

Functional Safety Concept Lane Assistance

**Document Version: [Version]**

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



# Document history

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Editor | Description |
| June 21, 2017 | 1.0 | Udacity, EB | Template version |
| April 22, 2019 | 1.1 | Ahmed Belal | Finalize the document |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# 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 (FSC) is the following:

* Derive functional safety requirement from the safety goals to refine the safety goals
* Allocating these safety requirements to the relevant parts of the system diagram which means defining which part of the system architecture will implement each requirement
* Refine the system architecture to handle the new requirements
* Assigning ASIL level to the system architecture blocks which will inherit the highest assigned requirement ASIL
* The fault tolerant time interval, which measures how quickly a system needs to react to a hazardous situation
* And the safe state, which discusses what a system looks like after it has avoided an accident

# Inputs to the Functional Safety Concept

## Safety goals from the Hazard Analysis and Risk Assessment

|  |  |
| --- | --- |
| **ID** | **Safety Goal** |
| Safety\_Goal\_01 | Lane Departure Warning (LDW) function shall apply a limited oscillating steering torque to provide the driver with haptic feedback |
| Safety\_Goal\_02 | The Lane Keeping Assistance (LKA) 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 |
| Safety\_Goal\_03 | Lane Keeping Assistance (LKA) function shall apply a limited steering torque when active in order to stay in ego lane |
| Safety\_Goal\_04 | Lane Keeping Assistance (LKA) function shall apply the steering torque in the correct direction when active in order to stay in ego lane |

## Preliminary Architecture



### Description of architecture elements

|  |  |
| --- | --- |
| **Element** | **Description** |
| Camera Sensor | Capture the road images (video) |
| Camera Sensor ECU | Processing the images (video) provided by the camera sensor for detecting the lane lines and determining when the vehicle leaves the lane by mistake |
| Car Display | Screen for showing the notification, warnings and vehicle status for the driver |
| Car Display ECU | Control the displayed data on the car display |
| Driver Steering Torque Sensor | Measure the steering torque applied on the steering wheels |
| Electronic Power Steering ECU | Control the steering wheels by sending the appropriate steering torque control signal to the steering motor driver |
| Motor | Apply the steering torque based on the received steering control signal from the Electronic power steering (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 a limited oscillating steering torque to provide the driver with haptic feedback | MORE | The lane departure warning (LDW) function applies an oscillating torque with very high torque amplitude (above limit) |
| Malfunction\_02 | Lane Departure Warning (LDW) function shall apply a limited oscillating steering torque to provide the driver with haptic feedback | MORE | The lane departure warning (LDW) function applies an oscillating torque with very high torque frequency (above limit) |
| Malfunction\_03 | The Lane Keeping Assistance (LKA) 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 | NO | The Lane Keeping Assistance (LKA) function is not limited in time duration which leads to misuse as an autonomous driving function. |
| Malfunction\_04 | Lane Keeping Assistance (LKA) function shall apply a limited steering torque when active in order to stay in ego lane | MORE | Lane Keeping Assistance (LKA) function applies a steering torque with very high torque amplitude which affect the driver ability to steer the vehicle(above limit) |
| Malfunction\_05 | Lane Keeping Assistance (LKA) function shall apply the steering torque in the correct direction when active in order to stay in ego lane | WRONG | Lane Keeping Assistance (LKA) function applies the steering torque in the wrong direction |

## 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 (EPS) ECU shall ensure that the lane departure oscillating torque amplitude is below the MAX\_TORQUE\_AMPLITUDE | C | 50ms | Shut the system down by setting lane assistance output is set to zero |
| Functional  Safety  Requirement  01-02 | The electronic power steering (EPS) ECU shall ensure that the lane departure oscillating torque frequency is below the MAX\_TORQUE\_FREQUENCY | C | 50ms | Shut the system down by setting lane assistance output is set 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 | Validate the LDW MAX\_TORQUE\_AMPLITUDE of the oscillating steering torque | Verify that the LDW will shut down if the MAX\_TORQUE\_AMPLITUDE exceeded |
| Functional  Safety  Requirement  01-02 | Validate the LDW MAX\_TORQUE\_FREQUENCY of the oscillating steering torque | Verify that the LDW will shut down if the MAX\_TORQUE\_ FREQUENCY exceeded |

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 (EPS) ECU shall ensure that the lane keeping assistance (LKA) torque is applied for only MAX\_DURATION | B | 500ms | Shut the system down by setting lane assistance output is set to zero |
| Functional  Safety  Requirement  03-01 | The electronic power steering (EPS) ECU shall ensure that the lane keeping assistance (LKA) torque is below the MAX\_TORQUE\_AMPLITUDE when active in order to stay in ego lane | C | 500ms | Shut the system down by setting lane assistance output is set to zero |
| Functional  Safety  Requirement  04-01 | The electronic power steering (EPS) ECU shall ensure that the lane keeping assistance (LKA) torque is applied in the correct direction when active in order to stay in ego lane | C | 500ms | Shut the system down by setting lane assistance output is set 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 | Validate the LKA MAX\_DURATION of the steering torque | Verify that the LKA will shut down if the steering torque MAX\_DURATION exceeded |
| Functional  Safety  Requirement  03-01 | Validate the LKA MAX\_TORQUE\_AMPLITUDE of the steering torque | Verify that the LKA will shut down if the MAX\_TORQUE\_AMPLITUDE exceeded |
| Functional  Safety  Requirement  04-01 | Validate the LKA correct steering torque direction | Verify that the LKA will shut down if the steering torque applied in the wrong direction |

## 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 (EPS) ECU shall ensure that the lane departure oscillating torque amplitude is below the MAX\_TORQUE\_AMPLITUDE | ✔ |  |  |
| Functional  Safety  Requirement  01-02 | The electronic power steering (EPS) ECU shall ensure that the lane departure oscillating torque frequency is below the MAX\_TORQUE\_FREQUENCY | ✔ |  |  |
| Functional  Safety  Requirement  02-01 | The electronic power steering (EPS) ECU shall ensure that the lane keeping assistance (LKA) torque is applied for only MAX\_DURATION | ✔ |  |  |
| Functional  Safety  Requirement  03-01 | The electronic power steering (EPS) ECU shall ensure that the lane keeping assistance (LKA) torque is below the MAX\_TORQUE\_AMPLITUDE when active in order to stay in ego lane | ✔ |  |  |
| Functional  Safety  Requirement  04-01 | The electronic power steering (EPS) ECU shall ensure that the lane keeping assistance (LKA) torque is applied in the correct direction when active in order to stay in ego lane | ✔ |  |  |

## Warning and Degradation Concept

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Degradation Mode** | **Trigger for Degradation Mode** | **Safe State invoked?** | **Driver Warning** |
| WDC-01 | Shut the system down by setting lane assistance output is set to zero | Malfunction\_01  Malfunction\_02 | Yes | Display LDW warning on driver dashboard |
| WDC-02 | Shut the system down by setting lane assistance output is set to zero | Malfunction\_03  Malfunction\_04  Malfunction\_05 | Yes | Display LKA warning on driver dashboard |