_Toc490397062)

[Preliminary Architecture 3](#_Toc490397063)

[Description of architecture elements 3](#_Toc490397064)

[Functional Safety Concept 4](#_Toc490397065)

[Functional Safety Analysis 4](#_Toc490397066)

[Functional Safety Requirements 5](#_Toc490397067)

[Refinement of the System Architecture 7](#_Toc490397068)

[Allocation of Functional Safety Requirements to Architecture Elements 7](#_Toc490397069)

[Warning and Degradation Concept 8](#_Toc490397070)

# Purpose of the Functional Safety Concept

Allocates safety goals and functional safety requirements to the system architecture. It looks at the general functionality of the item and does not cover technical implementation.

# 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 LDW 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 |
| Safety\_Goal\_03 | The LKA function shall be deactivated during snowfall (degraded view) conditions |
| Safety\_Goal\_04 | The LKA function shall be deactivated during heavy steering input by the driver |

## Preliminary Architecture



### Description of architecture elements

|  |  |
| --- | --- |
| **Element** | **Description** |
| Camera Sensor | Sends an image stream to the Camera Sensor ECU |
| Camera Sensor ECU | Responsible for detecting lane lines and determining when the vehicle leaves the lane by mistake |
| Car Display | Provides feedback to the driver about on/off and active/inactive status of the Lane Assistance system |
| Car Display ECU | Processes input from Camera Sensor ECU and engages/disengages LEDs on the Car Display |
| Driver Steering Torque Sensor | Responsible for measuring the torque provided by the driver |
| Electronic Power Steering ECU | Responsible for final steering torque output. Adds an appropriate amount of torque based on a Lane Assistance system torque request |
| Motor | Carries out the Electronic Power Steering ECU torque request and provides torque to 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 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 electronic power steering ECU shall ensure that the oscillating torque amplitude is below Max\_Torque\_Amplitude | C | 50ms | Off |
| Functional  Safety  Requirement  01-02 | The electronic power steering ECU shall ensure that the oscillating torque frequency is below Max\_Torque\_Frequency | C | 50ms | 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 how drivers react to different torque amplitudes to prove that we chose an appropriate value. | Software test: When the torque amplitude crosses the limit, the lane assistance output is set to zero within the 50 ms fault tolerant time interval |
| Functional  Safety  Requirement  01-02 | Test how drivers react to different torque frequencies to prove that we chose an appropriate value. | Software test: When the torque frequency crosses the limit, the lane assistance output is set to zero within the 50 ms fault tolerant time interval |

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 | 500ms | 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 that the max\_duration chosen really does dissuade drivers from taking their hands off the wheel | Software Test: Verify that the system really does turn off if the lane keeping assistance every exceeded max\_duration |

## Refinement of the System Architecture

## functionalconcept.png

## 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 oscillating torque amplitude is below Max\_Torque\_Amplitude | **X** |  |  |
| Functional  Safety  Requirement  01-02 | The electronic power steering ECU shall ensure that the 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 | Off | Oscillating torque frequency is above Max\_Torque\_Amplitude or Max\_Torque\_Frequency | Yes | LED on Car Display |
| WDC-02 | Off | Lane keeping assistance torque is applied for more than Max\_Duration | Yes | LED on Car Display |