

Functional Safety Concept Lane Assistance

**Document Version: 1.0**

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



# Document history

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Editor | Description |
| 03/03/2019 | 1.0 | Rangarajan Ramanujam | Initial 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 Functional Safety Concept documents the identified system high level requirements. These requirements are allocated to different parts of the item architecture. Technical Safety requirements are derived from the safety concept. The validation and verification concept for these requirements are presented as well.

# 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 LDW function shall be limited in amplitude. |
| Safety\_Goal\_02 | LKA function shall apply additional steering torque that will be time limited and shall end after a given timer interval so that the driver cannot misuse the system for autonomous driving. |
| Safety\_Goal\_03 | The oscillating steering torque from the LDW function shall stop when the driver is trying to control the car in bad weather conditions. |
| Safety\_Goal\_04 | LKA function shall not apply any steering torque and function shall be temporarily shut down when the driver is braking. |

## Preliminary Architecture

The following figure shows the architecture of the Lane Assistance system.

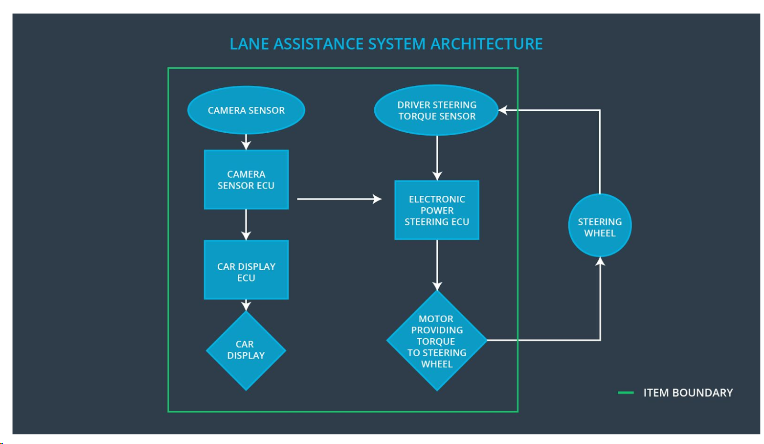


Fig 1: Lane Assistance System Architecture

### Description of architecture elements

Based on the architecture snapshot, the below description provides a detailed description of the individual elements.

|  |  |
| --- | --- |
| **Element** | **Description** |
| Camera Sensor | Capture road images and provide them to the Camera Sensor ECU |
| Camera Sensor ECU | Analyze provided images to calculate the car position on the road with respect to lane lines |
| Car Display | Provide feedback to the driver displaying warnings and the Lane Departure Assistance status |
| Car Display ECU | Drive the Car Display component to show the Lane Keeping Assistance warning and Lane Departure Assistance status |
| Driver Steering Torque Sensor | Measure the torque applied to the steering wheel by the driver |
| Electronic Power Steering ECU | Use the information received from the Driver Steering Torque Sensor and torque requested by the Lane Keeping Assistance and Lane Departure Warning and request necessary torque to be applied by the power steering motor actuator |
| Motor | Applies the torque indicated by the Electronic Power Steering ECU 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 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 |
| Malfunction\_04 | Lane Keeping Assistance (LKA) function shall apply the steering torque when active in order to stay in ego lane | MORE | The Lane Keeping Assistance function is not shut down when the driver is braking |
| Malfunction\_05 | 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 when the driver is trying to control the car in bad weather conditions. |

## 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 | LDW Torque amplitude is set to zero |
| 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 | LDW Torque amplitude is set to zero |
| Functional  Safety  Requirement  01-03 | The lane keeping item shall ensure that the lane departure oscillating torque will be turned off when the driver is applying more than Max\_Driver\_Torque\_Amplitude | B | 20 mS | LDW Torque amplitude 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 | Test and validate that the Max\_Torque\_Amplitude chosen is high enough to be detected by the driver and low enough that the driver does not lose control over the car | Verify the LDW functionality is deactivated if Max\_Torque\_Amplitude is exceeded |
| Functional  Safety  Requirement  01-02 | Test and validate that the Max\_Torque\_Frequency chosen is high enough to be detected by the driver and low enough that the driver does not lose control over the car | Verify the LDW functionality is deactivated if Max\_Torque\_Frequency is exceeded |
| Functional  Safety  Requirement  01-03 | Test and validate that the Max\_Driver\_Torque\_Amplitude is chosen to be high enough that the driver is able to gain control of the car (if desired)under all driving conditions | Verify whether the Lane departure functionality is temporarily deactivated when driver torque input has exceeded Max\_Driver\_Torque\_Amplitude |

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 only for Max\_Duration | B | 500 mS | Lane Keeping Assistance Torque is zero |
| Functional  Safety  Requirement  02-02 | The electronic power steering ECU shall ensure that the Lane Keeping Assistance shall be deactivated under braking conditions | A | 50 mS | 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 | Test and validate that Max\_Duration is chosen appropriately to not allow the driver to use the car as self-driving car | Verify the LKA functionality is deactivated if the Lane keeping assistance torque application exceed Max\_Duration |
| Functional  Safety  Requirement  02-02 | Test and Validate that the Lane Keeping Assistance shall be deactivated under braking conditions | Verify the LKA functionality is deactivated if the car is under braking conditions |

## Refinement of the System Architecture

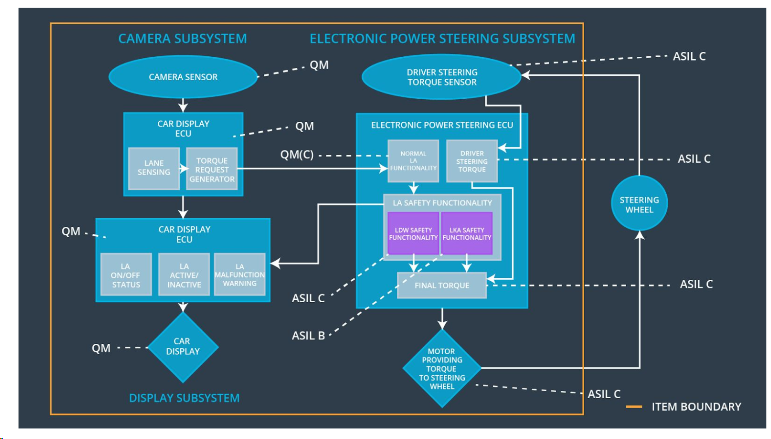


Fig 2: Refined Lane Assistance System Architecture

## 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 lane keeping item shall ensure that the lane departure oscillating torque amplitude is below Max\_torque\_Amplitude | **X** |  |  |
| Functional  Safety  Requirement  01-02 | The lane keeping item shall ensure that the lane departure oscillating torque frequency is below Max\_Torque\_Frequency | **X** |  |  |
| Functional  Safety  Requirement  01-03 | The lane keeping item shall ensure that the lane departure oscillating torque will be turned off when the driver is applying more than Max\_Driver\_Torque\_Amplitude | **X** |  |  |
| Functional Safety  Requirement  02-01 | The electronic power steering ECU shall ensure that the Lane Keeping Assistance torque is applied only for Max\_Duration | **X** |  |  |
| Functional  Safety  Requirement  02-02 | The electronic power steering ECU shall ensure that the Lane Keeping Assistance shall be deactivated under braking conditions | **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 warning on Car Display |