

Functional Safety Concept Lane Assistance

**Document Version: [Version]**

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



# Document history

**[Instructions: Fill in the date, version and description fields. You can fill out the Editor field with your name if you want to do so. Keep track of your editing as if this were a real world project.**

**For example, if this were your first draft or first submission, you might say version 1.0. If this is a second submission attempt, then you'd add a second line with a new date and version 2.0]**

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Editor | Description |
| 8th May, 2018 | 1.0 | MS Word | Initial version of functional safety |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# Table of Contents

[Document history](#_1t3h5sf)

[Table of Contents](#_ktt3lgighckp)

[Purpose of the Functional Safety Concept](#_fulgh8sf1ocg)

[Inputs to the Functional Safety Analysis](#_757cx6xm46zb)

[Safety goals from the Hazard Analysis and Risk Assessment](#_pi1c1upmo8jt)

[Preliminary Architecture](#_s0p6ihti6jgk)

[Description of architecture elements](#_cqb49updinx4)

[Functional Safety Concept](#_mx8us8onanqo)

[Functional Safety Analysis](#_mtn6qbhgsr36)

[Functional Safety Requirements](#_frlc9y84ede8)

[Refinement of the System Architecture](#_74udkdvf7nod)

[Allocation of Functional Safety Requirements to Architecture Elements](#_g2lqf7kmbspk)

[Warning and Degradation Concept](#_4w6r8buy4lrp)

# Purpose of the Functional Safety Concept

The functional safety concept looks at the general functionality of the item. Each functional safety requirement is then allocated to it’s appropriate place in the item architecture. All this information is taken and put into a document called the functional safety concept.

# 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 system shall be limited |
| Safety\_Goal\_02 | The lane keeping assistance 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. |

## Preliminary Architecture

### 

### Description of architecture elements

|  |  |
| --- | --- |
| **Element** | **Description** |
| Camera Sensor | Lane sensing |
| Camera Sensor ECU | Determine if the car is leaving the lane and if so, send a vibrational torque request to the power steering ECU |
| Car Display | Displaying whether the lane keeping assistance function is on/off; Displaying whether the lane departure warning function is activated or not. |
| Car Display ECU | Receives signals from the camera ECU if either of the functions have been activated |
| Driver Steering Torque Sensor | Senses how much torque is already being applied to the steering wheel. |
| Electronic Power Steering ECU | Receives the vibrational torque request from the camera ECU. Computes the residual torque needed to be applied after taking into account the input from the torque sensor. Sends the torque output request to the motor. |
| Motor | Motor providing the torque to 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 lane departure warning oscillating torque amplitude is below Max\_Torque\_Amplitude. | C | 50ms | Lane departure warning function is not activated |
| Functional  Safety  Requirement  01-02 | The electronic power steering ECU shall ensure that the lane departure warning oscillating torque frequency is below Max\_Torque\_Frequency. | C | 50ms | Lane departure warning function is not activated. |

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 | For whatever value we end up choosing for the max torque amplitude, we need to **validate** that we chose a reasonable value. We would need to test how drivers react to different torque amplitudes and frequencies to prove that we chose an appropriate value. | 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 | For whatever value we end up choosing for the max torque frequency, we need to validate that we chose a reasonable value. We would need to test how drivers react to different torque frequencies to prove that we chose an appropriate value. | when the torque amplitude 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 | Lane keeping assistance is not activated. |

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 | Validate that the max\_duration chosen really did dissuade drivers from taking their hands off the wheel. | The system really does turn off if the lane keeping assistance every 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 warning oscillating torque amplitude is below Max\_Torque\_Amplitude. | **YES** | **NO** | **NO** |
| Functional  Safety  Requirement  01-02 | The electronic power steering ECU shall ensure that the lane departure warning oscillating torque frequency is below Max\_Torque\_Frequency. | **YES** | **NO** | **NO** |
| Functional  Safety  Requirement  02-01 | The electronic power steering ECU shall ensure that the lane keeping assistance torque is applied for only Max\_Duration | **YES** | **NO** | **NO** |

## Warning and Degradation Concept

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Degradation Mode** | **Trigger for Degradation Mode** | **Safe State invoked?** | **Driver Warning** |
| WDC-01 | Turn off functionality | The malfunction of the steering wheel vibrating too much | YES | Warning light on the dashboard |
| WDC-02 | Turn off functionality | The malfunction of the lane keeping assistance function being applied for too long | YES | Warning light on the dashboard. |