

Functional Safety Concept Lane Assistance

**Document Version: 1.1**



# Document history

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Editor | Description |
| 11.03.2018 | 1.0 | Nathan Greco | First Draft |
| 18.03.2018 | 1.1 | Nathan Greco | Updated for second submission |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# 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 is a high level plan that defines both the architecture being implemented and the safety goals necessary to ensure the system satisfies ISO 26262.

# 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 lane departure warning function shall be limited |
| Safety\_Goal\_02 | The lane keeping assistance 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 | Alert driver by other means (audible or visual) when LDW cannot detect lane lines |
| Safety\_Goal\_04 | Alert driver by other means (audible or visual) when LDW cannot detect lane lines |

## Preliminary Architecture



**Figure 1** – System Architecture

### Description of architecture elements

The system can be broken down into main components as shown in figure 1, defined as:

|  |  |
| --- | --- |
| **Element** | **Description** |
| Camera Sensor | Camera device that retrieves images of the road in front of the vehicle |
| Camera Sensor ECU | Device which interfaces with camera, steering ECU, and camera display. It is also the processor of the image and interprets the road images with computer vision algorithms to determine the vehicles position relative to the road. |
| Car Display ECU | An informative display to display the road lines and their orientation, display warning and alert messages, and is the primary GUI for the vehicle operator. |
| Car Display | Controller for the camera display. Receives information from the camera ECU regarding the road line positions and any error or warning messages necessary to indicate. |
| Driver Steering Torque Sensor | A sensor that measures that amount of effort the driver is making to steer the vehicle. This is important so that we do not interfere with intentional steering commands from the driver and impede his ability to control the vehicle. |
| Electronic Power Steering ECU | The controller of steering assist motor. It takes input from the camera ECU and steering torque sensor and determines how much of a torque correction, if any, is necessary to correct the current vehicle path. |
| Motor | The actuator that directly influences the steering of the vehicle. It receives its command from the 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

|  |  |  |  |
| --- | --- | --- | --- |
| **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 Departure Warning (LDW) function shall apply an oscillating steering torque to provide the driver a haptic feedback | LATE | Systems fails to alert the driver about unintentional lane departure in sufficient time to correct |
| Malfunction\_05 | Lane Keeping Assistance (LKA) function shall apply the steering torque when active in order to stay in ego lane | NO | LKA fails to prevent an unintentional vehicle lane departure |

## 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 Disabled with visual indication |
| 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 Disabled with visual indication |
| Functional  Safety  Requirement  01-03 | As soon as the LDW function fails to detect the lane lines, the ‘LDW Safety' software block shall disable the system and send a signal to the car display ECU to turn on a warning light. | B | 50 ms | LDW Disabled with visual indication |

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 | Perform controlled study with multiple drivers to determine thresholds for noticeable haptic feedback amplitude that interferes with driver control | Verify that in conditions are established limits exceeded |
| Functional  Safety  Requirement  01-02 | Perform controlled study with multiple drivers to determine thresholds for noticeable haptic feedback frequency that interferes with driver control | Verify that in conditions are established limits exceeded |
| Functional  Safety  Requirement  01-03 | Testing must be done to determine the allowable time to pass before the system should be fully disabled | Verify that when camera vision is blocked the system shuts off within specified time |

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 | LDW Disabled with visual indication |
| Functional  Safety  Requirement  02-02 | As soon as the LKA function fails to detect the lane lines, the ‘LKA Safety' software block shall disable the system and send a signal to the car display ECU to turn on a warning light. | B | 50 ms | LKA Disabled with visual indication |

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 | Evaluate typical controller response time and tuning to determine what an acceptable response time is. | Verify that the actuator will always be disabled if it doesn’t respond to the time within that window |
| Functional  Safety  Requirement  02-02 | Testing must be done to determine the allowable time to pass before the system should be fully disabled | Verify that when camera vision is blocked the system shuts off within specified time |

## Refinement of the System Architecture

## 

**Figure 2** – Detailed system architecture with ASIL ratings

## 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 | As soon as the LDW function fails to detect the lane lines, the ‘LDW Safety' software block shall disable the system and send a signal to the car display ECU to turn on a warning light. | **X** |  | **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** |  |  |
| Functional  Safety  Requirement  02-02 | As soon as the LKA function fails to detect the lane lines, the ‘LKA Safety' software block shall disable the system and send a signal to the car display ECU to turn on a warning light. | **X** |  | **X** |

## Warning and Degradation Concept

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Degradation Mode** | **Trigger for Degradation Mode** | **Safe State invoked?** | **Driver Warning** |
| WDC-01 | Disable LDW and alert | Malfunction\_01 | Yes | Driver indication of fault in LDW system |
| WDC-02 | Disable LDW and alert | Malfunction\_02 | Yes | Driver indication of fault in LDW system |
| WDC-03 | Disable LKA and alert | Malfunction\_03 | Yes | Driver indication of fault in LKA system |
| WDC-04 | Disable LDW and alert | Malfunction\_04 | Yes | Driver indication of fault in LDW system |
| WDC-05 | Disable LKA and alert | Malfunction\_05 | Yes | Driver indication of fault in LKA system |