

Functional Safety Concept Lane Assistance

**Document Version: 1.0**

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



# Document history

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Editor | Description |
| 5/25/2018 | 1.0 | Rahul Bhartari | First revision |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# Table of Contents

[Document history](#_Toc515273186)

[Table of Contents](#_Toc515273187)

[Purpose of the Functional Safety Concept](#_Toc515273188)

[Inputs to the Functional Safety Concept](#_Toc515273189)

[Safety goals from the Hazard Analysis and Risk Assessment](#_Toc515273190)

[Preliminary Architecture](#_Toc515273191)

[Description of architecture elements](#_Toc515273192)

[Functional Safety Concept](#_Toc515273193)

[Functional Safety Analysis](#_Toc515273194)

[Functional Safety Requirements](#_Toc515273195)

[Refinement of the System Architecture](#_Toc515273196)

[Allocation of Functional Safety Requirements to Architecture Elements](#_Toc515273197)

[Warning and Degradation Concept](#_Toc515273198)

# Purpose of the Functional Safety Concept

The functional safety concept is a high level approach to look at the general functionality of the item without going into technical details. The goal is to identify new requirements and then allocate those requirements to different parts of the item architecture. Technical safety requirements can be derived from these safety concepts. Functional safety requirements also have a few attributes that need to be specified in the functional safety concept.  To prove that a system actually meets the functional safety requirements, verification and validation is also done.

# Inputs to the Functional Safety Concept

## Safety goals from the Hazard Analysis and Risk Assessment

|  |  |
| --- | --- |
| **ID** | **Safety Goal** |
| Safety\_Goal\_01 | The Lane departure warning system should be deactivated when driving on roads with faded or missing lane markings |
| Safety\_Goal\_02 | The amount of torque applied by Lane Keeping Assistance function on steering wheel should be limited and zero when driver applies torque more than some threshold |
| Safety\_Goal\_03 | The Lane Keeping Assistance function must engage for certain number of times in given duration and thereafter alert the driver and disengage to prevent misuse |
| Safety\_Goal\_04 | Steering wheel oscillations should be limited to reasonable levels |
| Safety\_Goal\_05 | The Lane Departure Warning system must show the status of essential sensors and warn the driver of any discrepancy when switched on, so that driver may not rely completely on the system while driving |

## Preliminary Architecture

Following diagram shows the preliminary architecture of the Lane Assistance system:



### Description of architecture elements

|  |  |
| --- | --- |
| **Element** | **Description** |
| Camera Sensor | Capture the scene and send the image data to Camera Sensor ECU |
| Camera Sensor ECU | Calculate the position of car on the road with respect to the lane markings |
| Car Display | Display the system status and warnings to the driver |
| Car Display ECU | Drive the Car Display component |
| Driver Steering Torque Sensor | Measure the torque applied by the driver on the steering wheel |
| Electronic Power Steering ECU | Get the measurements from Driver steering Torque Sensor and torque requested by Lane Keeping Assistance function and drive the motor to apply torque accordingly |
| Motor | Apply the torque to the 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 a high amplitude oscillating torque(above limits) |
| 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 a high frequency oscillating torque(above limits) |
| 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 by time and number of times engaged, leading to potential misuse |
| Malfunction\_04 | Lane Keeping Assistance (LKA) function shall apply limited torque when driver applies opposite torque above certain limit | NO | The Lane Keeping Assistance is not limited by torque amplitude, leading to accident in case an object suddenly comes in ego lane |
| Malfunction\_05 | Lane Departure Warning (LDW) function shall be deactivated when not able to find lanes on road and alert the driver | WRONG | The Lane Departure Warning function may give false alerts when used on roads with faded or missing lanes |
| Malfunction\_06 | The Lane Departure Warning (LDW) function shall be deactivated in case of any discrepancy with the system and alert the driver | WRONG | The Lane Departure Warning function does not monitor the state of the sensors and does not issue warning when required |

## 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 (LDW) function shall ensure that amplitude of oscillating torque is less than Max\_Torque\_Amplitude | C | 50ms | Oscillation torque amplitude is less than Max\_Torque\_Amplitude |
| Functional  Safety  Requirement  01-02 | The Lane Departure Warning (LDW) function shall ensure that frequency of oscillating torque is less than Max\_Torque\_Frequency | C | 50ms | Oscillation torque frequency is less than Max\_Torque\_Frequency |
| Functional  Safety  Requirement  01-03 | The Lane Departure Warning (LDW) function shall be deactivated when any discrepancy in sensors or state of Camera Subsystem is Lane\_Not\_Found | A | 50ms | Lane Departure Warning function is off |

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 if Max\_Torque\_Amplitude is chosen such that it is detectable by the driver and does not cause the loss of steering | Verify that system turns off if torque amplitude ever exceeds Max\_Torque\_Amplitude |
| Functional  Safety  Requirement  01-02 | Validate if Max\_Torque\_Frequency is chosen such that it is detectable by the driver and does not cause the loss of steering | Verify that system turns off if torque amplitude ever exceeds Max\_Torque\_Frequency |
| Functional  Safety  Requirement  01-03 | Validate if Lane Departure warning function turns off when Lane\_Not\_Found is set | Verify that system turns off is Lane\_Not\_Found is set |

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 (LKA) function must limit the number of times it engages to keep vehicle in lane | B | 100ms | The Lane Keeping Assistance Torque is zero |
| Functional  Safety  Requirement  02-02 | The Lane Keeping Assistance (LKA) function must limit the amplitude of torque it applies on steering wheel and disengage when driver applying opposite torque | B | 50ms | The Lane Keeping Assistance Torque is 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 | Validate if Lane Keeping Assistance function applies torque for duration Max\_Duration, Max\_Engage\_Count number of times and zero torque threafter | Verify that the system outputs zero torque after Max\_Duration and Max\_Engage\_Count is exceeded |
| Functional  Safety  Requirement  02-02 | Validate if Lane Keeping Assistance sends zero torque to motor if Driver applies torque more than Max\_Driver\_Torque on steering wheel | Verify that Lane Keeping Assistance function sends zero torque when driver torque is more than Max\_Driver\_Torque |

## 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 than oscillating torque amplitude is less than Max\_Torque\_Amplitude | **X** |  |  |
| Functional  Safety  Requirement  01-02 | The Electronic power steering ECU shall ensure than oscillating torque frequency is less than Max\_Torque\_Frequency | **X** |  |  |
| Functional  Safety  Requirement  01-03 | The Lane Departure warning function shall turn off when Lane\_Not\_Found is set |  | **X** |  |
| Functional  Safety  Requirement  02-01 | The Electronic power steering ECU shall apply torque for duration Max\_Duration and Max\_Engage\_Count number of times | **X** |  |  |
| Functional  Safety  Requirement  02-02 | The Electronic power steering ECU sends zero torque to motor if Driver applies torque more than Max\_Driver\_Torque on steering wheel | **X** |  |  |

## Warning and Degradation Concept

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Degradation Mode** | **Trigger for Degradation Mode** | **Safe State invoked?** | **Driver Warning** |
| WDC-01 | Turn off Lane Departure Warning Function | Malfunction\_01  Malfunction\_02  Malfunction\_05  Malfunction\_06 | Yes | Lane Departure Warning Malfunction warning on car display |
| WDC-02 | Turn off Lane Keeping Assistance Function | Malfunction\_03  Malfunction\_04 | Yes | Lane Keeping Assistance Malfunction warning on car display |