

Functional Safety Concept Lane Assistance

**Document Version: 2.0**

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



# Document history

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Editor | Description |
| 24 May 2018 | 1.0 | Vivekkumar Mehta | First version of functional safety concept |
| 24 May 2018 | 2.0 | Vivekkumar Mehta | Second version of functional safety concept |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# 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 will help in identifying new requirements and allocate these requirements to system diagrams. The functional safety concept is looking at the item from a higher level. The functional safety concept looks at the general functionality of the item.

# Inputs to the Functional Safety Concept

## Safety goals from the Hazard Analysis and Risk Assessment

|  |  |
| --- | --- |
| **ID** | **Safety Goal** |
| Safety\_Goal\_01 | The LDW steering torque function shall be limited. |
| Safety\_Goal\_02 | LKA function excess usage shall be alerted or stopped after certain time limit |

## Preliminary Architecture

This figure describes architecture of Lance assistance system.



### Description of architecture elements

|  |  |
| --- | --- |
| **Element** | **Description** |
| Camera Sensor | Provides visual input to camera sensor ECU |
| Camera Sensor ECU | Detects ego lane lines and gives torque input to Electronic power steering ECU. |
| Car Display | Gives visual feedback to driver |
| Car Display ECU | Generates warning signals from camera sensor ECU and electronic power steering ECU |
| Driver Steering Torque Sensor | Gives steering torque input to electronic power steering ECU given by driver |
| Electronic Power Steering ECU | Gets steering input from driver and camera sensor ECU, computes final torque and gives it to steering wheel motor. |
| Motor | Receives final torque and applies it 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 | MORE | The LDW function applies too much torque with high 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 LDW function applies too much torque with high oscillations (above limit). |
| Malfunction\_03 | Lane Keeping Assistance (LKA) function shall apply the steering torque when active in order to stay in ego lane | WRONG | The LKA functions works randomly when 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 keeping item shall ensure that the lane departure oscillating torque *amplitude* is below Max\_Torque\_Amplitude | C | 50 ms | Vibration torque amplitude below Max\_Torque\_Amplitude |
| Functional  Safety  Requirement  01-02 | The lane keeping item shall ensure that the lane departure oscillating torque *frequency* is below Max\_Torque\_Frequency | C | 50 ms | Vibration torque frequency below Max\_Torque\_Frequency |

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 an appropriate value was chosen. | Verify that system turns off if LDW ever exceeds Max\_Torque\_Amplitude. |
| Functional  Safety  Requirement  01-02 | Test how drivers react to different torque frequencies to prove that an appropriate value was chosen. | Verify that system turns off if LDW ever exceeds Max\_Torque\_Frequency. |

Lane Keeping Assistance (LKA) Requirements:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Functional Safety Requirement** | **ASIL** | **Fault Tolerant Time Interval** | **Safe State** |
| Functional  Safety  Requirement  02-01 | The lane keeping item shall ensure that the lane keeping assistance torque is applied for only Max\_Duration. | B | 500 ms | LKA torque amplitude is zero. |
| Functional  Safety  Requirement  02-02 | The electronic power steering ECU shall ensure that lane keeping assistance torque is zero if camera sensor ECU states Lane\_Not\_Found is true | A | 50 ms | LKA torque amplitude is zero. |
| Functional  Safety  Requirement  02-03 | The camera sensor ECU shall not request torque if Laneline\_Is\_Yellow is stated true by camera sensor ECU. | D | 25 ms | LKA torque amplitude 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 | Test and validate that the Max\_Duration chosen really dissuades drivers from taking their hands off the wheel. | Verify that system turns off if LKA ever exceeds MAX\_DURATION. |
| Functional  Safety  Requirement  02-02 | Test and validate that Lane\_Not\_Found is stated correctly if lane lines cannot be detected. | Verify that system turns off if Lane\_Not\_Found is true. |
| Functional  Safety  Requirement  02-03 | Test and validate that Laneline\_Is\_Yellow is stated correctly, if lanelines turn yellow. | Verify that system turns off if Laneline\_Is\_Yellow is true. |

## 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** |  |  |
| Functional  Safety  Requirement  02-02 | The electronic power steering ECU shall ensure that lane keeping assistance torque is zero if camera sensor ECU states Lane\_Not\_Found is true | **x** |  |  |
| Functional  Safety  Requirement  02-03 | The electronic power steering ECU shall ensure that lane keeping assistance torque is zero if camera sensor ECU states Laneline\_Is\_Yellow is true | **x** |  |  |

## Warning and Degradation Concept

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Degradation Mode** | **Trigger for Degradation Mode** | **Safe State invoked?** | **Driver Warning** |
| WDC-01 | Turn off Lane Assistant functionality | Malfunction\_01 | Yes | Lane Assistant Malfunction Warning on Car Display |
| WDC-02 | Turn off Lane Assistant functionality | Malfunction\_02 | Yes | Lane Assistant Malfunction Warning on Car Display |
| WDC-03 | Turn off Lane Assistant functionality | Malfunction\_03 | Yes | Lane Assistant Malfunction Warning on Car Display |
| WDC-04 | Turn off Lane Assistant functionality | Malfunction\_04 | Yes | Lane Assistant Malfunction Warning on Car Display |
| WDC-05 | Turn off Lane Assistant functionality | Malfunction\_05 | Yes | Lane Assistant Malfunction Warning on Car Display |