

Functional Safety Concept Lane Assistance

**Document Version: 1.0**



# 

# Document history

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Editor | Description |
| 06/06/2019 | 1.0 | M. Elbanhawi | First 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 purpose of the functional safety document is to allocate functional requirements and their attributes based on the safety goals defined in the hazard and risk assessment.

# Inputs to the Functional Safety Concept

## Safety goals from the Hazard Analysis and Risk Assessment

|  |  |
| --- | --- |
| **ID** | **Safety Goal** |
| Safety\_Goal\_01 | The LDW function shall be torque limited to avoid oscillations and loss of control. |
| Safety\_Goal\_02 | The LKA 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 as an autonomous driving feature. |
| Safety\_Goal\_03 | The LDW function shall not be active in case of a camera subsystem malfunction |
| Safety\_Goal\_04 | The LKA function shall not be active in case of a camera subsystem malfunction |

## Preliminary Architecture



### Description of architecture elements

|  |  |
| --- | --- |
| **Element** | **Description** |
| Camera Sensor | Responsible for capturing images sending them to the camera ECU. |
| Camera Sensor ECU | Responsible for processing image, detecting lanes and the position of the vehicle within the lane. |
| Car Display | Human machine interface for alert and warnings to the driver. |
| Car Display ECU | Responsible for controlling the display component to indicate the statues of LDW and LKA functions. |
| Driver Steering Torque Sensor | Measure input torque by the driver |
| Electronic Power Steering ECU | Apply a necessary torque to the steering wheel based on a command from LDA and LKD systems. |
| Motor | Applies torque requested by 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 | LDW apply a high torque on a slippery wet road at high speed driving |
| Malfunction\_02 | Lane Departure Warning (LDW) function shall apply an oscillating steering torque to provide the driver a haptic feedback | MORE | LDW apply a high torque on a slippery wet road at high speed driving |
| Malfunction\_03 | Lane Keeping Assistance (LKA) function shall apply the steering torque when active in order to stay in ego lane | NO | LKA is active and the driver is not required to keep hands on steering wheel. Results in misuse of LKW as Autonomous driving mode. |

## 

## 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 | Disable system |
| Functional  Safety  Requirement  01-02 | The lane keeping item shall ensure that the lane departure oscillating torque frequency is below Max\_Torque\_Frequency |  | 50 ms | Disable system |

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 | Apply an oscillating torque amplitude is below Max\_Torque\_Amplitude and validate the drive does not lose control of the vehicle and is aware of the warning | Verity the system is disabled if torque amplitude is above Max\_Torque\_Amplitude |
| Functional  Safety  Requirement  01-02 | Apply an oscillating torque frequency is below Max\_Torque\_Frequency and validate the drive does not lose control of the vehicle and is aware of the warning | Verity the system is disabled if frequency is below Max\_Torque\_Frequency |

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 limit lane keeping assistance torque for only Max\_Duration | B | 500 ms | Disable system. |

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 the Max\_Duration of 500ms and validate that drivers maintain their hands on the wheel and do not abuse the system. | Verify that the system is disabled after exceeding Max\_Duration |

## Refinement of the 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 | Apply an oscillating torque amplitude is below Max\_Torque\_Amplitude and validate the drive does not lose control of the vehicle and is aware of the warning | **X** |  |  |
| Functional  Safety  Requirement  01-02 | Apply an oscillating torque frequency is below Max\_Torque\_Frequency and validate the drive does not lose control of the vehicle and is aware of the warning | **X** |  |  |
| Functional  Safety  Requirement  02-01 | The electronic power steering ECU shall limit lane keeping assistance torque for only Max\_Duration | **X** |  |  |

## Warning and Degradation Concept

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Degradation Mode** | **Trigger for Degradation Mode** | **Safe State invoked?** | **Driver Warning** |
| WDC-01 | Disable LDW system | Malfunction\_01  Malfunction\_02 | Yes | Dashboard alert |
| WDC-02 | Disable LKA system | Malfunction\_03 | Yes | Dashboard alert |