

Functional Safety Concept Lane Assistance

**Document Version: [Version]**

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



# 

# Document history

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Editor | Description |
| 05/22/2018 | 1.0 | Swapnil More | First Draft |
| 06/15/2018 | 1.1 | Swapnil More | Updates to First Draft |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# 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 purpose of the functional safety concept is to look at the item from a high-level perspective, refine the safety goals from hazard analysis and risk assessment as functional safety requirements, allocate safety requirements to the relevant parts of the system diagram; and discuss the verification, validation i.e. how to prove that the system actually meets the requirements.

# Inputs to the Functional Safety Concept

## Safety goals from the Hazard Analysis and Risk Assessment

|  |  |
| --- | --- |
| **ID** | **Safety Goal** |
| Safety\_Goal\_01 | The oscillating torque to the steering wheel from the lane keeping assistance 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 Assistance provided by the Lane Keeping System shall be limited. |
| Safety\_Goal\_04 | The Lane Keeping Assistance function shall be deactivated when the camera sensor stops working. |

## 

## Preliminary Architecture

The lane assistance item preliminary architecture:



### Description of architecture elements

|  |  |
| --- | --- |
| **Element** | **Description** |
| Camera Sensor | Capture images and send them to the Camera Sensor ECU |
| Camera Sensor ECU | Process images to detect lane lines, calculate the vehicles position with respect to the lane lines and send information to the EPS ECU |
| Car Display | Display the Lane Departure Warning and status of the Lane Assistance System |
| Car Display ECU | Control the car display based on inputs from the camera sensor ECU |
| Driver Steering Torque Sensor | Measure Steering Wheel Torque |
| Electronic Power Steering ECU | Calculate the assistance torque, motor torque based on inputs from the camera sensor ECU |
| Motor | Generate torque requested by the EPS 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 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 | Lane Keeping Assistance (LKA) function shall apply the steering torque when active to stay in ego lane | MORE | The Lane Keeping Assistance applies a torque with very high torque amplitude (above limit) |
| Malfunction\_05 | Lane Departure Warning (LDW) function shall apply an oscillating steering torque to provide the driver with haptic feedback | WRONG | The Lane  Departure Warning  start acting  randomly when the  camera sensor is  not working. |

## 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\_A  mplitude. |
| 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\_Fr  equency. |
| Functional  Safety  Requirement  01-03 | The Lane Departure Warning function  shall be deactivated when the camera sensor stops working. | C | 50 ms | Camera sensor status is active. |

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. |

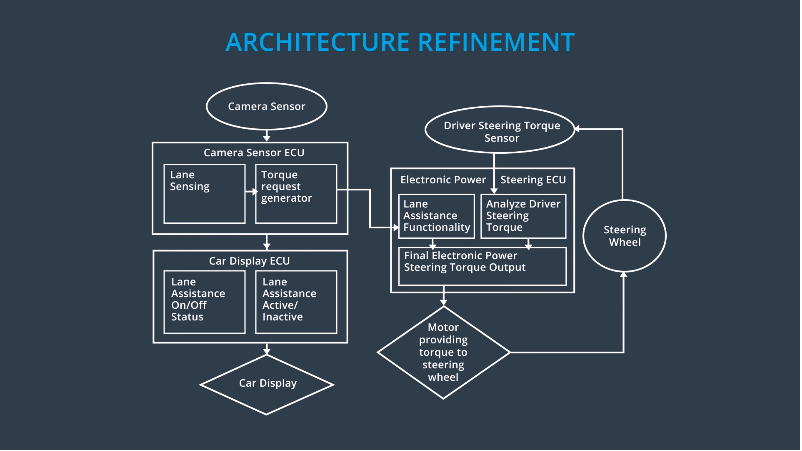
Lane Keeping Assistance (LKA) Requirements:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Functional Safety Requirement** | **ASIL** | **Fault Tolerant Time Interval** | **Safe State** |
| Functional  Safety  Requirement  02-01 | The Lane Keeping Assistance item shall ensure that the time duration for steering assistance is below Max\_Assist\_Time | B | 500 ms | Assistance time is below Max\_Assist\_Time |
| Functional  Safety  Requirement  02-02 | The Lane Keeping Assistance item shall  ensure that the lane assist torque amplitude is below  Max\_Assist\_Amplitude. | C | 50 ms | Assistance torque amplitude is below Max\_Assist\_Torque |

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 Max\_Assist\_Time  chosen is adequate to provide required assistance but not long enough for the driver to misuse the system | Verify the system does turn off if  the Lane Keeping Assistance  exceeded Max\_Assist\_Time |
| Functional  Safety  Requirement  02-02 | Validate Max\_Assist\_Amplitude  chosen is adequate to provide required assistance and not cause the loss of steering | Verify the system does turn off if  the Lane Keeping Assistance  exceeded Max\_Assist\_Amplitude |

## 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  01-03 | The Electronic Power Steering ECU shall deactivate the Lane Departure Warning function when the camera sensor stops working. | **X** |  |  |
| Functional  Safety  Requirement  02-01 | The Electronic Power Steering ECU shall ensure that the time duration for steering assistance is below Max\_Assist\_Time | **X** |  |  |
| Functional  Safety  Requirement  02-02 | The Electronic Power Steering ECU shall ensure that the lane assist torque amplitude is below Max\_Assist\_Amplitude. | **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\_05 | Yes | Lane  Departure  Warning  Malfunction  Warning on  Car Display |
| WDC-02 | Turn off Lane  Keeping  Assistance  functionality | Malfunction\_03,  Malfunction\_04 | Yes | Lane Keeping  Assistance  Malfunction  Warning on  Car Display |