

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 |
| 25/12/2018 | 1.0 | Manjunath Gasthi | Initial version |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# Table of Contents

**[Instructions: We have provided a table of contents. If you change the document structure, please update the table of contents accordingly. The table of contents should show each section of the document and page numbers or links. Most word processors can do this for you. In** [**Google Docs**](https://support.google.com/docs/answer/116338?co=GENIE.Platform%3DDesktop&hl=en)**, you can use headings for each section and then go to Insert > Table of Contents.** [**Microsoft Word**](https://support.microsoft.com/en-us/help/285059/how-to-create-a-table-of-contents-by-marking-text-in-word) **has similar capabilities]**

[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 documents the identified system high level requirements.

These requirements are allocated to different parts of the item architecture.

Technical safety requirements will be derived from the safety concept.

The validation and verification concept for these requirements are presented as well.

# 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 Lane Keeping Assistance function shall be time limited, and  additional steering torque shall end after a given time interval so  the driver cannot misuse the system for autonomous driving. |
| Safety\_Goal\_03 | The Lane Departure Warning function shall be deactivated when  the camera sensor stop working. |
| Safety\_Goal\_04 | The LKA function shall always react on time or inform the driver that it  has a malfunction and turns itself off. |

## Preliminary Architecture

### 

### Description of architecture elements

|  |  |
| --- | --- |
| **Element** | **Description** |
| Camera Sensor | Capture road images and provide them to the Camera  Sensor ECU. |
| Camera Sensor ECU | Analyze provided images to calculate the car position  on the road respect to the road lanes. |
| Car Display | Provide feedback to the driver displaying warnings and  the Lane Departure Assistance status. |
| Car Display ECU | Controls the Car Display component to show the Lane  Keeping Assistance warning and Lane Departure  Assistance status. |
| Driver Steering Torque Sensor | Measure the torque applied to the steering wheel by  the driver. |
| Electronic Power Steering ECU | Use the information received from the Driver Steering  Torque Sensor and the torque requested by the Lane  Keeping Assistance and Lane Warning and request the necessary torque to be applied by the Motor actuator. |
| Motor | Applies the torque indicated by the Electronic Power  Steering ECU 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 amplitude  (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 LKA 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 Departure Warning item shall  ensure that the lane departure  oscillating torque amplitude is below  Max\_Torque\_Amplitude. | C | 50 mS | Turn system off. |
| Functional  Safety  Requirement  01-02 | The Lane Departure Warning item shall  ensure that the lane departure  oscillating torque frequency is below  Max\_Torque\_Frequency. | C | 50 mS | Turn system off. |
| Functional  Safety  Requirement  01-03 | The Lane Departure Warning function  shall be deactivated when the camera sensor stop working. | C | 50 mS | Function is  deactivated. |

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 | Validate Max\_Torque\_Amplitude  chosen is high enough to be  detected by a driver while low  enough not to cause loss of steering | Verify the system does turn off if  the Lane Departure Warning  exceeded Max\_Torque\_Amplitude. |
| Functional  Safety  Requirement  01-02 | Validate Max\_Torque\_Frequency  chosen is adequate to be detected  by the driver and not cause the loss  of steering. | Verify the system does turn off if  the Lane Departure Warning  exceeded Max\_Torque\_Frequency. |
| Functional  Safety  Requirement  01-03 | Validate Lane Departure Warning is  off when the camera sensor is not  working. | Verify the Lane Departure Warning  is never on when the camera  sensor is not working. |

**[Instructions: Fill in the functional safety requirements for the lane keeping assistance]**

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 only  Max\_Duration. | B | 500mS | Lane Keeping  Assistance  torque is zero. |

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 really did  dissuade drivers from taking their  hands off the wheel. | Verify that the system 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 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 system off. | Malfunction\_01  Malfunction\_02 | Yes | Warning light on  the dashboard |
| WDC-02 | Turn system off. | Malfunction\_03 | Yes | Warning light on  the dashboard |