

Functional Safety Concept Lane Assistance

**Document Version: [Version]**

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



# Document history

**[Instructions: Fill in the date, version and description fields. You can fill out the Editor field with your name if you want to do so. Keep track of your editing as if this were a real world project.**

**For example, if this were your first draft or first submission, you might say version 1.0. If this is a second submission attempt, then you'd add a second line with a new date and version 2.0]**

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Editor | Description |
| 12/05/2018 | 1.0 | Sundeep Pundamale Selvaraj | First Draft |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# Table of Contents

**[Instructions: We have provided a table of contents. If you change the document structure, please update the table of contents accordingly. The table of contents should show each section of the document and page numbers or links. Most word processors can do this for you. In** [**Google Docs**](https://support.google.com/docs/answer/116338?co=GENIE.Platform%3DDesktop&hl=en)**, you can use headings for each section and then go to Insert > Table of Contents.** [**Microsoft Word**](https://support.microsoft.com/en-us/help/285059/how-to-create-a-table-of-contents-by-marking-text-in-word) **has similar capabilities]**

[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 main goal of the Functional Safety Concept is to avoid accidents by reducing the risk to acceptable levels. By looking at the architectural design and the subsystems the safety goals are derived. The safety goals are further refined to functional safety requirement and mapped to appropriate place in the item architecture.

# Inputs to the Functional Safety Concept

## Safety goals from the Hazard Analysis and Risk Assessment

**[Instructions:**

**REQUIRED:**

**Provide the lane departure warning and lane keeping assistance safety goals as discussed in the lessons and derived in the hazard analysis and risk assessment.**

**OPTIONAL:**

**If you expanded the hazard analysis and risk assessment to include other safety goals, include them here.**

**]**

|  |  |
| --- | --- |
| **ID** | **Safety Goal** |
| Safety\_Goal\_01 | The oscillating steering toque from the Lane Departure Warning should be limited |
| Safety\_Goal\_02 | The Lane Keeping Assistance to be time limited and the additional torque to end after a specific time interval so that the driver does not misuse the system for autonomous driving |
| Safety\_Goal\_03 | Lane Keeping Assistance (LKA) function to enable the steering torque based on the maximum distance from the centre of the lane and minimum distance from edge of the road |
| Safety\_Goal\_04 | When the Lane Departure Warning (LDW) fails the Lane Keeping Assistance should be de-activated |

## Preliminary Architecture



### Description of architecture elements

|  |  |
| --- | --- |
| **Element** | **Description** |
| Camera Sensor | The camera sensor reads the road images and provides the data to Camera Sensor ECU |
| Camera Sensor ECU | The camera sensor ECU calculates the position of the car with respect to the road lanes and sends the appropriate notification to the Car Display ECU and the Electronic Power Steering ECU |
| Car Display | The car display provides visual notification to warn the driver about the Lane departure status |
| Car Display ECU | The Car display ECU controls the car display by enabling or disabling the Lane keeping assistance and the Lane departure assistance status |
| Driver Steering Torque Sensor | The driver steering torque sensor measures the torque applied by the driver on the steering wheel |
| Electronic Power Steering ECU | The Electronic power steering ECU collects information from the Driver steering torque sensor and the torque request message from the camera sensor ECU and in turn notifies the collective torque to be applied by the Motor |
| Motor | The motor applies the torque to the steering wheel as notified by the Electronic power steering 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

**[Instructions: Fill in the functional safety analysis table below.]**

|  |  |  |  |
| --- | --- | --- | --- |
| **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 with haptic feedback | MORE | With the high haptic feedback the driver might lose control over the vehicle and collide with other vehicles or other infrastructure on the road |
| Malfunction\_02 | Lane Keeping Assistance (LKA) function shall apply the steering torque when active in order to stay in ego lane | MORE | The driver treats the function as if it was meant for autonomous driving and eventually does not react when required |
| Malfunction\_03 | Lane Keeping Assistance (LKA) function shall apply the steering torque when active in order to stay in ego lane | EARLY | With the Lane keeping assistance applying the steering torque too early might lead to confusion in the tunnel and the driver might lose control over the vehicle |
| Malfunction\_04 | Lane Departure Warning (LDW) function shall apply an oscillating steering torque to provide the driver with haptic feedback | NO | Without the Lane Departure warning providing haptic feedback, the driver might potentially oversteer the vehicle when the Lane Keeping Assistance applies the steering torque in order to keep the vehicle in the ego lane |

