

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 | Sharath Srinivasan | Initial Draft |
| 24-May-18 | 2.0 | Sharath Srinivasan | LKA Safe State Modification |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# 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 analyzes system functions and malfunctions methodically, converting potential malfunctions in 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 shall be limited to prevent the loss of the driver’s control. |
| Safety\_Goal\_02 | The lane keeping assistance function should be constrained time limited and the additional steering torque should end after a given time interval so that the driver does not misuse the system for autonomous driving. |

## Preliminary Architecture

Refer to Figure 1 for a system architecture diagram.

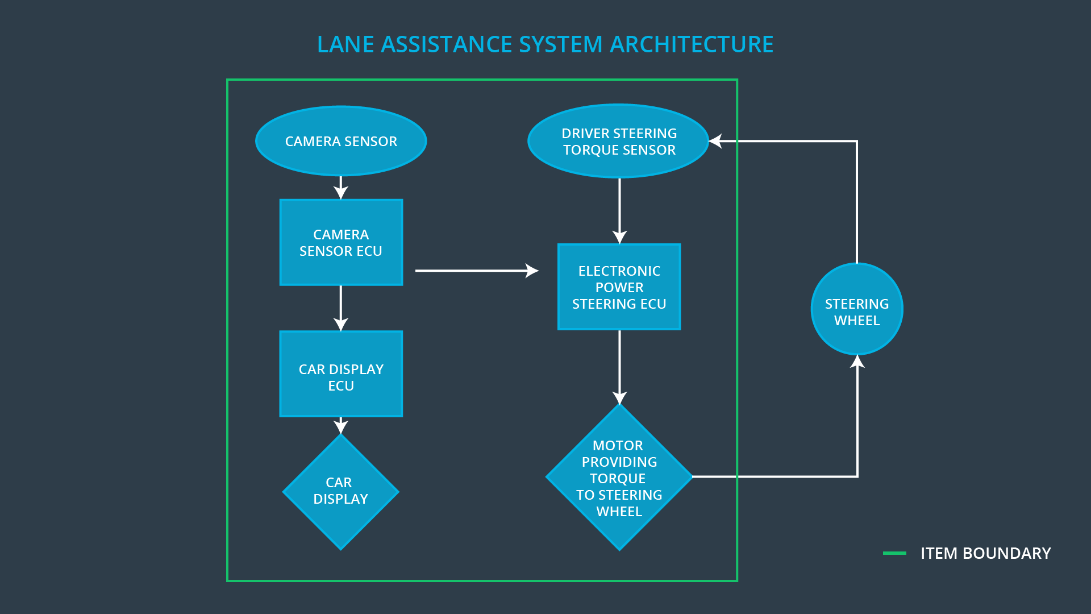


Figure : Lane Assistance System Architecture Diagram

### Description of architecture elements

|  |  |
| --- | --- |
| **Element** | **Description** |
| Camera Sensor | Images of the road surface that are captured and sent to the Camera Sensor ECU. |
| Camera Sensor ECU | This system receives input from the Camera Sensor. Identifies when the vehicle has accidentally left the ego lane and transmits the appropriate signals to the Car Display ECU and Electronic Power Steering ECU. |
| Car Display | This system displays warnings generated by the Car Display ECU to the driver regarding the status of various subsystems. |
| Car Display ECU | This system receives status from the Camera Sensor ECU and Electronic Power Steering ECU and activates lights on the car display if a warning is to be displayed. |
| Driver Steering Torque Sensor | This system senses the amplitude and frequency of steering torque and sends the information to the Electronic Power Steering ECU. |
| Electronic Power Steering ECU | This system receives input from the camera Sensor ECU and driver steering torque sensor and calculates the torque and time duration needed for LKA and update the motor. |
| Motor | This system receives input from the Electronic Power Steering ECU. Adjusts the steering angle by transmitting the appropriate torque amplitude and frequency. The signal is transmitted 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 | LDW 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 |

## 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 warning oscillating torque amplitude is below Max\_Torque\_Amplitude | C | 50 ms | The LDW will set the oscillating torque amplitude to 0. Since the oscillating torque is 0 there would be no torque is applied to the steering wheel) |
| Functional  Safety  Requirement  01-02 | The lane keeping item shall ensure that the lane departure warning oscillating torque amplitude is below Max\_Torque\_Frequency | C | 50 ms | It is in off state as the LDW will set 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 | When Max\_Torque\_Amplitude is exceeded, test whether the lane assistance output is set to zero within the 50 ms FTTI by fault injection. It is natural that when the torque amplitude crosses the defined limit, system is turned off within the 50ms |
| Functional  Safety  Requirement  01-02 | Test whether the chosen Max\_Torque\_Frequency is appropriate for drivers | As we know when the torque amplitude crosses the defined limit, system is turned off within the 50ms thus, we must test whether the lane assistance output is set to zero within the 50 ms FTTI by fault 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 shall ensure that the lane keeping assistance torque is applied for only Max\_Duration | B | 500 ms | The state will be at the off state as the LKA will set the oscillating torque amplitude to 0. |

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 whether the chose Max\_duration dissuades drivers from removing hands from the steering wheel | Verify that the system turns off if the LKA exceeds the Max\_Duration. |

## Refinement of the System Architecture

The refined System Architecture diagram is found in Figure 2.



Figure : 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 keeping item shall ensure that the lane departure warning oscillating torque amplitude is below Max\_Torque\_Amplitude | **X** |  |  |
| Functional  Safety  Requirement  01-02 | The lane keeping item shall 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 shall ensure that the lane keeping assistance torque is applied for only 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 |