

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 |
| 3/13/2018 | 1 | Scott Schnelle | First Draft of Function Safety Concept |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# 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 documents the system’s high level requirements. These requirements are allocated to different parts of the system architecture. Technical safety requirements will be derived from these safety concepts. Instruction on how to validate and verify the 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 Lane Keeping Assistance function shall be deactivated when the camera sensor stop working. |

## Preliminary Architecture

The following figure shows the Lane Assistance item architecture:



### Description of architecture elements

|  |  |
| --- | --- |
| **Element** | **Description** |
| Camera Sensor | Capture road images |
| Camera Sensor ECU | Analyze road images for vehicle/lane localization |
| Car Display | Provide visual feedback to driver |
| Car Display ECU | Provide the display with what systems are active |
| Driver Steering Torque Sensor | Measure driver torque input |
| Electronic Power Steering ECU | Determine how much torque needs to be applied to the steering wheel |
| Motor | Apply toque 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 lead to misuse as an autonomous driving function. |
| Malfunction\_04 | The Lane Departure Warning function shall be deactivated when the camera sensor malfunctions. | WRONG | The Lane Departure Warning start acting randomly when the camera sensor is malfunctioning |
| Malfunction\_05 | The Lane Keeping Assistance function shall be deactivated when the camera sensor malfunctions. | WRONG | The Lane Keeping Assistance start acting randomly when the camera sensor is malfunctioning. |

## 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 | Vibration torque amplitude below Max\_Torque\_Amplitude. |
| 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 | Vibration frequency is below Max\_Torque\_Frequency. |
| Functional Safety Requirement  01-03 | The Lane Departure Warning function shall be deactivated when the camera sensor malfunctions. | C | 10 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 malfunctions. | Verify the Lane Departure Warning is never on when the camera sensor malfunctions. |

Lane Keeping Assistance (LKA) Requirements:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Functional Safety Requirement** | **ASIL** | **Fault Tolerant Time Interval** | **Safe State** |
| Functional  Safety  Requirement  02-01 |  |  |  |  |

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 the Max\_Duration chosen not to allow the driver to use the car as self-driving car. | Verify the system does deactivate if the Lane Keeping Assistance torque application exceeded Max\_Duration. |
| Functional Safety Requirement 02-02 | Validate the Lane Keeping assistance shall be deactivated when the camera sensor malfunctions. | Verify the system does deactivate the Lane Keeping Assistance if the camera sensor malfunctions. |

## 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 Lane Departure Warning item shall ensure that the lane departure oscillating torque amplitude is below Max\_Torque\_Amplitude. | **X** |  |  |
| Functional  Safety  Requirement  01-02 | The Lane Departure Warning item shall ensure that the lane departure oscillating torque frequency is below Max\_Torque\_Frequency. | **X** |  |  |
| Functional Safety Requirement 01-03 | The Lane Departure Warning function shall be deactivated when the camera sensor malfunctions. | **X** |  |  |
| Functional  Safety  Requirement  02-01 | The electronic power steering ECU shall ensure that the Lane Keeping Assistance torque is applied only Max\_Duration. | **X** |  |  |
| Functional Safety Requirement 02-02 | The Lane Keeping assistance shall be deactivated when the electronic power steering ECU detects the camera sensor malfunctions. | **X** |  |  |

## Warning and Degradation Concept

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Degradation Mode** | **Trigger for Degradation Mode** | **Safe State invoked?** | **Driver Warning** |
| WDC-01 | Turn off Lane Departure Warning functionality | Malfunction\_01,  Malfunction\_02,  Malfunction\_04 | Yes | Lane Departure Warning Malfunction Warning on Car Display |
| WDC-02 | Turn off Lane Keeping Assistance functionality | Malfunction\_03,  Malfunction\_05 | Yes | Lane Keeping Assistance Malfunction Warning on Car Display |