

Functional Safety Concept Lane Assistance

**Document Version: [Version]**

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



# Document history

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Editor | Description |
| 2018/06/10 | 1.0 | Frank . W | First 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

Given the safety goal, deriving functional safety requirements based on preliminary architecture, determining the property of functional safety requirements such as ASIL, fault tolerant time interval, and safe state as well as verification and validation acceptance criteria, then refining the system architecture and allocating requirements, finally defining warning and degradation 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 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 | Transform ambient information into digital images and send them to Camera Sensor ECU. |
| Camera Sensor ECU | Detect lane line position from digital images send by Camera Sensor |
| Car Display | Transform the information sent by Car Display ECU into visual signals |
| Car Display ECU | Collect current vehicle status information and show the information to the driver by controlling Car Display. |
| Driver Steering Torque Sensor | Transform the Steering Torque into electrical signal |
| Electronic Power Steering ECU | Calculate the turning direction and torque of the motor according to the steering direction and torque size sent by the Driver Steering Torque Sensor. |
| Motor | Generate corresponding steering torque according to the instruction from 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 | 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 oscillating torque amplitude is below“Max\_Torque\_Amplitude” | C | 50ms | Set vibration torque amplitude to 0 |
| Functional  Safety  Requirement  01-02 | The electronic power steering ECU shall ensure that the lane departure oscillating torque frequency is below “Max\_Torque\_Frequency” | C | 50ms | Set vibration torque frequency to 0 |

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 | Test how drivers react to different torque amplitudes 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.  For this specific case, we would probably do a software test inserting a fault into the system and seeing what happens. |
| Functional  Safety  Requirement  01-02 | Test how drivers react to different torque frequencies to prove that we chose an appropriate value. | When the torque frequency crosses the limit, the lane assistance output is set to zero within the 50 ms fault tolerant time interval.  For this specific case, we would probably do a software test inserting a fault into the system and seeing what happens. |

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 | Set lane keeping assistance torque to 0 |

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 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 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 off LDW  function. | Malfunction\_01 /  Malfunction\_02 | Yes | Blink light on car display |
| WDC-02 | Turn off LKA  function. | Malfunction\_03 | Yes | Blink light on car display |