

Functional Safety Concept Lane Assistance

**Document Version: [Version]**

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



# Document history

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Editor | Description |
| 02/03/2018 | 0.1 | Michael Scharf | Initial attempt |
| 02/03/2018 | 0.2 | Michael Scharf | Start filling out document |
| 02/03/2018 | 0.3 | Michael Scharf | Fill out whole sheet |
| 02/03/2018 | 1.0 | Michael Scharf | Internal Review and smaller fixes. |
| 02/04/2018 | 2.0 | Michael Scharf | Correct review findings after submission. |

# 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

To achieve the overall goal of functional safety to avoid accidents by reducing risk to an acceptable level, the FSC is

* Identifying subsystems containing high level of risk
* Identifying countermeasure to reduce risks and therefore prevent accidents.

# 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 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 | Grab surrounding/ camera images of the road |
| Camera Sensor ECU | Lane Sensing: identifies if the vehicle departs its lane. Torque request generator: sends messages to the Car Display ECU in order to react on the situation the car departed from its lane. |
| Car Display | Display status of the Lane Assistance. If the Lane Assistance is activated or not and if the Lane Assistance is actually “active” in sense of triggering correction of the steering torque |
| Car Display ECU | Manages the state and loopback of the Lane Assistance On/Off status as well as the Lane Assistance Active/ Inactive status. The Car Display ECU will switch on/off corresponding indication in Car Display depending on the state of the Lane Assistance. |
| Driver Steering Torque Sensor | Sensing steering wheel torque |
| Electronic Power Steering ECU | Is the “Lane Assistance Functionality” itself. It analyzes Driver Steering torque and reacts on the triggers from Camera Sensor ECU in order to generate a final electronic power steering torque output. This output signal is send to the Motor then.  Depending on the status of the EPS ECU, a feedback is send to the Car Display ECU to indicate the active/ inactive state of the Lane Assistance (if it is currently influencing the steering wheel). |
| Motor | Providing 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 | The lane departure warning is giving MORE torque than what is safe | 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 | The lane departure warning is giving MORE torque than what is safe | 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 | The lane keeping assistance function has NO limit in time duration which leads to misuse as an autonomous driving function. | The lane keeping assistance if misused for autonomous driving |

## Functional Safety Requirements

Lane Departure Warning (LDW) Requirements:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Functional Safety Requirement** | **ASIL** | **Fault Tolerant Time Interval** | **Safe State** |
| Functional  Safety  Requirement  01-01 | 1. The lane keeping item shall ensure that the lane departure oscillating torque amplitude is below Max\_Torque\_Amplitude | C | 50 mS | Set amplitude to zero. |
| Functional  Safety  Requirement  01-02 | 1. The lane keeping item shall ensure that the lane departure oscillating torque frequency is below Max\_Torque\_Frequency | C | 50 mS | Set frequency to zero. |

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 | The drivers respond in a safe way on the chosen Max\_Torque\_Amplitude value chosen. | Test that in case of a violation of the Max\_Torque\_Amplitude, the lane assistence output Amplitude is set to zero within 50 mS (Safe state). |
| Functional  Safety  Requirement  01-02 | The drivers respond in a safe way on the chosen Max\_Torque\_Frequency value chosen. | Test that in case of a violation of the Max\_Torque\_ Frequency, the lane assistence output Frequency is set to zero within 50 mS (Safe state). |

Lane Keeping Assistance (LKA) Requirements:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Functional Safety Requirement** | **ASIL** | **Fault Tolerant Time Interval** | **Safe State** |
| Functional  Safety  Requirement  02-01 | 1. The lane keeping item shall ensure that the lane keeping assistance torque is applied for only Max\_Duration | B | 500 mS | Set the lane keeping assistance torque to 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 | The chosen Max\_Duration dissuade drivers from taking their hands of the wheel. | Verify that lane keeping assistance torque is set to zero if the lane keeping assitance 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 | 1. 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 | 1. 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 of functionality | ECU receives a vibrational torque request beyond the allowed maximum | yes | Indication of malfunction via driver dashboard |
| WDC-02 | Turn off functionality | ECU recognizes timeout of drivers interaction for lane keeping | yes | No automatic lane keeping. Eventually warning notification in drivers dashboard or hint in the manual that driver maintains responsibility for safe operation of the vehicle. |