## Functional Safety Requirements

**[Instructions: Fill in the functional safety requirements for the lane departure warning ]**

Lane Departure Warning (LDW) Requirements:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Functional Safety Requirement** | **ASIL** | **Fault Tolerant Time Interval** | **Safe State** |
| Functional  Safety  Requirement  01-01 | The Lane Departure Warning function shall ensure that the lane departure torque amplitude is always below the Max\_Torque\_Amplitude | C | 50 MS | The torque amplitude is always below Max\_Torque\_Amplitude |
| Functional  Safety  Requirement  01-02 | The Lane Departure Warning functional shall ensure that the lane departure torque amplitude is always below the Max\_Torque\_Frequency | C | 50 MS | The torque frequency is always below the Max\_Torque\_Frequency |
| Functional  Safety  Requirement  01-03 | The Lane Departure Warning function shall be de-activated when the Camera ECU stops working | C | 10 MS | The Lane Departure function is de-activated |

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 if the driver can control the steering when the value is close to Max\_Torque\_Amplitude | The driver is able to control the steering when the value is close to Max\_Torque\_Aplitude and the system is turned off when the value exceeds the set Max limit |
| Functional  Safety  Requirement  01-02 | Validate if the driver can control the steering when the value is close to Max\_Torque\_Frequency | The driver is able to control the steering wjhen the value is close to Max\_Torque\_Frequency and the system is turned off when the value exceeds the set Max limit |
| Functional  Safety  Requirement  01-03 | Validate if the Lane Departure function is off when the camera sensor is not working | The Lane Departure warning is never activated when the camera sensor is not working |

Lane Keeping Assistance (LKA) Requirements:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Functional Safety Requirement** | **ASIL** | **Fault Tolerant Time Interval** | **Safe State** |
| Functional  Safety  Requirement  02-01 | The Lane Keeping Assistance Warning shall ensure that the torque is applied on the steering for a Max\_Duration only | C | 500 MS | The Lane Keeping Assistance torque value is zero |
| Functional  Safety  Requirement  02-02 | The Lane Keeping Assistance shall ensure that the lane keeping torque is zero when the camera ECU specifies that the Max\_Distance\_From\_Center\_Lane is below the threshold and Min\_Distance\_From\_Edge of the road is above the threshold | C | 50 MS | The Lane Keeping Assistance is turned off |

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 if the Max\_Duration chosen does not let the driver to context switch from a self-driven car to autonomous car in the behavioural studies | Verify if the Lane Keeping Assistance is deactivated after exceeding the Max\_Duration |
| Functional  Safety  Requirement  02-01 | Validate if the lane keeping assistance is deactivated when the Max\_Distance\_From\_Center\_Lane is below the threshold and Min\_Distance\_From\_Edge of the road is above the threshold | Verify the Lane Keeping Assistance is always deactivated when the Max\_Distance\_From\_Center\_Lane is below the threshold and Min\_Distance\_From\_Edge of the road is above the threshold |

## Refinement of the System Architecture



## Allocation of Functional Safety Requirements to Architecture Elements

**[Instructions: Mark which element or elements are responsible for meeting the functional safety requirement. Hint: Only one ECU is responsible for meeting all of the requirements.]**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Functional Safety Requirement** | **Electronic Power Steering ECU** | **Camera ECU** | **Car Display ECU** |
| Functional  Safety  Requirement  01-01 | The Lane Departure Warning function shall ensure that the lane departure torque amplitude is always below the Max\_Torque\_Amplitude | **X** |  |  |
| Functional  Safety  Requirement  01-02 | The Lane Departure Warning functional shall ensure that the lane departure torque amplitude is always below the Max\_Torque\_Frequency | **X** |  |  |
| Functional  Safety  Requirement  01-03 | The Lane Departure Warning function shall be de-activated when the Camera ECU stops working | **X** |  |  |
| Functional  Safety  Requirement  02-01 | The Lane Keeping Assistance Warning shall ensure that the torque is applied on the steering for a Max\_Duration only | **X** |  |  |
| Functional  Safety  Requirement  02-02 | The Lane Keeping Assistance shall ensure that the lane keeping torque is zero when the camera ECU specifies that the Max\_Distance\_From\_Center\_Lane is below the threshold and Min\_Distance\_From\_Edge of the road is above the threshold | **X** |  |  |

## Warning and Degradation Concept

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Degradation Mode** | **Trigger for Degradation Mode** | **Safe State invoked?** | **Driver Warning** |
| WDC-01 | Turn off the Lane Departure Warning functionality | Malfunction\_01, Malfunction\_04 | YES | Lane departure status to be displayed as broken on the car display |
| WDC-02 | Turn off the Lane Keeping Assistance functionality | Malfunction\_02, Malfunction\_03 | YES | Lane keeping assistance to be displayed as broken on the car display |