

Functional Safety Concept Lane Assistance

**Document Version:** 2.0

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



# Document history

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Editor | Description |
| 23-May-18 | 1.0 | Shaurya Dwivedi | Initial Attempt |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# 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 methodically analyzes system functions and malfunctions and converts potential malfunctions into functional safety 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 must be limited to prevent loss of control of the driver. |
| Safety\_Goal\_02 | The lane departure warning function should be time limited and the additional steering torque should end after a given time interval so that the driver does not abuse the system for autonomous driving. |

## Preliminary Architecture

Refer to Figure 1 for a system architecture diagram.

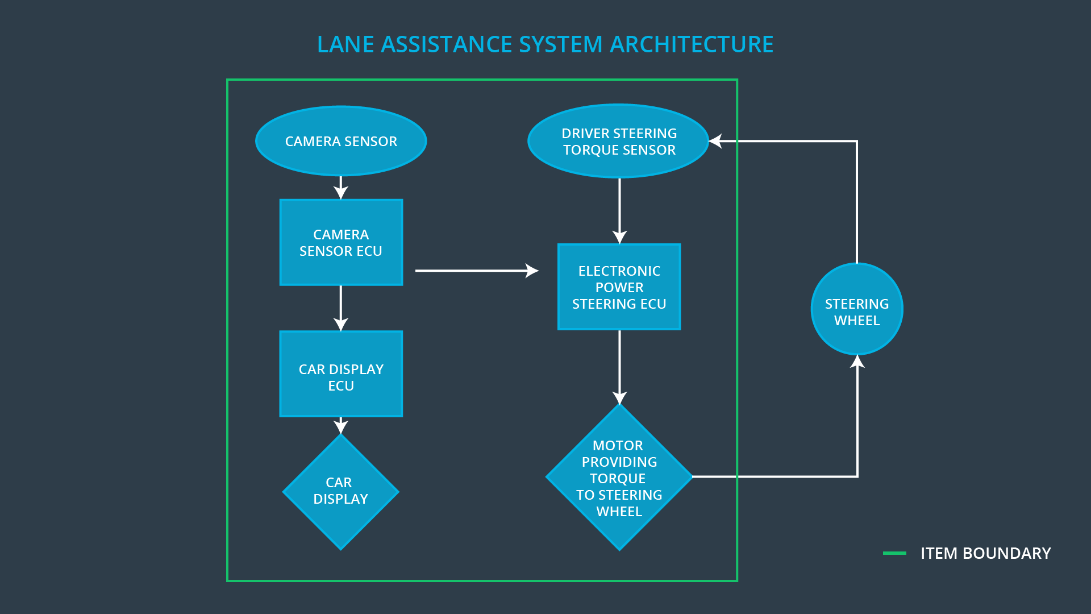


Figure 1: Lane Assistance System Architecture Diagram

### Description of architecture elements

|  |  |
| --- | --- |
| **Element** | **Description** |
| Camera Sensor | Images of the road surface captured and sent to the camera sensor controller. |
| Camera Sensor ECU | This system receives inputs from the camera sensor. Identified when the vehicle has accidentally left the ego lane, and sends the appropriate signals to the car display ECU and the electronic power steering ECU. |
| Car Display | Give the driver feedback with warnings and the status of Lane Departure Assistance. |
| Car Display ECU | Use the vehicle display component to view the lane departure warning and lane departure status. |
| Driver Steering Torque Sensor | This system senses the amplitude and frequency of the steering torque and sends the information to the electronic power steering controller. |
| Electronic Power Steering ECU | This system receives an input from the sensor ECU of the camera and the driver's steering torque sensor and calculates the torque and the time required for LKA and updates the engine. |
| Motor | Applies the torque indicated by the electronics. |

# Functional Safety Concept

The functional safety concept consists of:

* Functional safety analysis
* Functional safety requirements
* Functional security 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 | The Lane Departure Warning (LDW) function must use an oscillating steering torque to give the driver a haptic feedback | MORE | The LDW function generates an oscillating torque with a very high torque amplitude (above the limit). |
| Malfunction\_02 | The Lane Departure Warning (LDW) function must use an oscillating steering torque to give the driver a haptic feedback | MORE | The Lane Keeping Warning function applies a very high torque frequency oscillating torque (above the 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 |

## 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 point must ensure that the oscillating torque amplitude of the lane departure warning is below Max\_Torque\_Amplitude. | C | 50 ms | The LDW sets the oscillating torque amplitude to 0. Since the oscillating torque is 0, no torque would be applied to the steering wheel. |
| Functional  Safety  Requirement  01-02 | The lane departure point must ensure that the lane departure warning oscillating torque amplitude is below Max\_Torque\_Frequency | C | 50 ms | It is in the off state because the LDW sets the oscillating torque amplitude to 0. |

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 whether the chosen Max\_Torque\_Amplitude is appropriate for drivers | If Max\_Torque\_Amplitude is exceeded, test whether the Lane Assistant output within the 50 ms FTTI is zeroed by error injection. It is natural that if the torque amplitude exceeds the defined threshold, the system will be turned off within 50 ms. |
| Functional  Safety  Requirement  01-02 | Test whether the chosen Max\_Torque\_Frequency is appropriate for drivers | As we know, when the torque amplitude exceeds the defined limit, the system shuts off within 50 ms. Therefore, we need to test whether the track hold output within the 50 ms FTTI is set to zero by error injection. |

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 must ensure that the assistance torque for the tracking applies only to Max\_Duration | B | 500 ms | The state will be off since the LKA will set the oscillating torque amplitude 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 | Test if the Max\_duration selection prevents drivers from taking their hands off the steering wheel. | Make sure the system is turned off when the LKA exceeds Max\_Duration. |

## Refinement of the System Architecture

The refined System Architecture diagram is found in Figure 2.



Figure 2: Refined 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 departure point must ensure that the oscillating torque amplitude of the lane departure warning is below Max\_Torque\_Amplitude | **X** |  |  |
| Functional  Safety  Requirement  01-02 | The lane departure point must ensure that the lane departure warning oscillating torque amplitude is below Max\_Torque\_Frequency | **X** |  |  |
| Functional  Safety  Requirement  02-01 | The electronic power steering ECU must ensure that the assistance torque for the tracking applies only to Max\_Duration | **X** |  |  |

## Warning and Degradation Concept

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Degradation Mode** | **Trigger for Degradation Mode** | **Safe State invoked?** | **Driver Warning** |
| WDC-01 | Steering torque frequency and/or amplitude are degraded. | Steering torque exceeds Max\_Torque\_Frequency and/or Max\_Torque\_Amplitude | Yes | This system should turn on the warning light on dashboard. |
| WDC-02 | Lane keeping assistance function will turn off. | Torque is applied for a duration exceeding Max\_Duration | Yes | This system should turn on the warning light on dashboard |