

Functional Safety Concept Lane Assistance

**Document Version: 1.0**

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



# Document history

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Editor | Description |
| 16.02.2018 | 1.0 | VIvanov | Draft version |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# 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 is looking at the item from a higher level of architecture without going into technical details.

Functional safety requirements have a few attributes that need to be specified in the functional safety concept:

* The ASIL level
* The fault tolerant time interval, which measures how quickly a system needs to react to a hazardous situation
* The safe state, which discusses what a system looks like after it has avoided an accident

# 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 Lane Departure Warning function shall be limited |
| Safety\_Goal\_02 | Lane Keeping Assistance function shall be time limited and the additional steering torque shall end after a given timer interval so that the driver can not misuse the system for autonomous driving |
| Safety\_Goal\_03 | Lane Keeping Assistance function shall be deactivated, when camera sensor is not able to detect lane boundary. Deactivated status shall be displayed to the driver |
| Safety\_Goal\_04 | Lane Departure Warning function shall control not only lane boundaries, but also traffic in neighbor lanes |

## Preliminary Architecture

The following figure shows the Lane Assistance item architecture



### Description of architecture elements

|  |  |
| --- | --- |
| **Element** | **Description** |
| Camera Sensor | Image Processing and providing images to Camera Sensor ECU |
| Camera Sensor ECU | Object perception and recognition, detection of lane boundaries, evaluation of car position in the lane and generation of torque request to the Electronic Power Steering ECU |
| Car Display | Displaying of Lane Assistant item state, activity and warning messaged to the driver |
| Car Display ECU | Generating of warning messages triggered by Camera Sensor ECU and Electronic Power Steering ECU |
| Driver Steering Torque Sensor | Measuring of torque applied to the steering wheel by the driver to Electronic Power Steering ECU |
| Electronic Power Steering ECU | Processing of inputs from Camera Sensor ECU, Driver Steering Torque Sensor and the torque request from the Lane Keeping Assistance and Lane Warning, evaluating of final torque to be applied by motor |
| Motor | Applying the torque evaluated by the Electronic Power Steering ECU |

# 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 |  |  |
| Malfunction\_02 | Lane Departure Warning (LDW) function shall apply an oscillating steering torque to provide the driver a haptic feedback |  |  |
| Malfunction\_03 | Lane Keeping Assistance (LKA) function shall apply the steering torque when active in order to stay in ego lane |  |  |

## Functional Safety Requirements

**[Instructions: Fill in the functional safety requirements for the lane departure warning ]**

Lane Departure Warning (LDW) Requirements:

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

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 |  |  |
| Functional  Safety  Requirement  01-02 |  |  |

**[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 |  |  |  |  |

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 |  |  |

## Refinement of the System Architecture

**[Instructions: Include the refined system architecture. Hint: The refined system architecture should include the system architecture from the end of the functional safety lesson including all of the ASIL labels.]**

## Allocation of Functional Safety Requirements to Architecture Elements

**[Instructions: Mark which element or elements are responsible for meeting the functional safety requirement. Hint: Only one ECU is responsible for meeting all of the requirements.]**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Functional Safety Requirement** | **Electronic Power Steering ECU** | **Camera ECU** | **Car Display ECU** |
| Functional  Safety  Requirement  01-01 |  |  |  |  |
| Functional  Safety  Requirement  01-02 |  |  |  |  |
| Functional  Safety  Requirement  02-01 |  |  |  |  |

## Warning and Degradation Concept

**[Instructions: Fill in the warning and degradation concept.]**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Degradation Mode** | **Trigger for Degradation Mode** | **Safe State invoked?** | **Driver Warning** |
| WDC-01 |  |  |  |  |
| WDC-02 |  |  |  |  |