

Functional Safety Concept Lane Assistance

**Document Version: [Version]**

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



# 

# Document history

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Editor | Description |
| 12/12/17 | 1.0 | Raz Nissim | Initial version |
| 18/12/17 | 2.0 | Raz Nissim | Third 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

A Functional Safety Concept generates actual requirements from the general functional safety goals. These are then allocated to subsystems and parts of the system. The system architecture may require modification to meet the functional safety requirements. Each of the requirements has attributes relating to the ASIL level, the fault tolerant time interval and the safe state of the system. Verification and validation of the requirements are discussed. This document does not include the technical implementation of the design.

# 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 kepping 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. |

## Preliminary Architecture

The preliminary architecture is depicted in the figure below.

### https://d17h27t6h515a5.cloudfront.net/topher/2017/July/5976aa23_02-advanced-driver-assistance-system-architecture-02-1/02-advanced-driver-assistance-system-architecture-02-1.png

### Description of architecture elements

|  |  |
| --- | --- |
| **Element** | **Description** |
| Camera Sensor | Physical sensor responsible for detecting lane lines. |
| Camera Sensor ECU | Electronics hardware and processor responsible for processing camera data, identifying lane markings, determining vehicle position and issuing torque requests to the electronic power steering ECU. |
| Car Display | Visual indicator responsible for displaying warning to the driver, when the vehicle departs the lane. |
| Car Display ECU | Electronics hardware responsible for interpreting input from other systems and controlling the car display. |
| Driver Steering Torque Sensor | Sensor responsible for measuring steering torque input on the steering wheel from the driver. |
| Electronic Power Steering ECU | Responsible for receiving torque commands from other systems, monitoring the driver torque input and actuating the vehicle steering motor. |
| Motor | Responsible for applying the torque 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 | LDW function applies MORE oscillating steering torque to the steering wheel. | Driver loses control of the vehicle. Collision with other vehicle or obstacle. |
| Malfunction\_02 | Lane Departure Warning (LDW) function shall apply an oscillating steering torque to provide the driver a haptic feedback | LDW function applies oscillating steering torque in the WRONG situation. | Unexpected activation during normal city driving. |
| Malfunction\_03 | Lane Keeping Assistance (LKA) function shall apply the steering torque when active in order to stay in ego lane | LKA function applies WRONG correction steering torque. | Vehicle is steered off the road, resulting in a crash. |

## 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 EPS ECU shall ensure that the lane departure warning torque amplitude is below is Max\_Torque\_Amplitude | C | 50ms | Set vibration torque amplitude to 0. |
| Functional  Safety  Requirement  01-02 | The EPS ECU shall ensure that the lane departure warning torque frequency is below is Max\_Torque\_Frequency | C | 50ms | Set vibration 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 | Validate MAX\_TORQUE\_AMPLITUDE is high enough to be detected by the driver, while low enough not to cause loss of steering control. | Verify system turns off if MAX\_TORQUE\_AMPLITUDE is exceeded. |
| Functional  Safety  Requirement  01-02 | Validate MAX\_TORQUE\_FREQUENCY is high enough to be detected by the driver, while low enough not to cause loss of steering control. | Verify system turns off if MAX\_TORQUE\_FREQUENCY is exceeded. |

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 only applied for MAX\_DURATION | B | 500 | Set lane keeping assistance torque 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 | Driver testing is used to determine if applying assistance torque for only MAX\_DURATION keeps drivers from using the LKA as an autonomous function. | Timing is used to verify that the lane keeping assistance function is turned off after MAX\_DURATION. |

## Refinement of the System Architecture

The refined system architecture is depicted in the figure below.



## 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 function shall ensure that the lane departure oscillating torque amplitude is below Max\_Torque\_Amplitude | **Yes** | **No** | **No** |
| Functional  Safety  Requirement  01-02 | The lane keeping function shall ensure that the lane departure oscillating torque amplitude is below Max\_Torque\_Frequency | **Yes** | **No** | **No** |
| Functional  Safety  Requirement  02-01 | The electronic power steering ECU shall ensure that lane keeping assist torque is set to 0 when camera ECU stops detecting lanes. | **Yes** | **No** | **No** |

## Warning and Degradation Concept

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Degradation Mode** | **Trigger for Degradation Mode** | **Safe State invoked?** | **Driver Warning** |
| WDC-01 | turn off the functionality | Malfunction\_01/02 | yes | Car display |
| WDC-02 | turn off the functionality | Malfunction\_03 | yes | Car display |